Algebra[1]

Wolfgang Soergel

14. Dezember 2011

[1]Für die bebilderte 10MB-Version siehe . . ./ALGEBRAmitBildern.pdf

Inhaltsverzeichnis

Teil A

Grundlagen

Kapitel I

Allgemeine Grundlagen

Hier habe ich Notationen und Begriffsbildungen zusammengefaßt, von denen ich mir vorstelle, daß sie zu Beginn des Studiums in enger Abstimmung zwischen den beiden Grundvorlesungen erklärt werden könnten.

Inhalt

1 Einstimmung

1.1 Vollständige Induktion und binomische Formel

Satz 1.1.1. *Für jede natürliche Zahl* $n \geq 1$ *gilt* $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$.

Beweis. Bei diesem Beweis sollen Sie gleichzeitig das Beweisprinzip der **vollständigen Induktion** lernen. Wir bezeichnen mit $A(n)$ die Aussage, daß die Formel im Satz für ein gegebenes n gilt, und zeigen:

Induktionsbasis: Die Aussage $A(1)$ ist richtig. In der Tat gilt die Formel $1 = \frac{1(1+1)}{2}$.

Induktionsschritt: Aus $A(n)$ folgt $A(n+1)$. In der Tat, unter der Annahme, daß unsere Formel für ein gegebenes n gilt, der sogenannten **Induktionsannahme** oder **Induktionsvoraussetzung**, rechnen wir

$$\begin{aligned} 1 + 2 + \ldots + n + (n+1) &= \tfrac{n(n+1)}{2} + \tfrac{2(n+1)}{2} \\ &= \tfrac{(n+2)(n+1)}{2} \\ &= \tfrac{(n+1)((n+1)+1)}{2} \end{aligned}$$

und folgern so, daß die Formel auch für $n + 1$ gilt.

Es ist damit klar, daß unsere Aussage $A(n)$ richtig ist alias daß unsere Formel gilt für alle $n = 1, 2, 3, \ldots$. □

1.1.2. Das Zeichen □ deutet in diesem Text das Ende eines Beweises an und ist in der neueren Literatur weit verbreitet. Buchstaben in Formeln werden in der Mathematik üblicherweise kursiv notiert, so wie etwa das n oder auch das A im vorhergehenden Beweis. Nur Buchstaben oder Buchstabenkombinationen, die stets dasselbe bedeuten sollen, schreibt man nicht kursiv, wie etwa $\sin$ für den Sinus oder $\log$ für den Logarithmus. Diese Konvention steht in gewissem Widerspruch zur in der Physik üblichen Konvention, Abkürzungen für Einheiten kursiv zu setzen, wie etwa m für "Meter".

1.1.3. Der vorhergehende Beweis stützt sich auf unser intuitives Verständnis der natürlichen Zahlen. Man kann das Konzept der natürlichen Zahlen auch formal einführen und so die natürlichen Zahlen in gewisser Weise "besser" verstehen. Das mögen Sie in der Logik lernen. Das Wort "Induktion" meint eigentlich "Hervorrufen", so wie etwa das Betrachten einer Wurst die Ausschüttung von Spucke induziert alias den Mund wässrig macht. Im Zussammenhang der vollständigen Induktion ist es dahingehend zu verstehen, daß die Richtigkeit unserer Aussage $A(0)$ die Richtigkeit von $A(1)$ induziert, die Richtigkeit von $A(1)$ hinwiederum

die Richtigkeit von $A(2)$, die Richtigkeit von $A(2)$ die Richtigkeit von $A(3)$, und immer so weiter.

1.1.4. Es herrscht keine Einigkeit in der Frage, ob man die Null eine natürliche Zahl nennen soll. In diesem Text ist stets die Null mit gemeint, wenn von natürlichen Zahlen die Rede ist. Wollen wir die Null dennoch ausschließen, so sprechen wir wie oben von einer "natürlichen Zahl $n \geq 1$".

1.1.5. Ich will kurz begründen, warum es mir natürlich scheint, auch die Null eine natürliche Zahl zu nennen: Hat bildlich gesprochen jedes Kind einer Klasse einen Korb mit Äpfeln vor sich und soll seine Äpfel zählen, so kann es ja durchaus vorkommen, daß in seinem Korb gar kein Apfel liegt, weil es zum Beispiel alle seine Äpfel bereits gegessen hat. In der Begrifflichkeit der Mengenlehre ausgedrückt, die wir in 2.1 einführen werden, muß man die leere Menge endlich nennen, wenn man erreichen will, daß jede Teilmenge einer endlichen Menge wieder endlich ist. Will man dann zusätzlich erreichen, daß die Kardinalität jeder endlichen Menge eine natürliche Zahl ist, so darf man die Null nicht aus den natürlichen Zahlen herauslassen.

1.1.6. Man kann sich den Satz anschaulich klar machen als eine Formel für die Fläche eines Querschnitts für eine Treppe der Länge n mit Stufenabstand und Stufenhöhe eins. In der Tat bedeckt ein derartiger Querschnitt ja offensichtlich ein halbes Quadrat der Kantenlänge n nebst n halben Quadraten der Kantenlänge 1. Ein weiterer Beweis geht so:

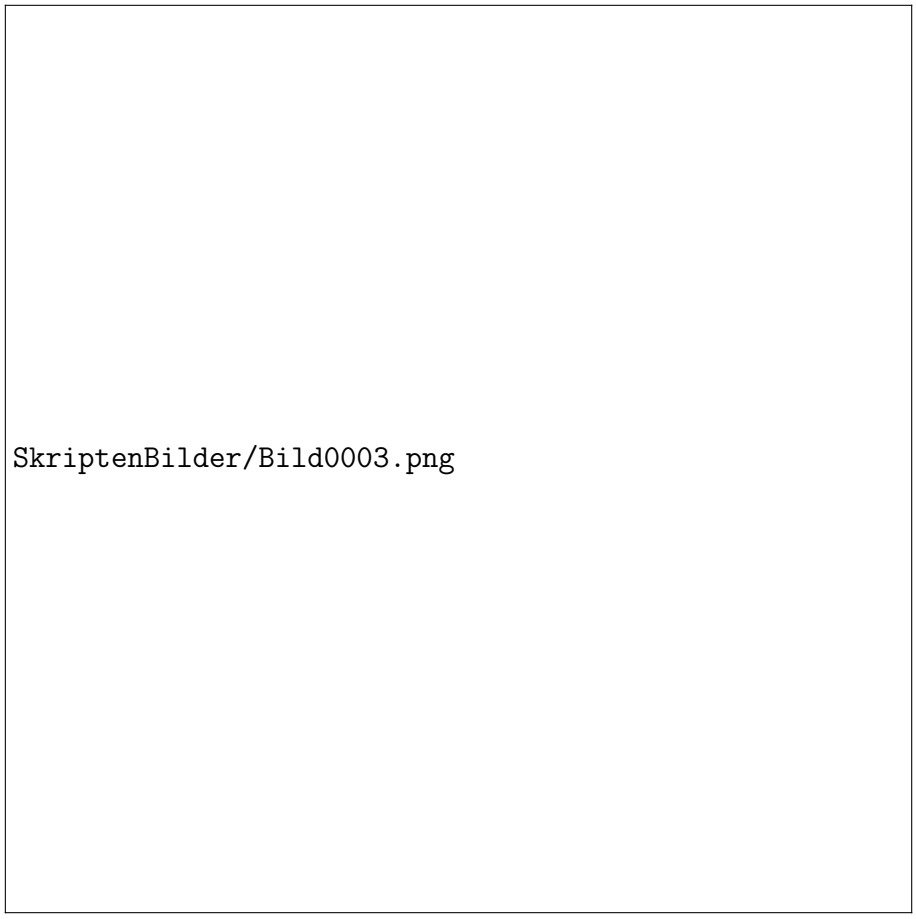
$$\begin{aligned} 1+2+\ldots+n &= \quad 1/2 \;+\; 2/2 \quad\; +\ldots\; + n/2 \\ &\quad + n/2 \;\; +(n-1)/2 \;\; +\ldots\; + 1/2 \\ &= \quad \tfrac{n+1}{2} \;+\; \tfrac{n+1}{2} \quad +\ldots\; + \tfrac{n+1}{2} \\ &= \quad n(n+1)/2 \end{aligned}$$

Ich will diesen Beweis benutzen, um eine neue Notation einzuführen.

Definition 1.1.7. Gegeben $a_1, a_2, \ldots, a_n$ schreiben wir

$$\sum_{i=1}^{n} a_i := a_1 + a_2 + \ldots + a_n$$

Das Symbol $\sum$ ist ein großes griechisches S und steht für "Summe". Das Symbol $:=$ deutet an, daß die Bedeutung der Symbole auf der doppelpunktbehafteten Seite des Gleichheitszeichens durch den Ausdruck auf der anderen Seite unseres Gleichheitszeichens definiert ist. Im obigen und ähnlichen Zusammenhängen heißen $a_1, \ldots, a_n$ die **Summanden** und i der **Laufindex**, da er eben etwa in unserem Fall von 1 bis n läuft und anzeigt alias "indiziert", welcher Summand gemeint ist.



Die Gesamtfläche dieses Treppenquerschnitts ist offensichtlich
$4^2/2 + 4/2 = 4 \cdot 5/2$

1.1.8. Das Wort "Definition" kommt aus dem Lateinischen und bedeutet "Abgrenzung". In Definitionen versuchen wir, die Bedeutung von Symbolen und Begriffen so klar wie möglich festzulegen. Sie werden merken, daß man in der Mathematik die Angwohnheit hat, in Definitionen Worte der Umgangssprache wie Menge, Gruppe, Körper, Unterkörper, Abbildung etc. "umzuwidmen" und ihnen ganz spezielle und meist nur noch entfernt mit der umgangssprachlichen Bedeutung verwandte Bedeutungen zu geben. In mathematischen Texten sind dann durchgehend diese umgewidmeten Bedeutungen gemeint. In dieser Weise baut die Mathematik also wirklich ihre eigene Sprache auf, bei der jedoch die Grammatik und auch nicht ganz wenige Wörter doch wieder von den uns geläufigen Sprachen übernommen werden. Das muß insbesondere für den Anfänger verwirrend sein, der sich auch bei ganz harmlos daherkommenden Wörtern stets wird fragen müssen, ob sie denn nun umgangssprachlich gemeint sind oder vielmehr bereits durch eine Definition festgelegt wurden. Um hier zu helfen, habe ich mir große Mühe mit dem Index gegeben, in dem alle an verschiedenen Stellen eingeführten oder umgewidmeten und dort fett gedruckten Begriffe verzeichnet sein sollten.

Beispiel 1.1.9. In der $\sum$-Notation liest sich der in 1.1.6 gegebene Beweis so:

$$\begin{aligned}
\textstyle\sum_{i=1}^{n} i &= \textstyle\sum_{i=1}^{n} \frac{i}{2} + \sum_{i=1}^{n} \frac{i}{2} \\
&\quad \text{und nach Indexwechsel } i = n+1-k \text{ hinten} \\
&= \textstyle\sum_{i=1}^{n} \frac{i}{2} + \sum_{k=1}^{n} \frac{n+1-k}{2} \\
&\quad \text{dann mache } k \text{ zu } i \text{ in der zweiten Summe} \\
&= \textstyle\sum_{i=1}^{n} \frac{i}{2} + \sum_{i=1}^{n} \frac{n+1-i}{2} \\
&\quad \text{und nach Zusammenfassen beider Summen} \\
&= \textstyle\sum_{i=1}^{n} \frac{n+1}{2} \\
&\quad \text{ergibt sich offensichtlich} \\
&= n(\tfrac{n+1}{2})
\end{aligned}$$

Beispiel 1.1.10. Ein anderer Beweis derselben Formel kann auch durch die folgende von der Mitte ausgehend zu entwickelnde Gleichungskette gegeben werden:

$$(n+1)^2 = \sum_{i=0}^{n} (i+1)^2 - i^2 = \sum_{i=0}^{n} 2i+1 = 2\sum_{i=0}^{n} i + \sum_{i=0}^{n} 1 = n+1+2\sum_{i=0}^{n} i$$

Definition 1.1.11. In einer ähnlichen Bedeutung wie $\sum$ verwendet man auch das Symbol $\prod$, ein großes griechisches P, für "Produkt" und schreibt

$$\prod_{i=1}^{n} a_i := a_1 a_2 \dots a_n$$

Die $a_1, \dots, a_n$ heißen in diesem und ähnlichen Zusammenhängen die **Faktoren** des Produkts.

Definition 1.1.12. Für jede natürliche Zahl $n \geq 1$ definieren wir die Zahl $n!$ (sprich: n **Fakultät**) durch die Formel

$$n! := 1 \cdot 2 \cdot \ldots \cdot n = \prod_{i=1}^{n} i$$

Wir treffen zusätzlich die Vereinbarung $0! := 1$ und haben also $0! = 1$, $1! = 1$, $2! = 2$, $3! = 6$, $4! = 24$ und so weiter.

Ergänzung 1.1.13. Wir werden in Zukunft noch öfter Produkte mit überhaupt keinem Faktor zu betrachten haben und vereinbaren deshalb gleich hier schon, daß Produkten, bei denen die obere Grenze des Laufindex um Eins kleiner ist als seine untere Grenze, der Wert 1 zugewiesen werden soll, also etwa $1 = \prod_{i=1}^{0} i$. Ebenso vereinbaren wir auch, daß Summen, bei denen die obere Grenze des Laufindex um Eins kleiner ist als seine untere Grenze, der Wert 0 zugewiesen werden soll, so daß wir in Erweiterung unserer Formel 1.1.1 etwa schreiben könnten $0 = \sum_{i=1}^{0} i$. Der Sinn dieser Erweiterungen zeigt sich darin, daß damit Formeln wie $\sum_{i=k}^{l} a_i = \sum_{i=k}^{m} a_i + \sum_{i=m+1}^{l} a_i$ auch für $m = k - 1$ richtig bleiben. Man mag sogar noch weiter gehen und die Definition von Summen auf beliebige untere und obere Grenzen so erweitern, daß diese Formeln richtig bleiben. In dieser Allgemeinheit ist diese Notation jedoch nur beim kontinuierlichen Analogon $\int$ des Summenzeichens üblich, wie in **??** ausgeführt wird.

Satz 1.1.14 (Bedeutung der Fakultät). *Es gibt genau $n!$ Möglichkeiten, n voneinander verschiedene Objekte in eine Reihenfolge zu bringen.*

Beispiel 1.1.15. Es gibt genau $3! = 6$ Möglichkeiten, die drei Buchstaben a, b und c in eine Reihenfolge zu bringen, nämlich

$$\begin{array}{ccc} abc & bac & cab \\ acb & bca & cba \end{array}$$

In gewisser Weise stimmt unser Satz sogar für $n = 0$: In der Terminologie, die wir in **??** einführen, gibt es in der Tat genau eine Anordnung der leeren Menge.

Beweis. Hat man n voneinander verschiedene Objekte, so hat man n Möglichkeiten, ein Erstes auszusuchen, dann $(n - 1)$ Möglichkeiten, ein Zweites auszusuchen und so weiter, bis schließlich nur noch eine Möglichkeit bleibt, ein Letztes auszusuchen. Insgesamt haben wir also in der Tat wie behauptet $n!$ mögliche Reihenfolgen. □

Definition 1.1.16. Wir definieren für beliebiges n und jede natürliche Zahl k die **Binomialkoeffizienten** $\binom{n}{k}$ (sprich: n **über** k) durch die Regeln

$$\binom{n}{k} := \prod_{j=0}^{k-1} \frac{n-j}{k-j} = \frac{n(n-1)\ldots \quad (n-k+1)}{k(k-1)\ldots \qquad 1} \text{ für } k \geq 1 \text{ und } \binom{n}{0} := 1.$$

Der Sonderfall $k = 0$ wird im Übrigen auch durch unsere allgemeine Formel gedeckt, wenn wir unsere Konvention 1.1.13 beherzigen. Im Lichte des folgenden Satzes schlage ich vor, die Binomialkoeffizienten $\binom{n}{k}$ statt "n über k" inhaltsreicher "k aus n" zu sprechen.

1.1.17. Die Bezeichnung als Binomialkoeffizienten leitet sich von dem Auftreten dieser Zahlen als Koeffizienten in der "binomischen Formel" 1.1.22 ab.

Satz 1.1.18 (Bedeutung der Binomialkoeffizienten). *Gegeben natürliche Zahlen n und k gibt es genau $\binom{n}{k}$ Möglichkeiten, aus n voneinander verschiedenen Objekten k Objekte auszuwählen.*

Beispiel 1.1.19. Es gibt genau $\binom{4}{2} = \frac{4\cdot 3}{2\cdot 1} = 6$ Möglichkeiten, aus den vier Buchstaben a, b, c, d zwei auszuwählen, nämlich

$$\begin{array}{lll} a,b & b,c & c,d \\ a,c & b,d & \\ a,d & & \end{array}$$

Beweis. Wir haben n Möglichkeiten, ein erstes Objekt auszuwählen, dann $n-1$ Möglichkeiten, ein zweites Objekt auszuwählen, und so weiter, also insgesamt $n(n-1)\ldots(n-k+1)$ Möglichkeiten, k Objekte *der Reihe nach* auszuwählen. Auf die Reihenfolge, in der wir ausgewählt haben, kommt es uns aber gar nicht an, jeweils genau $k!$ von unseren $n(n-1)\ldots(n-k+1)$ Möglichkeiten führen also nach 1.1.14 zur Auswahl derselben k Objekte. Man bemerke, daß unser Satz auch im Extremfall $k = 0$ noch stimmt, wenn wir ihn geeignet interpretieren: In der Terminologie, die wir gleich einführen werden, besitzt in der Tat jede Menge genau eine nullelementige Teilmenge, nämlich die leere Menge. □

1.1.20. Offensichtlich gilt für alle natürlichen Zahlen n mit $n \geq k$ die Formel

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \binom{n}{n-k}$$

Das folgt einerseits sofort aus der formalen Definition und ist andererseits auch klar nach der oben erklärten Bedeutung der Binomialkoeffizienten: Wenn wir aus n Objekten k Objekte auswählen, so bleiben $n-k$ Objekte übrig. Es gibt demnach gleichviele Möglichkeiten, k Objekte auszuwählen, wie es Möglichkeiten gibt, $n-k$ Objekte auszuwählen. Wir haben weiter $\binom{n}{n} = \binom{n}{0} = 1$ für jede natürliche Zahl $n \geq 0$ sowie $\binom{n}{1} = \binom{n}{n-1} = n$ für jede natürliche Zahl $n \geq 1$.

Definition 1.1.21. Wie in der Schule setzen wir $a^k := \prod_{i=1}^{k} a$, in Worten ist also gemeint "das Produkt von k-mal dem Faktor a", und verstehen im Lichte von 1.1.13 insbesondere $a^0 = 1$.

Satz 1.1.22. *Für jede natürliche Zahl n gilt die* **binomische Formel**

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

1.1.23. Man beachte, wie wichtig unsere Konvention $a^0 = 1$ und insbesondere auch $0^0 = 1$ für die Gültigkeit dieser Formel ist.

1.1.24. Die Bezeichung "binomische Formel" leitet sich ab von der Vorsilbe "bi" für Zwei, wie etwa in englisch "bicycle" für "Zweirad" alias "Fahrrad", und dem lateinischen Wort "nomen" für "Namen". Mit den beiden "Namen" sind hier a und b gemeint. Mehr dazu wird in **??** erklärt.

Erster Beweis. Beim Ausmultiplizieren erhalten wir so oft $a^k b^{n-k}$, wie es Möglichkeiten gibt, aus unseren n Faktoren $(a+b)$ die k Faktoren auszusuchen, "in denen wir beim Ausmultiplizieren das b nehmen". Dieses Argument werden wir in 2.1.19 noch besser formulieren. □

Zweiter Beweis. Dieser Beweis ist eine ausgezeichnete Übung im Umgang mit unseren Symbolen und mit der vollständigen Induktion. Er scheint mir jedoch auch in einer für Beweise durch vollständige Induktion typischen Weise undurchsichtig. Zunächst prüfen wir für beliebiges n und jede natürliche Zahl $k \geq 1$ die Formel

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$$

durch explizites Nachrechnen. Dann geben wir unserer Formel im Satz den Namen $A(n)$ und prüfen die Formel $A(0)$ und zur Sicherheit auch noch $A(1)$ durch Hinsehen. Schließlich gilt es, den Induktionsschritt durchzuführen, als da heißt,

$A(n+1)$ aus $A(n)$ zu folgern. Dazu rechnen wir

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n \\
&\quad \text{und mit der Induktionsvoraussetzung} \\
&= (a+b)\textstyle\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k} \\
&\quad \text{und durch Ausmultiplizieren} \\
&= \textstyle\sum_{k=0}^{n}\binom{n}{k}a^{k+1}b^{n-k} + \sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k+1} \\
&\quad \text{und Indexwechsel } k = i-1 \text{ in der ersten Summe} \\
&= \textstyle\sum_{i=1}^{n+1}\binom{n}{i-1}a^i b^{n-i+1} + \sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k+1} \\
&\quad \text{dann mit } k \text{ statt } i \text{ und Absondern von Summanden} \\
&= a^{n+1}b^0 + \textstyle\sum_{k=1}^{n}\binom{n}{k-1}a^k b^{n-k+1} + \\
&\qquad + \textstyle\sum_{k=1}^{n}\binom{n}{k}a^k b^{n-k+1} + a^0 b^{n+1} \\
&\quad \text{und nach Zusammenfassen der mittleren Summen} \\
&= a^{n+1}b^0 + \textstyle\sum_{k=1}^{n}\binom{n+1}{k}a^k b^{n-k+1} + a^0 b^{n+1} \\
&\quad \text{und Einbeziehen der abgesonderten Summanden} \\
&= \textstyle\sum_{k=0}^{n+1}\binom{n+1}{k}a^k b^{n+1-k}
\end{aligned}$$

und folgern so tatsächlich $A(n+1)$ aus $A(n)$. □

1.1.25. Die Formel $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$ für $k \geq 1$ kann man zur effektiven Berechnung der Binomialkoeffizienten mit dem sogenannten **Pascal'schen Dreieck** benutzen: Im Schema

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 &
\end{array}$$

seien die Einsen an den Rändern vorgegeben und eine Zahl in der Mitte berechne sich als die Summe ihrer beiden oberen "Nachbarn". Dann stehen in der $(n+1)$-ten Zeile der Reihe nach die Binomialkoeffizienten $\binom{n}{0} = 1, \binom{n}{1} = n, \ldots$ bis $\binom{n}{n-1} = n, \binom{n}{n} = 1$. Wir haben also zum Beispiel

$$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$$

Übung 1.1.26. Man finde und beweise eine Formel für $\sum_{i=1}^{n} i^2$. Hinweis: Man suche zunächst eine Formel für $\sum_{i=1}^{n} i^3 - (i-1)^3$ und beachte $i^3 - (i-1)^3 = 3i^2 - 3i + 1$.

1.2 Fibonacci-Folge und Vektorraumbegriff

Beispiel 1.2.1. Die **Fibonacci-Folge**

$$0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ldots$$

entsteht, indem man mit $f_0 = 0$ und $f_1 = 1$ beginnt und dann jedes weitere Folgenglied als die Summe seiner beiden Vorgänger bildet. Wir suchen nun für die Glieder f_i dieser Folge eine geschlossene Darstellung. Dazu vereinbaren wir, daß wir Folgen $x_0, x_1, x_2, \ldots$ mit der Eigenschaft $x_n = x_{n-1}+x_{n-2}$ für $n = 2, 3, 4, \ldots$ **Folgen vom Fibonacci-Typ** nennen wollen. Kennen wir die beiden ersten Glieder einer Folge vom Fibonacci-Typ, so liegt natürlich bereits die gesamte Folge fest. Nun bemerken wir, daß für jede Folge $x_0, x_1, x_2, \ldots$ vom Fibonacci-Typ und jedes α auch die Folge $\alpha x_0, \alpha x_1, \alpha x_2, \ldots$ vom Fibonacci-Typ ist, und daß für jede weitere Folge $y_0, y_1, y_2, \ldots$ vom Fibonacci-Typ auch die gliedweise Summe $(x_0 + y_0), (x_1 + y_1), (x_2 + y_2), \ldots$ eine Folge vom Fibonacci-Typ ist. Der Trick ist dann, danach zu fragen, für welche β die Folge $x_i = \beta^i$ vom Fibonacci-Typ ist. Das ist ja offensichtlich genau dann der Fall, wenn gilt $\beta^2 = \beta + 1$, als da heißt für $\beta_\pm = \frac{1}{2}(1 \pm \sqrt{5})$. Für beliebige c, d ist mithin die Folge

$$x_i = c\beta_+^i + d\beta_-^i$$

vom Fibonacci-Typ, und wenn wir c und d bestimmen mit $x_0 = 0$ und $x_1 = 1$, so ergibt sich eine explizite Darstellung unserer Fibonacci-Folge. Wir suchen also c und d mit

$$\begin{array}{rcl} 0 & = & c + d \\ 1 & = & c\left(\frac{1}{2}(1+\sqrt{5})\right) + d\left(\frac{1}{2}(1-\sqrt{5})\right) \end{array}$$

und folgern leicht $c = -d$ und $1 = c\sqrt{5}$ alias $c = 1/\sqrt{5} = -d$. Damit ergibt sich schließlich für unsere ursprüngliche Fibonacci-Folge die explizite Darstellung

$$f_i = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^i - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^i$$

Im übrigen ist der zweite Summand hier immer kleiner als $1/2$, so daß wir f_i auch beschreiben können als diejenige ganze Zahl, die am nächstem am ersten Summanden liegt. Es wäre rückblickend natürlich ein Leichtes gewesen, diese Formel einfach zu "raten" um sie dann mit vollständiger Induktion 1.1.1 zu beweisen. Diese Art mathematischer Zaubertricks halte ich jedoch für unehrenhaft. Ich werde deshalb stets nach Kräften versuchen, das Tricksen zu vermeiden, auch wenn die Beweise dadurch manchmal etwas länger werden sollten. Eine Möglichkeit, auch den letzten verbleibenden Trick aus den vorhergehenden Überlegungen zu eliminieren, zeigt II.2.8.17. Die bei unserer Lösung auftretende reelle Zahl

$\frac{1}{2}(1+\sqrt{5})$ ist im Übrigen auch bekannt als "goldener Schnitt" aus Gründen, die in nebenstehendem Bild diskutiert werden. In **??** dürfen Sie dann zur Übung zeigen, daß der Quotient zweier aufeinanderfolgender Fibonacci-Zahlen gegen den goldenen Schnitt strebt, daß also genauer und in Formeln für unsere Fibonacci-Folge $f_0, f_1, f_2, \ldots$ von oben gilt

$$\lim_{i\to\infty} \frac{f_{i+1}}{f_i} = \frac{1+\sqrt{5}}{2}$$

Übung 1.2.2. Kann man für jede Folge $x_0, x_1, \ldots$ vom Fibonacci-Typ Zahlen c, d finden mit $x_i = c\beta_+^i + d\beta_-^i$ für alle i? Finden Sie eine geschlossene Darstellung für die Glieder der Folge, die mit $0, 0, 1$ beginnt und dem Bildungsgesetz $x_n = 2x_{n-1} + x_{n-2} - 2x_{n-3}$ gehorcht.

Beispiel 1.2.3. Ein System von mehreren Gleichungen, in denen dieselben Unbekannten auftauchen, nennt man auch ein **Gleichungssystem**. Wir betrachten ein "homogenes lineares" Gleichungssystem alias ein Gleichungssystem der Gestalt

$$\begin{array}{rcl} \alpha_{11}x_1 + \alpha_{12}x_2 + \ldots + \alpha_{1m}x_m &=& 0 \\ \alpha_{21}x_1 + \alpha_{22}x_2 + \ldots + \alpha_{2m}x_m &=& 0 \\ \vdots & & \\ \alpha_{n1}x_1 + \alpha_{n2}x_2 + \ldots + \alpha_{nm}x_m &=& 0 \end{array}$$

Wie man zu vorgegebenen $\alpha_{i,j}$ für $1 \le i \le n$ und $1 \le j \le m$ die Menge L aller Lösungen $(x_1, \ldots, x_m)$ ermittelt, sollen sie später in dieser Vorlesung lernen. Zwei Dinge aber sind a priori klar:

1. Sind $(x_1, \ldots, x_m)$ und $(x'_1, \ldots, x'_m)$ Lösungen, so ist auch ihre komponentenweise Summe $(x_1 + x'_1, \ldots, x_m + x'_m)$ eine Lösung;
2. Ist $(x_1, \ldots, x_m)$ eine Lösung und α eine reelle Zahl, so ist auch das komponentenweise Produkt $(\alpha x_1, \ldots, \alpha x_m)$ eine Lösung.

Beispiel 1.2.4. Wir betrachten die Menge aller Funktionen $f : \mathbb{R} \to \mathbb{R}$, die zweimal differenzierbar sind und der Differentialgleichung

$$f'' = -f$$

genügen. Lösungen sind zum Beispiel die Funktionen $\sin, \cos,$ die Nullfunktion oder auch die Funktionen $f(x) = \sin(x+a)$ für konstantes a. Wie man die Menge L aller Lösungen beschreiben kann, sollen Sie nicht hier lernen. Zwei Dinge aber sind a priori klar:

1. Mit f und g ist auch die Funktion $f + g$ eine Lösung;

Der **goldene Schnitt** ist das Verhältnis, in dem eine Strecke geteilt werden muß, damit das Verhältnis vom größeren zum kleineren Stück gleich dem Verhältnis des Ganzen zum größeren Stück ist, also die positive Lösung der Gleichung $a/1 = (1+a)/a$ alias $a^2 - a - 1 = 0$, also $a = (1+\sqrt{5})/2$.

2. Ist f eine Lösung und α eine reelle Zahl, so ist auch αf eine Lösung.

Beispiel 1.2.5. Wir betrachten die Gesamtheit aller Parallelverschiebungen der Tafelebene. Graphisch stellen wir solch eine Parallelverschiebung dar durch einen Pfeil von irgendeinem Punkt zu seinem Bild unter der Verschiebung. Im nebenstehenden Bild stellen etwa alle gepunktelten Pfeile dieselbe Parallelverschiebung dar. Was für ein Ding diese Gesamtheit P aller Parallelverschiebungen eigentlich ist, scheint mir recht undurchsichtig, aber einiges ist a priori klar:

1. Sind p und q Parallelverschiebungen, so ist auch ihre "Hintereinanderausführung" $p \circ q$, sprich "p nach q", eine Parallelverschiebung.

2. Ist α eine reelle Zahl und p eine Parallelverschiebung, so können wir eine neue Parallelverschiebung αp bilden, das "α-fache von p". Bei negativen Vielfachen vereinbaren wir hierzu, daß eine entsprechende Verschiebung in die Gegenrichtung gemeint ist.

3. Führen wir eine neue Notation ein und schreiben für die Hintereinanderausführung $p \dot{+} q := p \circ q$, so gelten für beliebige Parallelverschiebungen p, q, r der Tafelebene und beliebige reelle Zahlen α, β die Formeln

$$\begin{array}{rcl} (p \dot{+} q) \dot{+} r & = & p \dot{+} (q \dot{+} r) \\ p \dot{+} q & = & q \dot{+} p \\ \alpha(\beta p) & = & (\alpha\beta)p \\ (\alpha + \beta)p & = & (\alpha p) \dot{+} (\beta p) \\ \alpha(p \dot{+} q) & = & (\alpha p) \dot{+} (\alpha q) \end{array}$$

Will man sich die Gesamtheit aller Parallelverschiebungen der Tafelebene anschaulich machen, so tut man im Übrigen gut daran, einen Punkt als "Ursprung" auszuzeichnen und jede Parallelverschiebung mit dem Punkt der Tafelebene zu identifizieren, auf den unsere Parallelverschiebung diesen Ursprung abbildet.

Beispiel 1.2.6. Analoges gilt für die Gesamtheit der Parallelverschiebung des Raums unserer Anschauung und auch für die Gesamtheit aller Verschiebungen einer Geraden und, mit noch mehr Mut, für die Gesamtheit aller Zeitspannen.

1.2.7. Die Formeln unserer kleinen Formelsammlung von 1.2.5.3 gelten ganz genauso auch für die Lösungsmenge unserer Differentialgleichung $f'' = -f$, wenn wir $f \dot{+} g := f + g$ verstehen, für die Lösungsmenge unseres linearen Gleichungssystems, wenn wir

$$(x_1, \ldots, x_m) \dot{+} (x'_1, \ldots, x'_m) := (x_1 + x'_1, \ldots, x_m + x'_m)$$

Die Hintereinanderausführung der beiden Parallelverschiebungen der Tafel- oder hier vielmehr der Papierebene, die durch die durchgezogenen Pfeile dargestellt werden, wird die durch die gepunktelten Feile dargestellt.

als “komponentenweise Addition” verstehen, und für die Menge aller Folgen vom Fibonacci-Typ, wenn wir ähnlich die Summe $\dotplus$ zweier Folgen erklären. Ein wesentliches Ziel der folgenden Vorlesungen über lineare Algebra ist es, einen abstrakten Formalismus aufzubauen, dem sich alle diese Beispiele unterordnen. Dadurch soll zweierlei erreicht werden:

1. Unser abstrakter Formalismus soll uns dazu verhelfen, die uns als Augentieren und Nachkommen von Ästehüpfern angeborene räumliche Anschauung nutzbar zu machen zum Verständnis der bis jetzt gegebenen Beispiele und der vielen weiteren Beispiele von Vektorräumen, denen Sie im Verlauf Ihres Studiums noch begegnen werden. So werden sie etwa lernen, daß man sich die Menge aller Folgen vom Fibonacci-Typ durchaus als Ebene vorstellen darf und die Menge aller Folgen mit vorgegebenem Folgenglied an einer vorgegebenen Stelle als eine Gerade in dieser Ebene. Suchen wir also alle Folgen vom Fibonacci-Typ mit zwei vorgegebenen Folgengliedern, so werden wir im allgemeinen genau eine derartige Lösung finden, da sich eben zwei Geraden aus einer Ebene im allgemeinen in genau einem Punkt schneiden. In diesem Licht betrachtet soll der abstrakte Formalismus uns also helfen, a priori unanschauliche Fragestellungen der Anschauung zugänglich zu machen. Ich denke, diese Nähe zur Anschauung ist auch der Grund dafür, daß die lineare Algebra meist an den Anfang des Studiums gestellt wird: Von der Schwierigkeit des Formalismus her gesehen gehört sie nämlich keineswegs zu den einfachsten Gebieten der Mathematik, hier würde ich eher an Gruppentheorie oder Graphentheorie oder dergleichen denken.

2. Unser abstrakter Formalismus soll so unmißverständlich sein und seine Spielregeln so klar, daß Sie in die Lage versetzt werden, alles nachzuvollziehen und mir im Prinzip und vermutlich auch in der Realität Fehler nachzuweisen. Schwammige Begriffe wie “Tafelebene” oder “Parallelverschiebung des Raums” haben in einem solchen Formalismus keinen Platz mehr. In diesem Licht betrachtet verfolgen wir mit dem Aufbau des abstrakten Formalismus auch das Ziel einer großen Vereinfachung durch die Reduktion auf die Beschreibung einiger weniger Aspekte der uns umgebenden in ihrer Komplexität kaum präzise faßbaren Wirklichkeit.

Die lineare Algebra hat in meinen Augen drei wesentliche Aspekte: Einen **geometrischen Aspekt**, wie ihn das Beispiel 1.2.5 der Gesamtheit aller Parallelverschiebungen illustriert; einen **algorithmischen Aspekt**, unter den ich das Beispiel 1.2.3 der Lösungsmenge eines linearen Gleichungssystems und insbesondere explizite Verfahren zur Bestimmung dieser Lösungsmenge einordnen würde; und einen **abstrakt-algebraischen Aspekt**, eine Art gedankliches Skelett, das Algorithmik und Geometrie verbindet und Brücken zu vielen weiteren Anwendungen schafft, die man dann auch als das Fleisch auf diesem Gerippe ansehen mag. Ich will im weiteren Verlauf dieser Vorlesungen zur linearen Algebra versuchen, die-

se drei Aspekte zu einer Einheit zu fügen. Ich hoffe, daß Sie dadurch in die Lage versetzt werden, eine Vielzahl von Problemen mit den verbundenen Kräften Ihrer räumlichen Anschauung, Ihrer algorithmischen Rechenfähigkeiten und Ihres abstrakt-logischen Denkens anzugehen. Als Motivation für den weiteren Fortgang der Vorlesungen über lineare Algebra beschreibe ich nun das "Rückgrat unseres Skeletts" und formuliere ohne Rücksicht auf noch unbekannte Begriffe und Notationen die abstrakte Definition eines reellen Vektorraums.

Definition 1.2.8. Ein **reeller Vektorraum** ist ein Tripel bestehend aus den folgenden drei Dingen:

1. Einer Menge V;

2. Einer Verknüpfung $V \times V \to V$, $(v, w) \mapsto v \dot{+} w$, die V zu einer abelschen Gruppe macht;

3. Einer Abbildung $\mathbb{R} \times V \to V$, $(\alpha, v) \mapsto \alpha v$,

derart, daß für alle $\alpha, \beta \in \mathbb{R}$ und alle $v, w \in V$ gilt:

$$\begin{array}{rcl} \alpha(\beta v) & = & (\alpha\beta)v \\ (\alpha + \beta)v & = & (\alpha v) \dot{+} (\beta v) \\ \alpha(v \dot{+} w) & = & (\alpha v) \dot{+} (\alpha w) \\ 1v & = & v \end{array}$$

Hier ist nun viel zu klären: Was ist eine Menge? Eine Verknüpfung? Eine abelsche Gruppe? Eine Abbildung? Was bedeuten die Symbole $\times$, $\to$, $\mapsto$, $\in$, $\mathbb{R}$? Wir beginnen in der nächsten Vorlesung mit der Klärung dieser Begriffe und Notationen.

1.2.9. Bereits hier will ich jedoch die Symbole α und β erklären: Sie heißen "Alpha" und "Beta" und sind die beiden ersten Buchstaben des griechischen Alphabets, das ja auch nach ihnen benannt ist. Bei der Darstellung von Mathematik hilft es, viele verschiedene Symbole und Symbolfamilien zur Verfügung zu haben. Insbesondere werden die griechischen Buchstaben oft und gerne verwendet. Ich schreibe deshalb hier zum Nachschlagen einmal das griechische Alphabet auf. In der ersten Spalte stehen der Reihe nach die griechischen Kleinbuchstaben, dahinter die zugehörigen Großbuchstaben, dann ihr lateinisches Analogon soweit vorhanden, und schließlich, wie man diesen griechischen Buchstaben auf Deutsch

benennt und spricht.

α	A	a	alpha
β	B	b	beta
γ	Γ	g	gamma
δ	Δ	d	delta
ϵ, ε	E	e	epsilon
ζ	Z	z	zeta
η	H	ä	eta
θ, ϑ	Θ	th	theta
ι	I	i	iota
κ	K	k	kappa
λ	Λ	l	lambda
μ	M	m	my, sprich “mü”
ν	N	n	ny, sprich “nü”
ξ	Ξ	x	xi
o	O	o	omikron
π	Π	p	pi
ρ, ϱ	P	r	rho
σ, ς	Σ	s	sigma
τ	T	t	tau
υ	Υ	y	ypsilon
ϕ, φ	Φ	f	phi
χ	X	ch	chi
ψ	Ψ	ps	psi
ω	Ω	oh	omega

2 Naive Mengenlehre und Kombinatorik

2.1 Mengen

2.1.1. Beim Arbeiten mit reellen Zahlen oder räumlichen Gebilden reicht auf der Schule ein intuitives Verständnis meist aus, und wenn die Intuition in die Irre führt, ist ein Lehrer zur Stelle. Wenn Sie jedoch selbst unterrichten oder etwas beweisen wollen, reicht dieses intuitive Verständnis nicht mehr aus. *Im folgenden werden deshalb zunächst der Begriff der reellen Zahlen und der Begriff des Raums zurückgeführt auf Grundbegriffe der Mengenlehre, den Begriff der rationalen Zahlen und elementare Logik.* Bei der Arbeit mit diesen Begriffen führt uns die Intuition nicht so leicht in die Irre, wir geben uns deshalb mit einem intuitiven Verständnis zufrieden und verweisen jeden, der es noch genauer wissen will, auf eine Vorlesung über Logik. Wir beginnen mit etwas naiver Mengenlehre, wie sie von Georg Cantor in den Jahren 1874-1897 begründet wurde, und von der der berühmte Mathematiker David Hilbert einmal sagte: "Aus dem Paradies, das Cantor uns geschaffen, soll uns niemand vertreiben können". Natürlich gab es auch vor der Mengenlehre schon hoch entwickelte Mathematik, bei Carl Friedrich Gauß Tod 1855 gab es diese Theorie noch gar nicht und Fourier fand seine "Fourierentwicklung" sogar bereits zu Beginn des 19.-ten Jahrhunderts. Er behauptete auch gleich in seiner "Théorie analytique de la chaleur", daß sich jede beliebige periodische Funktion durch eine Fouriereihe darstellen lasse, aber diese Behauptung stieß bei anderen berühmten Mathematikern seiner Zeit auf Ablehnung und es entstand darüber ein heftiger Disput. Erst in besagtem "Paradies der Mengenlehre" konnten die Fourier's Behauptung zugrundeliegenden Begriffe soweit geklärt werden, daß dieser Disput nun endgültig beigelegt ist. Ähnlich verhält es sich auch mit vielen anderen Fragestellungen. Da die Mengenlehre darüber hinaus auch vom didaktischen Standpunkt aus eine äußerst klare und durchsichtige Darstellung mathematischer Sachverhalte ermöglicht, hat sie sich als Grundlage der höheren Mathematik und der Ausbildung von Mathematikern an Universitäten schnell durchgesetzt und ist nun weltweit ein wesentlicher Teil des "Alphabets der Sprache der Mathematiker". Man wird an Universitäten sogar geradezu dazu erzogen, geometrischen Argumenten keine Beweiskraft zuzugestehen, und ich halte das bei der Ausbildung von Mathematikern auch für angemessen. Bei der Mathematik-Ausbildung im allgemeinen scheint mir dieses Vorgehen dahingegen nicht zielführend: In diesem Kontext sollte man meines Erachtens nicht mit demselben Maß messen, auch ohne alle Mengenlehre geometrisch erklärte Begriffe wie Gerade und Kreis, Ebene und Raum, als wohldefinierte Objekte der Mathematik zulassen, und geometrischen Argumenten durchaus Beweiskraft zugestehen.

2.1.2. Im Wortlaut der ersten Zeilen des Artikels "Beiträge zur Begründung der

transfiniten Mengenlehre (Erster Aufsatz)" von Georg Cantor, erschienen im Jahre 1895, hört sich die Definition einer Menge so an:

> Unter einer **Menge** verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objecten m unserer Anschauung oder unseres Denkens (welche die **Elemente** von M genannt werden) zu einem Ganzen.

Verbinden wir mit einer Menge eine geometrische Vorstellung, so nennen wir ihre Elemente auch **Punkte** und die Menge selbst einen **Raum**. Ein derartiges Herumgerede ist natürlich keine formale Definition und birgt auch verschiedene Fallstricke, vergleiche 2.1.21. Das Ziel dieser Vorlesung ist aber auch nicht eine formale Begründung der Mengenlehre, wie Sie sie später in der Logik kennenlernen können. Sie sollen vielmehr die Bedeutung dieser Worte intuitiv erfassen wie ein Kleinkind, das Sprechen lernt: Indem sie mir und anderen Mathematikern zuhören, wie wir mit diesen Worten sinnvolle Sätze bilden, uns nachahmen, und beobachten, welchen Effekt Sie damit hervorrufen. Unter anderem dazu sind die Übungsgruppen da.

Beispiele 2.1.3. Endliche Mengen gibt man oft durch eine vollständige Liste ihrer Elemente in geschweiften Klammern an, zum Beispiel in der Form $X = \{x_1, x_2, \ldots, x_n\}$. Diese geschweiften Klammern heißen auch **Mengenklammern**. Die Elemente dürfen mehrfach genannt werden und es kommt nicht auf die Reihenfolge an, in der sie genannt werden. So haben wir also $\{1, 1, 2\} = \{2, 1\}$. Die Aussage "x ist Element von X" wird mit $x \in X$ abgekürzt, ihre Verneinung "x ist nicht Element von X" mit $x \notin X$. Es gibt auch die sogenannte **leere Menge** $\emptyset = \{\ \}$, die gar kein Element enthält. Andere Beispiele sind die Menge der **natürlichen Zahlen** $\mathbb{N} = \{0, 1, 2, \ldots\}$, die Menge der **ganzen Zahlen** $\mathbb{Z} = \{0, 1, -1, 2, -2, \ldots\}$ und die Menge der **rationalen Zahlen** $\mathbb{Q} = \{p/q \mid p, q \in \mathbb{Z},\ q \neq 0\}$. Deren Name kommt von lateinisch "ratio" für "Verhältnis". Man beachte, daß wir auch hier Elemente mehrfach genannt haben, es gilt ja $p/q = p'/q'$ genau dann, wenn $pq' = p'q$. Auf deutsch bezeichnet man die rationalen Zahlen manchmal auch als **Bruchzahlen**.

Ergänzung 2.1.4. Das Gleichheitszeichen $=$ scheint auf ein 1557 von Robert Recorde publiziertes Buch zurückzugehen und soll andeuten, daß das, was auf der linken und rechten Seite dieses Zeichens steht, so gleich ist wie die beiden Strichlein, die das uns heute so selbstverständliche Gleichheitszeichen bilden. Davor schrieb man statt einem Gleichheitszeichen meist ae für "äquivalent".

2.1.5. In Texten, in deren Konventionen die Null keine natürliche Zahl ist, verwendet man meist die abweichenden Notationen $\mathbb{N}$ für die Menge $\{1, 2, \ldots\}$ und $\mathbb{N}_0$ für die Menge $\{0, 1, 2, \ldots\}$. Die in diesem Text verwendete Notation $\mathbb{N} = \{0, 1, 2, \ldots\}$ stimmt mit der internationalen Norm ISO 31-11 überein.

Definition 2.1.6. Eine Menge Y heißt **Teilmenge** einer Menge X genau dann, wenn jedes Element von Y auch ein Element von X ist. Man schreibt dafür $Y \subset X$ oder $X \supset Y$. Zum Beispiel gilt stets $\emptyset \subset X$, und $\{x\} \subset X$ ist gleichbedeutend zu $x \in X$. Zwei Teilmengen einer gegebenen Menge, die kein gemeinsames Element haben, heißen **disjunkt**.

Bemerkung 2.1.7. Unsere Notation $\subset$ weicht ab von der internationalen Norm ISO 31-11, die statt unserem $\subset$ das Symbol $\subseteq$ vorschlägt. In den Konventionen ISO 31-11 hat das Symbol $\subset$ abweichend die Bedeutung einer **echten**, d.h. von der ganzen Menge verschiedenen Teilmenge, für die wir hinwiederum die Bezeichnung $\subsetneq$ verwenden werden. Meine Motivation für diese Abweichung ist, daß das Symbol für beliebige Teilmengen sehr häufig und das für echte Teilmengen nur sehr selten vorkommt. Die hier verwendete Notation ist auch weit verbreitet und schon sehr viel länger in Gebrauch, das Symbol $\subseteq$ ist eine vergleichsweise neue Konvention. Ich komme muß jedoch zugeben, daß die hier gewählte Notation mit den üblichen und auch in diesem Text verwendeten Notationen $<$ und $\leq$ nicht gut zusammenpaßt.

Definition 2.1.8. Wir vereinbaren, daß wir die leere Menge endlich nennen wollen, damit jede Teilmenge einer endlichen Menge auch wieder endlich ist. Die Zahl der Elemente einer endlichen Menge X nennen wir ihre **Kardinalität** oder **Mächtigkeit** und notieren sie $|X|$ oder $\operatorname{card}(X)$. In der Literatur findet man auch die Notation $\sharp X$. Ist X unendlich, so schreiben wir kurz $|X| = \infty$ und ignorieren in unserer Notation, daß auch unendliche Mengen "verschieden groß" sein können, für ein Beispiel siehe **??** und für eine genauere Diskussion des Begriffs der Kardinalität **??**. Für endliche Mengen X ist demnach ihre Kardinalität stets eine natürliche Zahl $|X| \in \mathbb{N}$ und $|X| = 0$ ist gleichbedeutend zu $X = \emptyset$.

Definition 2.1.9. Oft bildet man neue Mengen als Teilmengen bestehender Mengen und schreibt $Y = \{x \in X \mid x \text{ hat eine gewisse Eigenschaft}\}$. Zum Beispiel gilt $\mathbb{N} = \{a \in \mathbb{Z} \mid a \geq 0\}$ oder $\{0,1\} = \{a \in \mathbb{N} \mid a^2 = a\}$.

2.1.10. Bereits an dieser Stelle ist unsere Notation nicht eindeutig: Ich wollte mit $\{0,1\}$ die zweielementige Menge mit den beiden Elementen Null und Eins andeuten, das könnte jedoch auch als die Menge mit der Dezimalzahl $0,1$ als einzigem Element interpretiert werden. Es wird noch oft vorkommen, daß sich die Bedeutung einer Formel erst aus dem Kontext erschließt. Im folgenden werden Kommas fast nie als Kommas einer Dezimalzahl zu verstehen sein.

Definition 2.1.11. Es ist auch erlaubt, die "Menge aller Teilmengen" einer gegebenen Menge X zu bilden. Sie heißt die **Potenzmenge** von X und wird mit $\mathcal{P}(X)$ bezeichnet.

2.1.12. Ist X eine endliche Menge, so ist auch ihre Potenzmenge endlich und es gilt $|\mathcal{P}(X)| = 2^{|X|}$. Für die drei-elementige Menge $X = \{1, 2, 3\}$ besteht zum Beispiel $\mathcal{P}(X)$ aus $2^3 = 8$ Elementen, genauer gilt

$$\mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

Definition 2.1.13. Gegeben zwei Mengen X, Y können wir auf verschiedene Arten neue Mengen bilden:

1. Die **Vereinigung** $X \cup Y := \{z \mid z \in X \text{ oder } z \in Y\}$, zum Beispiel ist $\{1, 2\} \cup \{2, 3\} = \{1, 2, 3\}$.

2. Den **Schnitt** $X \cap Y := \{z \mid z \in X \text{ und } z \in Y\}$, zum Beispiel ist $\{1, 2\} \cap \{2, 3\} = \{2\}$. Zwei Mengen sind also disjunkt genau dann, wenn ihr Schnitt die leere Menge ist.

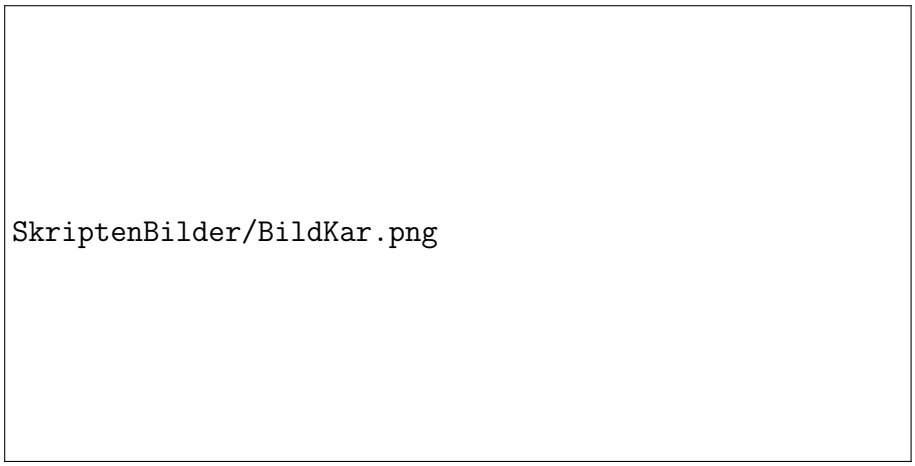
3. Die **Differenz** $X \backslash Y := \{z \in X \mid z \notin Y\}$, zum Beispiel haben wir $\{1, 2\} \backslash \{2, 3\} = \{1\}$. Man schreibt statt $X \backslash Y$ auch $X - Y$. Ist Y eine Teilmenge von X, so heißt $X \backslash Y$ das **Komplement** von Y in X.

4. Das **kartesische Produkt** $X \times Y := \{(x, y) \mid x \in X,\ y \in Y\}$, als da heißt die Menge aller geordneten Paare. Es gilt also $(x, y) = (x', y')$ genau dann, wenn gilt $x = x'$ und $y = y'$. Zum Beispiel haben wir $\{1, 2\} \times \{1, 2, 3\} = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3)\}$. Oft benutzt man für das kartesische Produkt $X \times X$ einer Menge X mit sich selbst die Abkürzung $X \times X = X^2$.

2.1.14. Wir werden in unserer naiven Mengenlehre die ersten drei Operationen nur auf Teilmengen einer gemeinsamen Obermenge anwenden, die uns in der einen oder anderen Weise bereits zur Verfügung steht. Die Potenzmenge und das kartesische Produkt dahingegen benutzen wir, um darüber hinaus neue Mengen zu erschaffen. Diese Konstruktionen erlauben es, im Rahmen der Mengenlehre so etwas wie Abstraktionen zu bilden: Wenn wir uns etwa die Menge T aller an mindestens einem Tag der Weltgeschichte lebenden oder gelebt habenden Tiere als eine Menge im Cantor'schen Sinne denken, so würden wir Konzepte wie "männlich" oder "Hund" oder "Fleischfresser" formal als Teilmengen dieser Menge definieren, d.h. als Elemente von $\mathcal{P}(T)$, und das Konzept "ist Kind von" als eine Teilmenge des kartesischen Produkts dieser Menge T mit sich selbst, also als ein Element von $\mathcal{P}(T \times T)$.

Eine gute Anschauung für die ersten drei Operationen liefern die sogenannten **van-de-Ven-Diagramme** wie sie die obenstehenden Bilder zeigen. Sie sind allerdings nicht zu genau zu hinterfragen, denn ob die Punkte auf einem Blatt Papier im Sinne von Cantor "bestimmte wohlunterschiedene Objekte unserer Anschauung" sind, scheint mir sehr fraglich. Wenn man jedoch jedes der schraffierten Gebiete im Bild auffasst als die Menge aller darin liegenden Kreuzungspunkte auf einem dazugedachten Millimeterpapier und keine dieser Kreuzungspunkte auf den Begrenzungslinien liegen, so können sie wohl schon als eine Menge im Cantor'schen Sinne angesehen werden.

Anschauliche Darstellung des Produkts einer Menge mit fünf und einer Menge mit drei Elementen. Hier wird ein Paar (x, y) dargestellt durch einen fetten Punkt, der über x und neben y liegt.



Dies Bild muß anders interpretiert werden als das Vorherige. Die Mengen X und Y sind nun zu verstehen als die Mengen der Punkte der vertikalen und horizontalen Geradensegmente und ein Punkt des Quadrats meint das Element $(x, y) \in X \times Y$, das in derselben Höhe wie $y \in Y$ senkrecht über $x \in X$ liegt.

2.1.15. Für das Rechnen mit Mengen überlegt man sich die folgenden Regeln:

$$\begin{aligned} X \cap (Y \cap Z) &= (X \cap Y) \cap Z \\ X \cup (Y \cup Z) &= (X \cup Y) \cup Z \\ X \cup (Y \cap Z) &= (X \cup Y) \cap (X \cup Z) \\ X \cap (Y \cup Z) &= (X \cap Y) \cup (X \cap Z) \\ X \backslash (Y \cup Z) &= (X \backslash Y) \cap (X \backslash Z) \\ X \backslash (Y \cap Z) &= (X \backslash Y) \cup (X \backslash Z) \\ X \backslash (X \backslash Y) &= X \cap Y \end{aligned}$$

Eine gute Anschauung für diese Regeln liefern die van-de-Ven-Diagramme, wie sie die nebenstehenden Bilder zeigen. Die vorletzte und vorvorletzte Gleichung faßt man auch unter der Bezeichnung **de Morgan'sche Regeln** zusammen.

Übung 2.1.16. Sind X und Y endliche Mengen, so gilt für die Kardinalitäten $|X \times Y| = |X| \cdot |Y|$ und $|X \cup Y| = |X \backslash Y| + |X \cap Y| + |Y \backslash X|$.

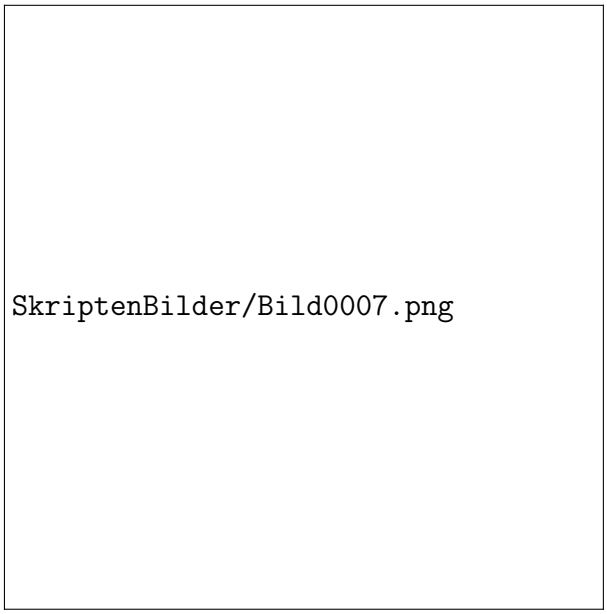
Satz 2.1.17 (Bedeutung der Binomialkoeffizienten). *Gegeben $n, k \in \mathbb{N}$ gibt der Binomialkoeffizient $\binom{n}{k}$ die Zahl der k-elementigen Teilmengen einer n-elementigen Menge an, in Formeln:*

$$|X| = n \quad \textit{impliziert} \quad |\{Y \subset X \mid |Y| = k\}| = \binom{n}{k}$$

Beweis. Vollständige Induktion über n. Für $n = 0$ gilt die Aussage, denn eine nullelementige Menge hat genau eine k-elementige Teilmenge falls $k = 0$ und keine k-elementige Teilmenge falls $k \geq 1$. Nehmen wir nun an, die Aussage sei für ein n schon bewiesen. Eine $(n+1)$-elementige Menge X schreiben wir als $X = M \cup \{x\}$, wo M eine n-elementige Menge ist und $x \notin M$. Ist $k = 0$, so gibt es genau eine k-elementige Teilmenge von $M \cup \{x\}$, nämlich die leere Menge. Ist $k \geq 1$, so gibt es in $M \cup \{x\}$ nach Induktionsannahme genau $\binom{n}{k}$ k-elementige Teilmengen, die x nicht enthalten. Die k-elementigen Teilmengen dahingegen, die x enthalten, ergeben sich durch Hinzunehmen von x aus den $(k-1)$-elementigen Teilmengen von M, von denen es gerade $\binom{n}{k-1}$ gibt. Insgesamt hat $M \cup \{x\}$ damit also genau $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$ k-elementige Teilmengen. □

Bemerkung 2.1.18. Wieder scheint mir dieser Beweis in der für vollständige Induktion typischen Weise undurchsichtig. Ich ziehe deshalb den in 1.1.18 gegebenen weniger formellen Beweis vor. Man kann auch diesen Beweis formalisieren und verstehen als Spezialfall der sogenannten "Bahnformel" II.8.2.2, vergleiche II.8.2.3.

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$$



$$X \setminus (Y \cap Z) = (X \setminus Y) \cup (X \setminus Z)$$

Bemerkung 2.1.19. Wir geben nun die versprochene präzise Formulierung unseres ersten Beweises der binomischen Formel 1.1.22. Wir rechnen dazu

$$(a+b)^n = \sum_{Y \subset \{1,2,\ldots,n\}} a^{|Y|} b^{n-|Y|}$$

wo die rechte Seite in Verallgemeinerung der in Abschnitt 1.1 eingeführten Notation bedeuten soll, daß wir für jede Teilmenge Y von $\{1,2,\ldots,n\}$ den angegebenen Ausdruck $a^{|Y|}b^{n-|Y|}$ nehmen und alle diese Ausdrücke aufsummieren. Dann fassen wir gleiche Summanden zusammen und erhalten mit 2.1.17 die binomische Formel.

Ergänzende Übung 2.1.20. Es gilt $\sum_k \binom{n}{k} = 2^n$.

Ergänzung 2.1.21. Ich will nicht verschweigen, daß der in diesem Abschnitt dargestellte naive Zugang zur Mengenlehre durchaus begriffliche Schwierigkeiten mit sich bringt: Zum Beispiel darf die Gesamtheit $\mathcal{M}$ aller Mengen nicht als Menge angesehen werden, da wir sonst die "Menge aller Mengen, die sich nicht selbst als Element enthalten", gegeben durch die formelhafte Beschreibung $\mathcal{N} = \{A \in \mathcal{M} \mid A \notin A\}$, bilden könnten. Für diese Menge kann aber weder $\mathcal{N} \in \mathcal{N}$ noch $\mathcal{N} \notin \mathcal{N}$ gelten ... Diese Art von Schwierigkeiten kann erst ein formalerer Zugang klären und auflösen, bei dem man unsere naiven Vorstellungen durch Ketten von Zeichen aus einem wohlbestimmten endlichen Alphabet ersetzt und unsere Vorstellung von Wahrheit durch die Verifizierbarkeit vermittels rein algebraischer "erlaubter Manipulationen" solcher Zeichenketten, die in "Axiomen" festgelegt werden. Diese Verifikationen kann man dann durchaus auch einer Rechenmaschine überlassen, so daß wirklich auf "objektivem" Wege entschieden werden kann, ob ein "Beweis" für die "Richtigkeit" einer unserer Zeichenketten in einem vorgegebenen axiomatischen Rahmen stichhaltig ist. Allerdings kann in derartigen Systemen von einer Zeichenkette algorithmisch nur entschieden werden, ob sie eine "sinnvolle Aussage" ist, nicht aber, ob sie "bewiesen" werden kann. Noch viel stärker zeigt der Unvollständigkeitssatz von Gödel, daß es in einem derartigen axiomatischen Rahmen, sobald er reichhaltig genug ist für eine Beschreibung des Rechnens mit natürlichen Zahlen, stets sinnvolle Aussagen gibt derart, daß entweder sowohl die Aussage als auch ihre Verneinung oder aber weder die Aussage noch ihre Verneinung bewiesen werden können. Mit diesen und ähnlichen Fragestellungen beschäftigt sich die Logik.

2.1.22. Um mich nicht dem Vorwurf auszusetzen, während des Spiels die Spielregeln ändern zu wollen, sei bereits hier erwähnt, daß in II.1.2 noch weitere wichtige Konstruktionen der Mengenlehre eingeführt werden, und daß in **??** einige weniger offensichtliche Folgerungen erläutert werden, die meines Erachtens bereits an den Rand dessen gehen, was man in unserem informellen Rahmen als Argumentation noch vertreten kann.

Aus $X = X_1 \cup X_2$ und $Y = Y_1 \cup Y_2$ folgt noch lange nicht
$X \times Y = (X_1 \times Y_1) \cup (X_2 \times Y_2)$

2.2 Abbildungen

Definition 2.2.1. Seien X, Y Mengen. Eine **Abbildung** $f : X \to Y$ ist eine Zuordnung, die jedem Element $x \in X$ genau ein Element $f(x) \in Y$ zuordnet, das **Bild** von x unter f, auch genannt der **Wert** von f an der Stelle x. Man spricht dann auch vom **Auswerten** der Funktion f an der Stelle x oder vom **Einsetzen** von x in f.

2.2.2. Wem das zu vage ist, der mag die alternative Definition vorziehen, nach der eine **Abbildung** $f : X \to Y$ eine Teilmenge $f \subset X \times Y$ ist derart, daß es für jedes $x \in X$ genau ein $y \in Y$ gibt mit $(x, y) \in f$. Dies eindeutig bestimmte y schreiben wir dann $f(x)$ und sind auf einem etwas formaleren Weg wieder am selben Punkt angelangt. In unseren Konventionen nennen wir besagte Teilmenge den **Graphen von** f und notieren sie mit dem Symbol Γ (sprich: Gamma), einem großen griechischen G, und schreiben also

$$\Gamma(f) := \{(x, f(x)) \mid x \in X\} \subset X \times Y$$

Definition 2.2.3. Ist $f : X \to Y$ eine Abbildung, so nennen wir X ihren **Definitionsbereich** und Y ihren **Wertebereich**. Zwei Abbildungen nennen wir gleich genau dann, wenn sie denselben Definitionsbereich X, denselben Wertebereich Y und dieselbe Abbildungsvorschrift $f \subset X \times Y$ haben. Die Menge aller Abbildungen von X nach Y bezeichnen wir mit

$$\mathrm{Ens}(X, Y)$$

nach der französischen Übersetzung **ensemble** des deutschen Begriffs "Menge". Üblich ist auch die Notation Y^X.

Bemerkung 2.2.4. Noch gebräuchlicher ist die Bezeichnung $\mathrm{Abb}(X, Y)$ für die Menge aller Abbildungen von X nach Y. Ich will jedoch sehr viel später die "Kategorie aller Mengen" mit Ens bezeichnen und für je zwei Objekte X, Y einer Kategorie $\mathcal{C}$ die Menge aller "Morphismen" von X nach Y mit $\mathcal{C}(X, Y)$, und das motiviert dann auch erst eigentlich die hier gewählte Bezeichnung für Mengen von Abbildungen.

2.2.5. Wir notieren Abbildungen oft in der Form

$$\begin{array}{rccc} f: & X & \to & Y \\ & x & \mapsto & f(x) \end{array}$$

und in verschiedenen Verkürzungen dieser Notation. Zum Beispiel sprechen wir von "einer Abbildung $X \to Y$" oder "der Abbildung $n \mapsto n^3$ von der Menge der natürlichen Zahlen in sich selber". Wir benutzen unsere zwei Arten von Pfeilen auch im allgemeinen in derselben Weise.

Eine Abbildung einer Menge mit fünf in eine mit drei Elementen

Der Graph der oben angegebenen Abbildung, wobei das X oben mit dem X hier identifiziert wurde durch “Umkippen nach Rechts”

Beispiel 2.2.6. Für jede Menge X haben wir die **identische Abbildung** oder **Identität**

$$\begin{array}{rccc} \mathrm{id} = \mathrm{id}_X : & X & \to & X \\ & x & \mapsto & x \end{array}$$

Ein konkreteres Beispiel für eine Abbildung ist das Quadrieren

$$\begin{array}{rccc} q : & \mathbb{Z} & \to & \mathbb{Z} \\ & n & \mapsto & n^2 \end{array}$$

Beispiel 2.2.7. Gegeben zwei Mengen X, Y erklärt man die sogenannten **Projektionsabbildungen** oder **Projektionen** $\mathrm{pr}_X : X \times Y \to X$ bzw. $\mathrm{pr}_Y : X \times Y \to Y$ durch die Vorschrift $(x, y) \mapsto x$ bzw. $(x, y) \mapsto y$.

Definition 2.2.8. Ist $f : X \to Y$ eine Abbildung und $A \subset X$ eine Teilmenge, so definieren wir ihr **Bild** oder genauer ihre **Bildmenge** $f(A)$, eine Teilmenge von Y, durch

$$f(A) := \{y \in Y \mid \text{Es gibt } x \in A \text{ mit } f(x) = y\}$$

Eine Abbildung, deren Bild aus höchstens einem Element besteht, nennen wir eine **konstante Abbildung**. Eine Abbildung, deren Bild aus genau einem Element besteht, nennen wir eine **einwertige Abbildung**. In anderen Worten ist eine einwertige Abbildung also eine konstante Abbildung mit nichtleerem Definitionsbereich.

Beispiel 2.2.9. Vielfach verwendet man für die Bildmenge auch die abkürzende Notation $f(A) := \{f(x) \mid x \in A\}$. Für unsere Abbildung $q : \mathbb{Z} \to \mathbb{Z}$, $n \mapsto n^2$ von eben könnten wir etwa die Menge aller Quadratzahlen schreiben als

$$q(\mathbb{Z}) = \{a^2 \mid a \in \mathbb{Z}\}$$

Ebenso wäre $\{2a \mid a \in \mathbb{N}\}$ eine mögliche formelmäßige Darstellung der Menge aller geraden natürlichen Zahlen, und $\{ab \mid a, b \in \mathbb{N}, a \geq 2, b \geq 2\}$ wäre eine formelmäßige Darstellung der Menge aller natürlichen Zahlen, die nicht prim und auch nicht Null oder Eins sind.

2.2.10. Gegeben ein festes $c \in Y$ schreiben wir oft auch kurz c für die konstante Abbildung $X \to Y$, $x \mapsto c$ für alle $x \in X$. Damit verbunden ist die Hoffnung, daß aus dem Kontext klar wird, ob im Einzelfall die Abbildung $c : X \to Y$ oder das Element $c \in Y$ gemeint sind.

Definition 2.2.11. Ist $f : X \to Y$ eine Abbildung und $B \subset Y$ eine Teilmenge, so definieren wir ihr **Urbild** $f^{-1}(B)$, eine Teilmenge von X, durch

$$f^{-1}(B) := \{x \in X \mid f(x) \in B\}$$

Besteht B nur aus einem Element x, so schreiben wir auch $f^{-1}(x)$ statt $f^{-1}(\{x\})$ und nennen diese Menge die **Faser von** f **über** x. Das Quadrieren q aus 2.2.9 hat etwa die Fasern $q^{-1}(1) = \{1, -1\}$ und $q^{-1}(-1) = \emptyset$.

Definition 2.2.12. Sind schließlich drei Mengen X, Y, Z gegeben und Abbildungen $f : X \to Y$ und $g : Y \to Z$, so definieren wir eine Abbildung $g \circ f : X \to Z$, die **Verknüpfung** der Abbildungen f und g, durch die Vorschrift

$$\begin{array}{rccc} g \circ f : & X & \to & Z \\ & x & \mapsto & g(f(x)) \end{array}$$

2.2.13. Die Notation $g \circ f$, sprich "g nach f", für "erst f, dann g" ist gewöhnungsbedürftig, erklärt sich aber durch die Formel $(g \circ f)(x) = g(f(x))$.

Beispiel 2.2.14. Betrachten wir zusätzlich zum Quadrieren $q : \mathbb{Z} \to \mathbb{Z}$ die Abbildung $t : \mathbb{Z} \to \mathbb{Z}, x \mapsto x+1$, so gilt $(q \circ t)(x) = (x+1)^2$ aber $(t \circ q)(x) = x^2 + 1$. Natürlich gilt $(g \circ f)(A) = g(f(A))$ für jede Teilmenge $A \subset X$ und umgekehrt auch $(g \circ f)^{-1}(C) = f^{-1}(g^{-1}(C))$ für jede Teilmenge $C \subset Z$.

Ergänzende Übung 2.2.15. Sei X eine Menge und $f : X \to X$ eine Abbildung. Bezeichne $f^n = f \circ f \circ \ldots \circ f : X \to X$ das "n-malige Ausführen von f". Im Extremfall $n = 0$ verstehen wir $f^0 = \mathrm{id}$. Sei nun $C \subset X$ eine Teilmenge. Man zeige: Stimmen für ein $n \in \mathbb{N}$ die Bildmengen $f^n(C)$ und $f^{n+1}(C)$ überein, so gilt bereits $f^n(C) = f^{n+1}(C) = f^{n+2}(C) \ldots$ Stimmen für ein $n \in \mathbb{N}$ die Urbildmengen $(f^n)^{-1}(C)$ und $(f^{n+1})^{-1}(C)$ überein, so gilt bereits $(f^n)^{-1}(C) = (f^{n+1})^{-1}(C) = (f^{n+2})^{-1}(C) \ldots$

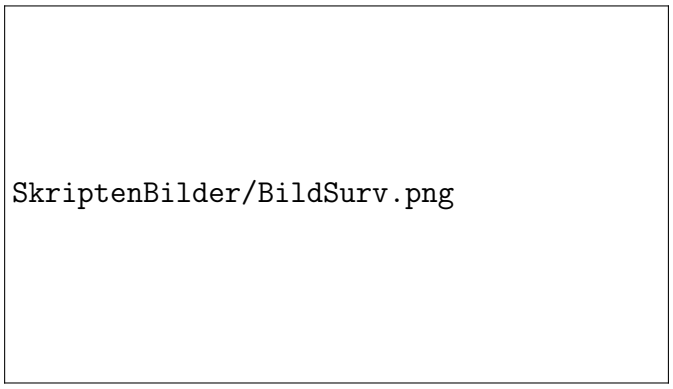
Definition 2.2.16. Sei $f : X \to Y$ eine Abbildung.

1. f heißt **injektiv** oder eine **Injektion** genau dann, wenn aus $x \neq x'$ folgt $f(x) \neq f(x')$. Gleichbedeutend ist die Forderung, daß es für jedes $y \in Y$ höchstens ein $x \in X$ gibt mit $f(x) = y$. Injektionen schreibt man oft $\hookrightarrow$.

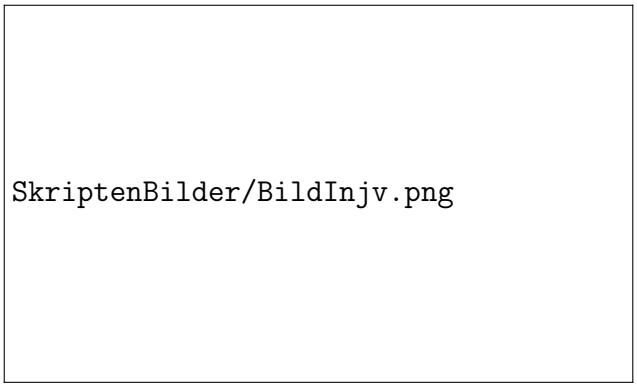
2. f heißt **surjektiv** oder eine **Surjektion** genau dann, wenn es für jedes $y \in Y$ mindestens ein $x \in X$ gibt mit $f(x) = y$. Surjektionen schreibt man manchmal $\twoheadrightarrow$.

3. f heißt **bijektiv** oder eine **Bijektion** genau dann, wenn f injektiv und surjektiv ist. Gleichbedeutend ist die Forderung, daß es für jedes $y \in Y$ genau ein $x \in X$ gibt mit $f(x) = y$. Bijektionen schreibt man oft $\xrightarrow{\sim}$.

2.2.17. Ist $X \subset Y$ eine Teilmenge, so ist die **Einbettung** oder **Inklusion** $i : X \to Y, x \mapsto x$ stets injektiv. Ist $g : Y \to Z$ eine Abbildung und $X \subset Y$ eine Teilmenge, so nennen wir die Verknüpfung $g \circ i$ von g mit der Inklusion



Eine Surjektion



Eine Injektion

Eine Bijektion

auch die **Einschränkung** von g auf X und notieren sie $g \circ i = g|X = g|_X : X \to Z$. Oft bezeichnen wir eine Einschränkung aber auch einfach mit demselben Buchstaben g in der Hoffnung, daß der Leser aus dem Kontext erschließen kann, welche Abbildung genau gemeint ist.

2.2.18. Ist $f : X \to Y$ eine Abbildung, so ist die Abbildung $f : X \to f(X)$, $x \mapsto f(x)$ stets surjektiv. Der Leser möge entschuldigen, daß wir hier zwei verschiedene Abbildungen mit demselben Symbol f bezeichnet haben. Das wird noch öfter vorkommen. Überhaupt ignorieren wir, gegeben Mengen X, Y und eine Teilmenge $Z \subset Y$, im folgenden meist den Unterschied zwischen "Abbildungen von X nach Y, deren Bild in Z enthalten ist" und "Abbildungen von X nach Z".

Ergänzung 2.2.19. Eine Abbildung $f : X \to \mathcal{P}(X)$ von einer Menge in ihre Potenzmenge kann nie surjektiv sein. In der Tat, betrachten wir in X die Teilmenge $A = \{x \in X \mid x \notin f(x)\}$, so kann es kein $y \in X$ geben mit $f(y) = A$, denn für solch ein y hätten wir entweder $y \in A$ oder $y \notin A$, und aus $y \in A$ alias $y \in f(y)$ folgte $y \notin A$, wohingegen aus $y \notin A$ alias $y \notin f(y)$ folgte $y \in A$.

Beispiele 2.2.20. Unsere Abbildung $q : \mathbb{Z} \to \mathbb{Z}, n \mapsto n^2$ ist weder injektiv noch surjektiv. Die Identität $\mathrm{id} : X \to X$ ist stets bijektiv. Sind X und Y endliche Mengen, so gibt es genau dann eine Bijektion von X nach Y, wenn X und Y dieselbe Kardinalität haben, in Formeln $|X| = |Y|$.

Satz 2.2.21. *Seien $f, f_1 : X \to Y$ und $g, g_1 : Y \to Z$ Abbildungen.*

1. *Ist $g \circ f$ injektiv, so ist f injektiv.*
2. *Sind g und f injektiv, so auch $g \circ f$.*
3. *Genau dann ist g injektiv, wenn aus $g \circ f = g \circ f_1$ schon folgt $f = f_1$.*

Beweis. Übung. Besonders elegant ist es, zunächst die letzte Aussage zu zeigen, und dann die vorderen Aussagen ohne weitere Betrachtung von Elementen zu folgern. □

Satz 2.2.22. *Seien $f, f_1 : X \to Y$ und $g, g_1 : Y \to Z$ Abbildungen.*

1. *Ist $g \circ f$ surjektiv, so ist g surjektiv.*
2. *Sind g und f surjektiv, so auch $g \circ f$.*
3. *Genau dann ist f surjektiv, wenn aus $g \circ f = g_1 \circ f$ schon folgt $g = g_1$.*

Beweis. Übung. Besonders elegant ist es, zunächst die letzte Aussage zu zeigen, und dann die vorderen Aussagen ohne weitere Betrachtung von Elementen zu folgern. □

2.2.23. Ist $f : X \to Y$ eine bijektive Abbildung, so ist offensichtlich die Menge $\{(f(x), x) \in Y \times X \mid x \in X\}$ im Sinne von 2.2.2 eine Abbildung oder, vielleicht klarer, der Graph einer Abbildung $Y \to X$. Diese Abbildung in die Gegenrichtung heißt die **Umkehrabbildung** oder **Umkehrfunktion** auch die **inverse Abbildung** zu f und wird mit $f^{-1} : Y \to X$ bezeichnet. Offensichtlich ist mit f auch f^{-1} eine Bijektion.

Beispiel 2.2.24. Die Umkehrabbildung unserer Bijektion $t : \mathbb{Z} \to \mathbb{Z}, x \mapsto x + 1$ ist die Abbildung $\mathbb{Z} \to \mathbb{Z}, x \mapsto x - 1$.

Übung 2.2.25. Gegeben eine Bijektion $f : X \to Y$ ist $g = f^{-1}$ die einzige Abbildung $g : Y \to X$ mit $f \circ g = \mathrm{id}_Y$. Ebenso ist auch $h = f^{-1}$ die einzige Abbildung $h : Y \to X$ mit $h \circ f = \mathrm{id}_X$.

2.2.26. Gegeben drei Mengen X, Y, Z haben wir eine offensichtliche Bijektion

$$\mathrm{Ens}(X \times Y, Z) \xrightarrow{\sim} \mathrm{Ens}(X, \mathrm{Ens}(Y, Z))$$

Etwas vage formuliert ist also eine Abbildung $X \times Y \to Z$ von einem kartesischen Produkt $X \times Y$ in eine weitere Menge Z dasselbe wie eine Abbildung, die jedem $x \in X$ eine Abbildung $Y \to Z$ zuordnet, und symmetrisch natürlich auch dasselbe wie eine Abbildung, die jedem $y \in Y$ eine Abbildung $X \to Z$ zuordnet. In der exponentiellen Notation liest sich das ganz suggestiv als kanonische Bijektion $Z^{(X \times Y)} \xrightarrow{\sim} (Z^X)^Y$. In diesem Sinne sind also die in der Schule derzeit so beliebten "Funktionen mit Parameter" nichts anderes als "Funktionen von zwei Variablen".

Satz 2.2.27 (Bedeutung der Fakultät). *Sind X und Y zwei Mengen mit je n Elementen, so gibt es genau $n!$ bijektive Abbildungen $f : X \to Y$.*

Beweis. Sei $X = \{x_1, \ldots, x_n\}$. Wir haben n Möglichkeiten, ein Bild für x_1 auszusuchen, dann noch $(n-1)$ Möglichkeiten, ein Bild für x_2 auszusuchen, und so weiter, bis schließlich nur noch 1 Element von Y als mögliches Bild von x_n in Frage kommt. Insgesamt gibt es also $n(n-1)\cdots 1 = n!$ Möglichkeiten für f. Da wir $0! = 1$ vereinbart hatten, stimmt unser Satz auch für $n = 0$. □

Ergänzende Übung 2.2.28. Seien X, Y endliche Mengen. So gibt es genau $|Y|^{|X|}$ Abbildungen von X nach Y, und unter diesen Abbildungen sind genau $|Y|(|Y|-1)(|Y|-2)\ldots(|Y|-|X|+1)$ Injektionen.

Ergänzende Übung 2.2.29. Sei X eine Menge mit n Elementen, und seien $\alpha_1, \ldots, \alpha_r \in \mathbb{N}$ gegeben mit $n = \alpha_1 + \ldots + \alpha_r$. Man zeige: Es gibt genau $n!/(\alpha_1! \cdots \alpha_r!)$ Abbildungen $f : X \to \{1, \ldots, r\}$, die jedes i genau α_i-mal als Wert annehmen, in Formeln

$$\frac{n!}{\alpha_1! \cdots \alpha_r!} = \mathrm{card}\{f \mid |f^{-1}(i)| = \alpha_i \text{ für } i = 1, \ldots r\}$$

Ergänzung 2.2.30. Manche Autoren bezeichnen die Zahlen aus der vorherigen Übung 2.2.29 auch als **Multinomialkoeffizienten** und verwenden die Notation

$$\frac{n!}{\alpha_1! \cdots \alpha_r!} = \binom{n}{\alpha_1; \ldots; \alpha_r}$$

Mich überzeugt diese Notation nicht, da sie im Gegensatz zu unserer Notation für die Binomialkoeffizienten recht eigentlich nichts kürzer macht.

Ergänzende Übung 2.2.31. Man zeige die Formel

$$(x_1 + \ldots + x_r)^n = \sum_{\alpha_1 + \ldots + \alpha_r = n} \frac{n!}{\alpha_1! \cdots \alpha_r!} x_1^{\alpha_1} \cdots x_r^{\alpha_r}$$

Hier ist zu verstehen, daß wir für alle $\alpha_1, \ldots, \alpha_r \in \mathbb{N}$ mit $\alpha_1 + \ldots + \alpha_r = n$ den angegebenen Ausdruck nehmen und alle diese Ausdrücke aufsummieren.

Ergänzende Übung 2.2.32. Eine **zyklische Anordnung** einer endlichen Menge M ist eine Abbildung $z : M \to M$ derart, daß wir durch mehrmaliges Anwenden von z auf ein beliebiges Element $x \in M$ jedes Element $y \in M$ erhalten können. Man zeige, daß es auf einer n-elementigen Menge mit $n \geq 1$ genau $(n-1)!$ zyklische Anordnungen gibt. Die Terminologie "zyklische Anordnung" macht mich nicht besonders glücklich, da unsere Struktur nun beim besten Willen keine Anordnung im Sinne von **??** ist. Andererseits ist aber das Angeben einer Anordnung auf einer endlichen Menge M schon auch etwas Ähnliches.

Ergänzende Übung 2.2.33. Sei X eine Menge mit $n \geq 1$ Elementen und sei m eine natürliche Zahl. Man zeige, daß es genau $\binom{n+m-1}{n-1}$ Abbildungen $f : X \to \mathbb{N}$ gibt mit $\sum_{x \in X} f(x) = m$. Hinweis: Man denke sich $X = \{1, 2, \ldots, n\}$ und veranschauliche sich dann f als eine Folge auf $f(1)$ Punkten gefolgt von einem Strich gefolgt von $f(2)$ Punkten gefolgt von einem Strich und so weiter, insgesamt also eine Folge aus $n + m - 1$ Symbolen, davon m Punkten und $n - 1$ Strichen.

Ergänzung 2.2.34. Gegeben eine Menge X mag man sich eine Abbildung $X \to \mathbb{N}$ veranschaulichen als eine "Menge von Elementen von X, in der jedes Element mit einer wohlbestimmten Vielfachheit vorkommt". Aufgrund dieser Vorstellung nennt man eine Abbildung $X \to \mathbb{N}$ auch eine **Multimenge** von Elementen von X. Unter der Kardinalität einer Multimenge verstehen wir die Summe über alle Werte der entsprechenden Abbildung, aufgefaßt als ein Element von $\mathbb{N} \sqcup \{\infty\}$. Ich notiere eine Multimenge mit normalen Mengenklammern, so wäre etwa $\{5, 5, 5, 7, 7, 1\}$ die hoffentlich offensichtliche Multimenge von natürlichen Zahlen der Kardinalität 6. Der Leser muß aus dem Kontext erschließen, wann bei der Verwendung von Mengenklammern eine Multimenge und wann eine normale Menge gemeint ist.

Versuch der graphischen Darstellung einer zyklischen Anordnung auf der Menge $\{1, 2, \ldots, 7\}$. Die Pfeile $\mapsto$ sollen jeweils den Effekt der Abbildung z veranschaulichen.

Eine Abbildung $f : \{1, 2, \ldots, n\} \to \mathbb{N}$ im Fall $n = 6$ mit Wertesumme $m = 10$ und die Veranschaulichung nach der Vorschrift aus Übung 2.2.33 als Folge bestehend aus m Punkten und $n - 1$ Strichen.

2.3 Logische Symbole und Konventionen

2.3.1. In der Mathematik meint **oder** immer, daß auch beides erlaubt ist. Wir haben diese Konvention schon benutzt bei der Definition der Vereinigung wenn wir schreiben $X \cup Y = \{z \mid z \in X \text{ oder } z \in Y\}$, zum Beispiel haben wir $\{1,2\} \cup \{2,3\} = \{1,2,3\}$.

2.3.2. Sagt man der Mathematik, es gebe ein Objekt mit diesen und jenen Eigenschaften, so ist stets gemeint, daß es *mindestens ein* derartiges Objekt geben soll. Hätten wir diese Sprachregelung rechtzeitig vereinbart, so hätten wir zum Beispiel das Wörtchen "mindestens" in Teil 2 von 2.2.16 bereits weglassen können. Sagt ihnen also ein Mathematiker, er habe einen Bruder, so kann es auch durchaus sein, daß er noch weitere Brüder hat! Will man in der Mathematik Existenz und Eindeutigkeit gleichzeitig ausdrücken, so sagt man, es gebe **genau ein** Objekt mit diesen und jenen Eigenschaften. Sagt ihnen also ein Mathematiker, er habe genau einen Bruder, so können sie sicher sein, daß er nicht noch weitere Brüder hat.

2.3.3. Die folgenden Abkürzungen erweisen sich als bequem und werden recht häufig verwendet:

$\forall$	für alle (ein umgedrehtes A wie "alle")
$\exists$	es gibt (ein umgedrehtes E wie "existiert")
$\exists!$	es gibt genau ein
$\ldots \Rightarrow \cdots$	aus $\ldots$ folgt $\cdots$
$\ldots \Leftarrow \cdots$	$\ldots$ folgt aus $\cdots$
$\ldots \Leftrightarrow \cdots$	$\ldots$ ist gleichbedeutend zu $\cdots$

Ist zum Beispiel $f : X \to Y$ eine Abbildung, so können wir unsere Definitionen injektiv, surjektiv, und bijektiv etwas formaler so schreiben:

$$\begin{array}{lcl} f \text{ injektiv} & \Leftrightarrow & ((f(x) = f(z)) \Rightarrow (x = z)) \\ f \text{ surjektiv} & \Leftrightarrow & \forall y \in Y \exists x \in X \text{ mit } f(x) = y \\ f \text{ bijektiv} & \Leftrightarrow & \forall y \in Y \exists! x \in X \text{ mit } f(x) = y \end{array}$$

Ergänzung 2.3.4. In den Zeiten des Bleisatzes war es nicht einfach, neue Symbole in Zeitschriften gedruckt zu kriegen, aber irgendwelche Buchstaben verdreht zu setzen, war unproblematisch. So entstanden dann auch die Symbole $\forall$ und $\exists$.

2.3.5. Bei den "für alle" und "es gibt" kommt es in der Mathematik, anders als in der weniger präzisen Umgangssprache, entscheidend auf die Reihenfolge an. Man betrachte zum Beispiel die beiden folgenden Aussagen:

"Für alle $n \in \mathbb{N}$ gibt es $m \in \mathbb{N}$ so daß gilt $m \geq n$"

"Es gibt $m \in \mathbb{N}$ so daß für alle $n \in \mathbb{N}$ gilt $m \geq n$"

Offensichtlich ist die Erste richtig, die Zweite aber falsch. Weiter mache man sich klar, daß die "für alle" und "es gibt" bei Verneinung vertauscht werden. Äquivalent sind zum Beispiel die beiden folgenden Aussagen

"Es gibt kein $n \in \mathbb{N}$ mit $n^2 = 2$"

"Für alle $n \in \mathbb{N}$ gilt nicht $n^2 = 2$"

2.3.6. Wollen wir zeigen, daß aus einer Aussage A eine andere Aussage B folgt, so können wir ebensogut zeigen: Gilt B nicht, so gilt auch A nicht. In formelhafter Schreibweise haben wir also

$$(A \Rightarrow B) \Leftrightarrow ((\text{nicht } B) \Rightarrow (\text{nicht } A))$$

Wollen wir zum Beispiel zeigen $(g \circ f \text{ surjektiv}) \Rightarrow (g \text{ surjektiv})$, so reicht es, wenn wir uns überlegen: Ist g nicht surjektiv, so ist $g \circ f$ erst recht nicht surjektiv.

2.3.7. In der Literatur findet man oft die Abkürzung **oBdA** für "ohne Beschränkung der Allgemeinheit".

3 Algebraische Grundbegriffe

Auf der Schule versteht man unter einer "reellen Zahl" meist einen unendlichen Dezimalbruch, wobei man noch aufpassen muß, daß durchaus verschiedene unendliche Dezimalbrüche dieselbe reelle Zahl darstellen können, zum Beispiel gilt in den reellen Zahlen ja

$$0,99999\ldots = 1,00000\ldots$$

Diese reellen Zahlen werden dann addiert, subtrahiert, multipliziert und dividiert ohne tiefes Nachdenken darüber, wie man denn zum Beispiel mit den eventuell unendlich vielen Überträgen bei der Addition und Subtraktion umgehen soll, und warum dann Formeln wie $(a+b)-c = a+(b-c)$ wirklich gelten, zum Beispiel für $a = b = c = 0,999\ldots$. Dieses tiefe Nachdenken wollen wir im Folgenden vom Rest der Vorlesung abkoppeln und müssen dazu sehr präzise formulieren, welche Eigenschaften für die Addition, Multiplikation und Anordnung in "unseren" reellen Zahlen gelten sollen: In der Terminologie, die in den folgenden Abschnitten eingeführt wird, werden wir die reellen Zahlen charakterisieren als einen angeordneten Körper, in dem jede nichtleere Teilmenge mit einer unteren Schranke sogar eine größte untere Schranke besitzt. Von dieser Charakterisierung ausgehend erklären wir dann, welche reelle Zahl ein gegebener unendlicher Dezimalbruch darstellt, und errichten das Gebäude der Analysis. In demselben Begriffsgebäude modellieren wir auch den Anschauungsraum, vergleiche 1.2.8 oder besser II.1.7.7 und II.4.1.4. Um diese Charakterisierungen und Modellierungen verständlich zu machen, führen wir zunächst einige grundlegende algebraische Konzepte ein, die Ihnen im weiteren Studium der Mathematik noch oft begegnen werden.

3.1 Mengen mit Verknüpfung

Definition 3.1.1. Eine **Verknüpfung $\top$ auf einer Menge** A ist eine Abbildung

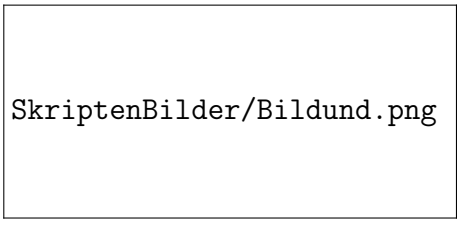
$$\begin{array}{rccc} \top: & A\times A & \to & A \\ & (a,b) & \mapsto & a\top b \end{array}$$

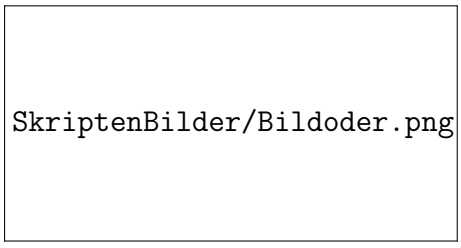
die also jedem geordneten Paar (a,b) mit $a,b\in A$ ein weiteres Element $(a\top b)\in A$ zuordnet.

Beispiele 3.1.2. 1. Die Addition von ganzen Zahlen ist eine Verknüpfung

$$\begin{array}{rccc} +: & \mathbb{Z}\times\mathbb{Z} & \to & \mathbb{Z} \\ & (a,b) & \mapsto & a+b \end{array}$$

Man kann Verknüpfungen auf endlichen Mengen darstellen durch ihre **Verknüpfungstafel**. Hier habe ich etwa die Verknüpfungstafel der Verknüpfung $\min$ auf der Menge $\{0, 1, 2, 3, 4\}$ angegeben. Eigentlich muß man sich dazu einigen, ob im Kästchen aus der Spalte a und der Zeile b nun $a \top b$ oder vielmehr $b \top a$ stehen soll, aber bei einer kommutativen Verknüpfung wie $\min$ kommt es darauf zum Glück nicht an.





Die Wahrheitstafeln für “und” und “oder”. Gemeint ist hier wie stets in der Mathematik das “nichtausschließende oder”. Sagen wir, es gelte A oder B, so ist insbesondere auch erlaubt, daß beides gilt. Bei der Wahrheitstafel für das “ausschließende oder” müßte oben links als Verknüpfung von “Wahr” mit “Wahr” ein “Falsch” stehen.

2. Die Multiplikation von ganzen Zahlen ist eine Verknüpfung

$$\begin{array}{rccc} \cdot : & \mathbb{Z} \times \mathbb{Z} & \to & \mathbb{Z} \\ & (a,b) & \mapsto & a \cdot b \end{array}$$

3. Die Zuordnung $\min$, die jedem Paar von natürlichen Zahlen die kleinere zuordnet (wenn sie verschieden sind, man setzt sonst $\min(a,a) = a$), ist eine Verknüpfung

$$\begin{array}{rccc} \min : & \mathbb{N} \times \mathbb{N} & \to & \mathbb{N} \\ & (a,b) & \mapsto & \min(a,b) \end{array}$$

4. Sei X eine Menge. Die Verknüpfung von Abbildungen liefert eine Verknüpfung auf der Menge $\mathrm{Ens}(X,X)$ aller Abbildungen von X in sich selber

$$\begin{array}{rccc} \circ : & \mathrm{Ens}(X,X) \times \mathrm{Ens}(X,X) & \to & \mathrm{Ens}(X,X) \\ & (f,g) & \mapsto & f \circ g \end{array}$$

   Oft kürzen wir auch $\mathrm{Ens}(X,X) = \mathrm{Ens}(X)$ ab.

5. Die Subtraktion von ganzen Zahlen ist eine Verknüpfung

$$\begin{array}{rccc} - : & \mathbb{Z} \times \mathbb{Z} & \to & \mathbb{Z} \\ & (a,b) & \mapsto & a - b \end{array}$$

6. Jede Verknüpfung $\top$ auf einer Menge induziert eine Verknüpfung auf ihrer Potenzmenge vermittels der Vorschrift

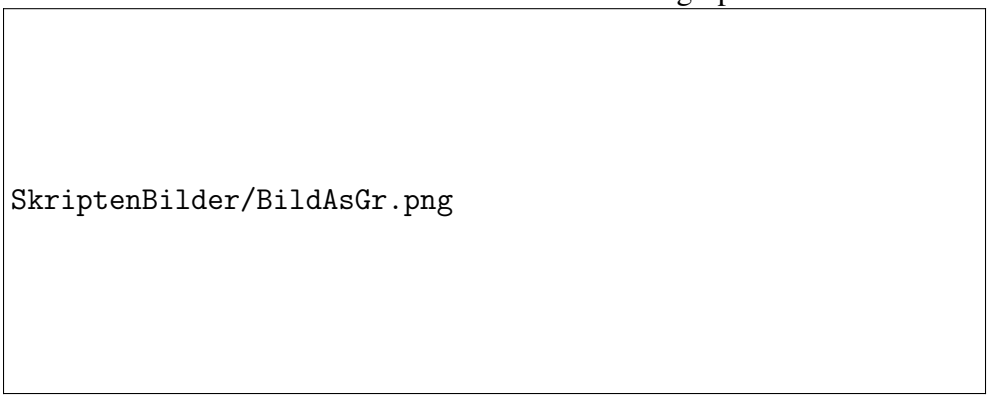
$$U \top V = \{u \top v \mid u \in U,\ v \in V\}$$

7. Gegeben Mengen mit Verknüpfung $(A, \top)$ und $(B, \perp)$ erhalten wir eine Verknüpfung auf ihrem Produkt $A \times B$ vermittels der Vorschrift $((a,b),(a',b')) \mapsto ((a \top a'),(b \perp b'))$. Sie heißt die **komponentenweise Verknüpfung**.

8. Die logischen Operationen "und", "oder", "impliziert" und dergleichen mehr können auch als Verknüpfungen auf der zweielementigen Menge $\{\text{Wahr}, \text{Falsch}\}$ aufgefaßt werden. Die zugehörigen Verknüpfungstabellen heißen **Wahrheitstafeln**. Bei einem formalen Zugang werden diese Tafeln, wie sie für "und" und "oder" auf der vorhergehenden Seite zu finden sind, sogar zur Definition der jeweiligen Begriffe.

Definition 3.1.3. Eine Verknüpfung $\top$ auf einer Menge A heißt **assoziativ** genau dann, wenn gilt $a \top (b \top c) = (a \top b) \top c \quad \forall a,b,c \in A$. Sie heißt **kommutativ** genau dann, wenn gilt $a \top b = b \top a \quad \forall a,b \in A$.

Mögliche “Klammerungen” mag man sich graphisch wie oben angedeutet veranschaulichen. Die Assoziativität bedeutet dann graphisch so etwas wie



wobei das Gleichheitszeichen nur meint, daß beide Klammerungen stets dasselbe liefern, wenn wir oben drei Elemente unserer Menge mit Verknüpfung einfüllen. . .

Beispiele 3.1.4. Von unseren Beispielen sind die ersten drei assoziativ und kommutativ, das vierte ist assoziativ aber nicht kommutativ falls X mehr als ein Element hat, das fünfte ist weder assoziativ noch kommutativ.

3.1.5. Ist eine Verknüpfung assoziativ, so liefern auch ungeklammerte Ausdrücke der Form $a_1 \top a_2 \ldots \top a_n$ wohlbestimmte Elemente von A, das Resultat ist genauer unabhängig davon, wie wir die Klammern setzen. Um diese Erkenntnis zu formalisieren, vereinbaren wir für so einen Ausdruck die Interpretation

$$a_1 \top a_2 \ldots \top a_n = a_1 \top (a_2 \top (\ldots (a_{n-1} \top a_n) \ldots))$$

und zeigen

Lemma 3.1.6. *Gegeben $(A, \top)$ eine Menge mit einer assoziativen Verknüpfung und $a_1, \ldots, a_n, b_1, \ldots, b_m \in A$ gilt*

$$(a_1 \top \ldots \top a_n) \top (b_1 \top \ldots \top b_m) = a_1 \top \ldots \top a_n \top b_1 \top \ldots \top b_m$$

Beweis. Wir folgern aus dem Assoziativgesetz $(a_1 \top \ldots \top a_n) \top (b_1 \top \ldots \top b_m) = a_1 \top ((a_2 \top \ldots \top a_n) \top (b_1 \top \ldots \top b_m))$ und sind fertig mit vollständiger Induktion über n. □

3.1.7. Das Wort Lemma, im Plural Lemmata, kommt wohl von griechisch $\lambda\alpha\mu\beta\alpha\nu\epsilon\iota\nu$ "nehmen" und bezeichnet in der Mathematik kleinere Resultate oder auch Zwischenschritte von größeren Beweisen, denen der Autor außerhalb ihres engeren Kontexts keine große Bedeutung zumißt.

Ergänzung 3.1.8. Die Zahl der Möglichkeiten, einen Ausdruck in $n+1$ Faktoren so zu verklammern, daß in jedem Schritt nur die Verknüpfung von je zwei Elementen zu berechnen ist, heißt die **n-te Catalan-Zahl** und wird C_n notiert. Die ersten Catalan-Zahlen sind $C_0 = C_1 = 1$, $C_2 = 2$, $C_3 = 5$: Die fünf möglichen Verklammerungen von 4 Elementen sind etwa $(ab)(cd)$, $a(b(cd))$, $a((bc)d)$, $((ab)c)d$ und $(a(bc))d$. Im allgemeinen zeigen wir in **??**, daß sich die Catalan-Zahlen durch die Binomial-Koeffizienten 1.1.16 ausdrücken lassen vermittels der amüsanten Formel

$$C_n = \frac{1}{n+1}\binom{2n}{n} = \binom{2n}{n} - \binom{2n}{n+1}$$

Definition 3.1.9. Sei $(A, \top)$ eine Menge mit Verknüpfung. Ist $n \in \{1, 2, \ldots\}$ eine von Null verschiedene natürliche Zahl und $a \in A$, so schreiben wir

$$\underbrace{a \top a \top \ldots \top a}_{n\text{-mal}} = n^{\top} a$$

3.1.10. Ist m eine zweite von Null verschiedene natürliche Zahl, so erhalten wir für assoziative Verknüpfungen mithilfe unseres Lemmas 3.1.6 die Regeln $(n+m)^\top a = (n^\top a)\top(m^\top a)$ und $(nm)^\top a = n^\top(m^\top a)$. Ist unsere Verknüpfung auch noch kommutativ, so gilt zusätzlich $n^\top(a\top b) = (n^\top a)\top(n^\top b)$.

3.1.11. Sei $(A,\top)$ eine Menge mit Verknüpfung. Eine Teilmenge $B \subset A$ heißt **abgeschlossen unter der Verknüpfung** genau dann, wenn aus $a,b \in B$ folgt $a\top b \in B$. Natürlich ist in diesem Fall auch $(B,\top)$ eine Menge mit Verknüpfung, man spricht dann von der **auf B induzierten Verknüpfung**. Zum Beispiel ist $\mathbb{N} \subset \mathbb{Z}$ abgeschlossen unter der Addition, aber $\mathbb{Z}_{\neq 0} \subset \mathbb{Q}_{\neq 0}$ ist nicht abgeschlossen unter der durch die Division gegebenen Verknüpfung $(a,b) \mapsto a/b$.

Definition 3.1.12. Sei $(A,\top)$ eine Menge mit Verknüpfung. Ein Element $e \in A$ heißt **neutrales Element** von $(A,\top)$ genau dann, wenn gilt

$$e\top a = a\top e = a \quad \forall a \in A$$

3.1.13. In einer Menge mit Verknüpfung $(A,\top)$ kann es höchstens ein neutrales Element e geben, denn für jedes weitere Element e' mit $e'\top a = a\top e' = a \quad \forall a \in A$ haben wir $e' = e'\top e = e$. Wir dürfen also den bestimmten Artikel verwenden und in einer Menge mit Verknüpfung von *dem* neutralen Element reden.

Definition 3.1.14. Ein **Monoid** ist eine Menge mit einer assoziativen Verknüpfung, in der es ein neutrales Element gibt. Ist $(A,\top)$ ein Monoid, so erweitern wir unsere Notation $n^\top a$ aus 3.1.9 auf alle natürlichen Zahlen $n \in \mathbb{N}$, indem wir $0^\top a$ als das neutrale Element von A verstehen, für alle $a \in A$.

3.1.15. Das Wort "Monoid" ist wohl von griechisch "$\mu o\nu o\varsigma$" für "allein" abgeleitet: Ein Monoid besitzt nur eine einzige Verknüpfung.

3.1.16. In Monoiden gelten die Regeln 3.1.10 für alle $n,m \in \mathbb{N}$. Die natürlichen Zahlen bilden mit der Addition ein Monoid $(\mathbb{N},+)$ mit neutralem Element 0. Sie bilden auch unter der Multiplikation ein Monoid $(\mathbb{N},\cdot)$ mit neutralem Element 1. Für jede Menge X ist die Menge $\mathrm{Ens}(X)$ der Abbildungen von X in sich selbst ein Monoid. Die leere Menge ist *kein* Monoid, ihr fehlt das neutrale Element.

3.1.17. Gegeben eine Abbildung $I \to A$, $i \mapsto a_i$ von einer endlichen Menge in ein kommutatives additiv bzw. multiplikativ notiertes Monoid vereinbaren wir die Notationen

$$\sum_{i\in I} a_i \qquad \text{bzw.} \qquad \prod_{i\in I} a_i$$

für die "Verknüpfung aller a_i". Ist I die leere Menge, so vereinbaren wir, daß dieser Ausdruck das neutrale Element von A bedeuten möge, also 0 bzw. 1. Wir

haben diese Notation bereits verwendet in 2.1.19, und für die konstante Abbildung $I \to \mathbb{N}, i \mapsto 1$ hätten wir zum Beispiel

$$\sum_{i \in I} 1 = |I|$$

Unsere Konvention 1.1.13 für mit einem Laufindex notierte Summen bzw. Produkte verwenden wir bei Monoiden analog.

Übung 3.1.18. Sei X eine Menge. Das Schneiden von Teilmengen ist eine Verknüpfung

$$\begin{array}{rccc} \cap : & \mathcal{P}(X) \times \mathcal{P}(X) & \to & \mathcal{P}(X) \\ & (A, B) & \mapsto & A \cap B \end{array}$$

auf der Potenzmenge. Dasselbe gilt für die Vereinigung und das Bilden der Differenzmenge. Welche dieser Verknüpfungen sind kommutativ oder assoziativ? Welche besitzen neutrale Elemente?

Ergänzende Übung 3.1.19. Man gebe die Wahrheitstafeln für $\Rightarrow$ und $\Leftrightarrow$ an. Bezeichne weiter $\neg : \{\text{Wahr}, \text{Falsch}\} \to \{\text{Wahr}, \text{Falsch}\}$ die "Verneinung". Man zeige, daß die Formel

$$(A \Rightarrow B) \Leftrightarrow ((\neg B) \Rightarrow (\neg A))$$

beim Einsetzen beliebiger Wahrheitswerte aus $\{\text{Wahr}, \text{Falsch}\}$ für A und B stets den Wert "Wahr" ausgibt, in Übereinstimmung mit unseren eher intuitiven Überlegungen in 2.3.6.

3.2 Gruppen

3.2.1. Ich empfehle, bei der Lektüre dieses Abschnitts die Tabelle auf Seite 59 gleich mitzulesen, die die Bedeutungen der nun folgenden Formalitäten in den zwei gebräuchlichsten Notationssystemen angibt. In diesen Notationssystemen sollten alle Formeln aus der Schulzeit vertraut sein. Wir erinnern uns an die Definition eines Monoids aus 3.1.14: Ein Monoid ist eine Menge mit einer assoziativen Verknüpfung, für die es in unserer Menge ein neutrales Element gibt.

Definition 3.2.2.

1. Ist $(A, \top)$ ein Monoid und $a \in A$ ein Element, so nennen wir ein weiteres Element $\bar{a} \in A$ **invers zu** a genau dann, wenn gilt $a \top \bar{a} = e = \bar{a} \top a$ für $e \in A$ das neutrale Element unseres Monoids. Ein Element, das ein Inverses besitzt, heißt **invertierbar**.

2. Eine **Gruppe** ist ein Monoid, in dem jedes Element ein Inverses besitzt.

3. Eine **kommutative Gruppe** oder **abelsche Gruppe** ist eine Gruppe, deren Verknüpfung kommutativ ist.

3.2.3. Der Begriff einer "Gruppe" wurde von Évariste Galois (1811-1832) in die Mathematik eingeführt. Er verwendet den Begriff "Gruppe von Transformationen" sowohl in der Bedeutung einer "Menge von bijektiven Selbstabbildungen einer gegebenen Menge" als auch in der Bedeutung einer "Menge von bijektiven Selbstabbildungen einer gegebenen Menge, die abgeschlossen ist unter Verknüpfung und Inversenbildung", und die damit in der Tat ein Beispiel für eine Gruppe im Sinne der obigen Definition bildet. Unsere obige Definition 3.2.2 konnte Galois beim besten Willen nicht geben: Er starb ein gutes halbes Jahrhundert, bevor Cantor die Sprache der Mengenlehre entwickelte. Die Terminologie "abelsche Gruppe" wurde zu Ehren des norwegischen Mathematikers Niels Hendrik Abel eingeführt.

Lemma 3.2.4. *Jedes Element eines Monoids besitzt höchstens ein Inverses.*

Beweis. Aus $a \top \bar{a} = e = \bar{a} \top a$ und $a \top b = e = b \top a$ folgt durch Anwenden von $b\top$ auf die erste Gleichung mit dem Assoziativgesetz sofort $\bar{a} = b$. □

3.2.5. Wir dürfen also den bestimmten Artikel benutzen und von nun an von *dem* Inversen eines Elements eines Monoids und insbesondere auch einer Gruppe reden. Offensichtlich ist das Inverse des Inversen stets das ursprüngliche Element, in Formeln $\bar{\bar{a}} = a$.

Lemma 3.2.6. *Sind a und b Elemente einer Gruppe oder allgemeiner invertierbare Elemente eines Monoids, so wird das Inverse von $a \top b$ wird gegeben durch die Formel $\overline{(a \top b)} = \bar{b} \top \bar{a}$.*

Beweis. In der Tat rechnen wir schnell $(a \top b) \top (\bar{b} \top \bar{a}) = e = (\bar{b} \top \bar{a}) \top (a \top b)$. Diese Formel ist auch aus dem täglichen Leben vertraut: Wenn man sich morgends zuerst die Strümpfe anzieht und dann die Schuhe, so muß man abends zuerst die Schuhe ausziehen und dann die Strümpfe. □

Beispiele 3.2.7. Von unseren Beispielen 3.1.2 für Verknüpfungen oben ist nur $(\mathbb{Z}, +)$ eine Gruppe, und diese Gruppe ist kommutativ. Ein anderes Beispiel für eine kommutative Gruppe ist die Menge $\mathbb{Q}\backslash\{0\}$ der von Null verschiedenen rationalen Zahlen mit der Multiplikation als Verknüpfung.

Übung 3.2.8. Die invertierbaren Elemente eines Monoids bilden stets eine Gruppe. Ein Element a eines Monoids A ist invertierbar genau dann, wenn es $b, c \in A$ gibt mit $b \top a = e = a \top c$ für e das neutrale Element.

Definition 3.2.9. Ist $(A, \top)$ eine Gruppe, so erweitern wir unsere Notation $n^\top a$ aus 3.1.14 auf alle $n \in \mathbb{Z}$, indem wir setzen $n^\top a = (-n)^\top \bar{a}$ für $n \in \{-1, -2, \ldots\}$.

Die Verknüpfungstafel der Gruppe aller Permutationen der Menge $\{1, 2, 3\}$. Eine solche Permutation σ habe ich dargestellt durch das geordnete Zahlentripel $\sigma(1)\sigma(2)\sigma(3)$, und im Kästchen aus der Zeile τ und der Spalte σ steht $\tau \circ \sigma$.

abstrakt	additiv	multiplikativ
$a \top b$	$a + b$	$a \cdot b$, $a \circ b$, ab
e	0	1
$\bar{b}$	$-b$	$1/b$
$a \top \bar{b}$	$a - b$	a/b
$n^\top a$	na	a^n
$e \top a = a \top e = a$	$0 + a = a + 0 = a$	$1 \cdot a = a \cdot 1 = a$
$a \top \bar{a} = e$	$a - a = 0$	$a/a = 1$
$\bar{\bar{a}} = a$	$-(-a) = a$	$1/(1/a) = a$
$(-1)^\top a = \bar{a}$	$(-1)a = -a$	$a^{-1} = 1/a$
$\overline{(a \top b)} = \bar{b} \top \bar{a}$	$-(a + b) = (-b) + (-a)$	$(ab)^{-1} = b^{-1}a^{-1}$, $1/ab = (1/b)(1/a)$
$\overline{(a \top \bar{b})} = b \top \bar{a}$	$-(a - b) = b - a$	$1/(a/b) = b/a$
$n^\top (m^\top a) = (nm)^\top a$	$n(ma) = (nm)a$	$(a^m)^n = a^{nm}$
$(m + n)^\top a = (m^\top a) \top (n^\top a)$	$(m + n)a = (ma) + (na)$	$a^{(m+n)} = (a^m)(a^n)$
$\overline{n^\top a} = (-n)^\top a$	$-(na) = (-n)a$	$(a^n)^{-1} = a^{-n}$
$0^\top a = e$	$0a = 0$	$a^0 = 1$
$n^\top (a \top b) = (n^\top a) \top (n^\top b)$	$n(a + b) = (na) + (nb)$	$(ab)^n = (a^n)(b^n)$

Tabelle I.1: Konventionen und Formeln in verschiedenen Notationssystemen. Bereits diese Tabelle muß mit einigen Hintergedanken gelesen werden, weil die Symbole $+, -, 0, 1$ darin in zweierlei Bedeutung vorkommen: Manchmal meinen sie konkrete Operationen in $\mathbb{Z}$ bzw. Elemente von $\mathbb{Z}$, manchmal stehen sie aber auch für Verknüpfung, Inversenbildung und neutrale Elemente in abstrakten Monoiden. Es scheint mir eine gute Übung, die Tabelle durchzugehen und allen Symbolen $0, 1$ einen Hut aufzusetzen, wenn sie nicht ganze Zahlen bedeuten.

3.2.10. In einer Gruppe gelten offensichtlich sogar für alle ganzen Zahlen $n \in \mathbb{Z}$ die Regeln $(n+m)^\top a = (n^\top a)\top(m^\top a)$ und $(nm)^\top a = n^\top(m^\top a)$. Ist die Gruppe kommutativ, so gilt zusätzlich $n^\top(a\top b) = (n^\top a)\top(n^\top b)$ für alle $n \in \mathbb{Z}$.

3.2.11. Verknüpfungen werden meist additiv oder multiplikativ geschrieben, also $a + b$ oder $a \cdot b$, wobei die additive Schreibweise kommutativen Verknüpfungen vorbehalten ist und die Bruchnotation $1/a$ und b/a aus nebenstehender Tabelle kommutativen multiplikativ geschriebenen Monoiden, in denen b invertierbar ist. Bei additiv geschriebenen Gruppen bezeichnet man das Inverse von a meist als das **Negative** von a. Bei nichtkommutativen und multiplikativ notierten Gruppen oder Monoiden benutzt man für das Inverse von a nur die von der allgemeinen Notation a^n abgeleitete Notation a^{-1}. Die nebenstehende Tabelle faßt die üblichen Notationen für unsere abstrakten Begriffsbildungen in diesem Kontext zusammen und gibt unsere allgemeinen Resultate und Konventionen in diesen Notationen wieder. Diejenigen Formeln und Konventionen, die keine Inversen brauchen, benutzt man auch allgemeiner für beliebige Monoide. Für die Gruppe der invertierbaren Elemente eines multiplikativ notierten Monoids A verwenden wir die Notation $A^\times$. Zum Beispiel haben wir $\mathbb{Z}^\times = \{1, -1\}$.

Beispiel 3.2.12. Für jede Menge X ist die Menge aller Bijektionen von X auf sich selbst eine Gruppe, mit der Komposition von Abbildungen als Verknüpfung. Wir notieren diese Gruppe $\mathrm{Ens}^\times(X)$ in Übereinstimmung mit unserer Konvention 3.2.11, schließlich handelt es sich um die Gruppe der invertierbaren Elemente des Monoids $\mathrm{Ens}(X)$. Ihre Elemente heißen die **Permutationen von** X. Die Gruppe der Permutationen einer Menge X ist für $|X| > 2$ nicht kommutativ. Das Inverse einer Bijektion ist ihre Umkehrabbildung.

Übung 3.2.13. Sind a, b, c Elemente einer Gruppe, so folgt aus $a\top b = a\top c$ bereits $b = c$. Ebenso folgt auch aus $b\top a = c\top a$ bereits $b = c$. Salopp gesprochen dürfen wir also in einer Gruppe "kürzen". Dasselbe gilt allgemeiner in einem beliebigen Monoid, wenn wir a invertierbar annehmen.

Ergänzende Übung 3.2.14. Sei A ein Monoid und e sein neutrales Element. Man zeige: Unser Monoid ist genau dann eine Gruppe, wenn es für jedes $a \in A$ ein $\bar{a} \in A$ gibt mit $\bar{a}\top a = e$, und dies Element $\bar{a}$ ist dann notwendig das Inverse von a in A. Noch Mutigere zeigen: Ist A eine Menge mit assoziativer Verknüpfung und existiert ein $e \in A$ mit $e\top a = a\ \forall a \in A$ sowie für jedes $a \in A$ ein $\bar{a} \in A$ mit $\bar{a}\top a = e$, so ist A eine Gruppe.

3.3 Körper

Definition 3.3.1. Ein **Körper** $(K, +, \cdot)$ (englisch **field**, französisch **corps**) ist eine Menge K mit zwei assoziativen und kommutativen Verknüpfungen, der sogenannten **Addition** $+$ und **Multiplikation** $\cdot$ des Körpers, derart daß die folgenden drei Bedingungen erfüllt sind:

1. $(K, +)$ ist eine Gruppe, die **additive Gruppe** des Körpers.
2. Bezeichnet $0_K \in K$ das neutrale Element der Gruppe $(K, +)$, so folgt aus $a \neq 0_K \neq b$ schon $a \cdot b \neq 0_K$ und $(K\backslash\{0_K\}, \cdot)$ ist eine Gruppe, die **multiplikative Gruppe** des Körpers.
3. Es gilt das **Distributivgesetz**

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad \forall a, b, c \in K$$

Ergänzung 3.3.2. Der Begriff "Körper" ist in diesem Zusammenhang wohl zu verstehen als "besonders gut unter den verschiedensten Rechenoperationen abgeschlossener Zahlbereich", in Analogie zu geometrischen Körpern wie Kugeln oder Zylindern, die man entsprechend als "besonders gut in sich geschlossene Bereiche des Raums" ansehen könnte. Die Bezeichnung "Distributivgesetz" rührt daher, daß uns dies Gesetz erlaubt, beim Multiplizieren eines Elements mit einer Summe den "Faktor auf die Summanden zu verteilen".

3.3.3. Wenn wir mit Buchstaben rechnen, werden wir meist $a \cdot b = ab$ abkürzen. Zusätzlich vereinbaren wir zur Vermeidung von Klammern die Regel "Punkt vor Strich", so daß also zum Beispiel das Distributivgesetz kürzer in der Form $a(b + c) = ab + ac$ geschrieben werden kann. Die multiplikative Gruppe eines Körpers K notieren wir $K^\times = K\backslash\{0_K\}$ in Übereinstimmung mit unserer allgemeinen Notation 3.2.11, schließlich handelt es sich um die Menge der invertierbaren Elemente des multiplikativen Monoids K. Für das neutrale Element der Multiplikation vereinbaren wir die Bezeichnung $1_K \in K^\times$. Wir kürzen meist 0_K ab durch 0 und 1_K durch 1 in der Erwartung, daß man aus dem Kontext erschließt, ob mit 0 und 1 natürliche Zahlen oder Elemente eines speziellen Körpers gemeint sind. Meist kommt es darauf im Übrigen gar nicht an.

3.3.4. Für alle a, b in einem Körper und alle $n \geq 0$ gilt die binomische Formel

$$(a + b)^n = \sum_{\nu=0}^{n} \binom{n}{\nu} a^\nu b^{n-\nu}$$

Um das einzusehen prüft man, daß wir bei der Herleitung nach 1.1.22 nur Körperaxiome verwandt haben. Man beachte hierbei unsere Konvention $0_K^0 = 1_K$

aus 3.1.14, angewandt auf das Monoid $(K, \cdot)$ in Verbindung mit der notationellen Konvention auf Seite 59. Die Multiplikation mit den Binomialkoeffizienten in dieser Formel ist zu verstehen als wiederholte Addition im Sinne der Bezeichnungskonvention na auf Seite 59, angewandt auf den Spezialfall der additiven Gruppe unseres Körpers.

Beispiele 3.3.5. Ein Beispiel für einen Körper ist der Körper der rationalen Zahlen $(\mathbb{Q}, +, \cdot)$. Ein anderes Beispiel ist der zweielementige Körper mit den durch die Axiome erzwungenen Rechenregeln, der fundamental ist in der Informatik. Die ganzen Zahlen $(\mathbb{Z}, +, \cdot)$ bilden keinen Körper, da $(\mathbb{Z} \setminus \{0\}, \cdot)$ keine Gruppe ist, da es nämlich in $\mathbb{Z} \setminus \{0\}$ nur für 1 und -1 ein multiplikatives Inverses gibt. Es gibt keinen einelementigen Körper, da das Komplement seines Nullelements die leere Menge sein müßte: Dies Komplement kann dann aber unter der Multiplikation keine Gruppe sein, da es eben kein neutrales Element haben könnte.

Lemma 3.3.6 (Folgerungen aus den Körperaxiomen). *Sei K ein Körper. So gilt*

1. $a0 = 0 \quad \forall a \in K$.
2. $ab = 0 \Rightarrow a = 0$ *oder* $b = 0$.
3. $-a = (-1)a \quad \forall a \in K$.
4. $(-1)(-1) = 1$.
5. $(-a)(-b) = ab \quad \forall a, b \in K$.
6. $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$ *für alle* $a, c \in K$ *und* $b, d \in K^\times$.
7. $\frac{ac}{bc} = \frac{a}{b}$ *für alle* $a \in K$ *und* $b, c \in K^\times$.
8. $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ *für alle* $a, c \in K$ *und* $b, d \in K^\times$.
9. $m(ab) = (ma)b$ *für alle* $m \in \mathbb{Z}$ *und* $a, b \in K$.

Beweis.

1. Man folgert das aus $a0 + a0 = a(0+0) = a0$ durch Hinzuaddieren von $-(a0)$ auf beiden Seiten.
2. In der Tat folgt aus ($a \neq 0$ und $b \neq 0$) schon ($ab \neq 0$) nach den Körperaxiomen.
3. In der Tat gilt $a + (-1)a = 1a + (-1)a = (1 + (-1))a = 0a = 0$, und $-a$ ist ja gerade definiert als das eindeutig bestimmte Element von K so daß $a + (-a) = 0$.
4. In der Tat gilt nach dem Vorhergehenden $(-1)(-1) = -(-1) = 1$.
5. Um das nachzuweisen ersetzen wir einfach $(-a) = (-1)a$ und $(-b) = (-1)b$ und verwenden $(-1)(-1) = 1$.
6. Das ist klar.
7. Das ist klar.
8. Das wird bewiesen, indem man die Brüche auf einen Hauptnenner bringt und das Distributivgesetz anwendet.
9. Das folgt durch wiederholtes Anwenden des Distributivgesetzes.

□

3.3.7. Die Frage, wie das Produkt zweier negativer Zahlen zu bilden sei, war lange umstritten. Mir scheint der vorhergehende Beweis das überzeugendste Argument für "Minus mal Minus gibt Plus": Es sagt salopp gesprochen, daß man diese Regel adoptieren muß, wenn man beim Rechnen das Ausklammern ohne alle Einschränkungen erlauben will.

Definition 3.3.8. Gegeben Mengen mit Verknüpfung $(A, \top)$ und $(B, \bot)$ verstehen wir unter einem **Homomorphismus** von A nach B eine Abbildung $\varphi : A \to B$ derart, daß gilt $\varphi(a \top a') = \varphi(a) \bot \varphi(a')$ für alle $a, a' \in A$. Sind unsere beiden Mengen mit Verknüpfung Monoide, so verstehen wir unter einem **Homomorphismus von Monoiden** einen Homomorphismus von Mengen mit Verknüpfung, der zusätzlich das neutrale Element auf das neutrale Element abbildet. Einen Monoidhomomorphismus zwischen zwei Gruppen nennen wir auch einen **Gruppenhomomorphismus**. Einen bijektiven Homomorphismus nennen wir oft auch einen **Isomorphismus**.

3.3.9. Jeder Homomorphismus φ von Mengen mit Verknüpfung zwischen zwei Gruppen ist bereits ein Gruppenhomomorphismus, bildet also das neutrale Element auf das neutrale Element ab: In der Tat folgt das aus $\varphi(e) = \varphi(e \cdot e) = \varphi(e) \cdot \varphi(e)$ durch Kürzen unmittelbar. Für einen Homomorphismus von Mengen mit Verknüpfung zwischen zwei Monoiden muß das jedoch nicht gelten, wie das Beispiel der Nullabbildung $(\mathbb{Z}, +) \to (\mathbb{Z}, \cdot)$ zeigt.

3.3.10. Den Begriff eines Isomorphismus haben wir hier etwas schlampig eingeführt: Im allgemeinen nennt man einen Homomorphismus ϕ nach II.10.1.13 einen Isomorphismus genau dann, wenn es einen Homomorphismus ψ in die Gegenrichtung gibt derart, daß beide Kompositionen $\psi \circ \phi$ und $\phi \circ \psi$ die Identität sind. In den Fällen, die uns bis auf weiteres begegnen werden, ist jedoch diese "richtige" Definition zu der oben gegebenen schlampigen Definition äquivalent. Der erste Fall, in dem das nicht mehr richtig ist, wird Ihnen in diesen Vorlesungen in **??** begegnen: Eine bijektive stetige Abbildung von topologischen Räumen muß keineswegs ein Isomorphismus von topologischen Räumen sein alias eine stetige Umkehrabbildung besitzen.

3.3.11. Die Terminologie kommt von griechisch "$\mu o \rho \varphi \eta$" für "Gestalt" oder für uns besser "Struktur" und griechisch "$o \mu o \iota \varsigma$" für "gleich, ähnlich". Auf deutsch könnte man statt Homomorphismus auch "strukturerhaltende Abbildung" sagen. Das Wort "Isomorphismus" wird analog gebildet mit griechisch "$\iota \sigma o \varsigma$" für "gleich".

Übung 3.3.12. Gegeben Gruppen H und G bezeichne

$$\mathrm{Grp}(H, G)$$

die Menge aller Gruppenhomomorphismen von H nach G. Man zeige, daß für jede Gruppe G die Vorschrift $\varphi \mapsto \varphi(1)$ eine Bijektion $\mathrm{Grp}(\mathbb{Z}, G) \xrightarrow{\sim} G$ liefert.

Ein Gruppenhomomorphismus von der additiven Gruppe der ganzen Zahlen in irgendeine weitere Gruppe ist also festgelegt und festlegbar durch das Bild von Eins. Hinweis: Man erinnere 3.2.10. Man beachte, daß die 1 nicht das neutrale Element der Gruppe $\mathbb{Z}$ meint, die hier vielmehr als additive Gruppe zu verstehen ist.

3.3.13. Dieselben Definitionen verwenden wir auch bei Mengen mit mehr als einer Verknüpfung. Zum Beispiel ist ein **Körperhomomorphismus** φ von einem Körper K in einen Körper L eine Abbildung $\varphi : K \to L$ derart, daß gilt $\varphi(a+b) = \varphi(a) + \varphi(b)$ und $\varphi(ab) = \varphi(a)\varphi(b)$ für alle $a, b \in K$ und $\varphi(1) = 1$. Die Bedingung $\varphi(1) = 1$ ist nur nötig, um den Fall der Nullabbildung auszuschließen. In anderen Worten mag man einen Körperhomomorphismus auch definieren als eine Abbildung, die sowohl für die Addition als auch für die Multiplikation ein Monoidhomomorphismus ist. Unter einem **Körperisomorphismus** verstehen wir wieder einen bijektiven Körperhomomorphismus.

Übung 3.3.14. Ist K ein Körper derart, daß es kein $x \in K$ gibt mit $x^2 = -1$, so kann man die Menge $K \times K = K^2$ zu einem Körper machen, indem man die Addition und Multiplikation definiert durch

$$\begin{array}{rcl} (a,b) + (c,d) & = & (a+c, b+d) \\ (a,b) \cdot (c,d) & = & (ac - bd, ad + bc) \end{array}$$

Die Abbildung $K \to K^2$, $a \mapsto (a,0)$ ist dann ein Körperhomomorphismus. Kürzen wir $(a,0)$ mit a ab und setzen $(0,1) = \mathrm{i}$, so gilt $\mathrm{i}^2 = -1$ und $(a,b) = a + b\,\mathrm{i}$ und die Abbildung $a + b\,\mathrm{i} \mapsto a - b\,\mathrm{i}$ ist ein Körperisomorphismus $K^2 \xrightarrow{\sim} K^2$.

3.3.15. Auf die in der vorhergehenden Übung 3.3.14 erklärte Weise können wir etwa aus dem Körper $K = \mathbb{R}$ der "reellen Zahlen", sobald wir ihn kennengelernt haben, direkt den Körper $\mathbb{C}$ der **komplexen Zahlen** konstruieren. Unser Körperisomorphismus gegeben durch die Vorschrift $a + b\,\mathrm{i} \mapsto a - b\,\mathrm{i}$ heißt in diesem Fall die **komplexe Konjugation** und wird auch $z \mapsto \bar{z}$ notiert. In II.2.1 diskutieren wir die komplexen Zahlen noch ausführlicher. Man beachte, wie mühelos das alles in der Sprache der Mengenlehre zu machen ist. Als die komplexen Zahlen erfunden wurden, gab es noch keine Mengenlehre und beim Rechnen beschränkte man sich auf das Rechnen mit "reellen" Zahlen, ja selbst das Multiplizieren zweier negativer Zahlen wurde als eine fragwürdige Operation angesehen, und das Ziehen einer Quadratwurzel aus einer negativen Zahl als eine rein imaginäre Operation. In gewisser Weise ist es das ja auch geblieben, aber die Mengenlehre liefert eben unserer Imagination eine wunderbar präzise Sprache, in der wir uns auch über imaginierte Dinge unmißverständlich austauschen können. Man kann dieselbe Konstruktion auch allgemeiner durchführen, wenn man statt -1 irgendein anderes Element eines Körpers K betrachtet, das kein Quadrat ist. Noch

allgemeinere Konstruktionen zur "Adjunktion höherer Wurzeln" oder sogar der "Adjunktion von Nullstellen polynomialer Gleichungen" können sie in der Algebra kennenlernen, vergleiche etwa III.3.4.8.

Übung 3.3.16. Ein Gruppenhomomorphismus $\varphi : G \to H$ vertauscht mit Inversenbildung, in Formeln $\varphi(a^{-1}) = (\varphi(a))^{-1}\ \forall a \in G$. Ein Körperhomomorphismus ist stets injektiv.

Teil B

Algebra

Die Bezeichnung “Algebra” kommt von arabisch “al-jabr”, das in der Medizin das Wiedereinrenken eines Gelenks bezeichnete und in der Mathematik für eine Umformung stand, die man heute das “Herüberschaffen durch Subtraktion” eines Terms von der einen auf die andere Seite einer Gleichung nennen würde. In diesem Zusammenhang wurde wohl auch das Rechnen mit negativen Zahlen entwickelt.

Kapitel II

Lineare Algebra

Der im folgenden vorgestellte Teil der Algebra heißt “linear” , da das einfachste der darin untersuchten Gleichungssysteme dem geometrischen Problem entspricht, den Schnittpunkt zweier Geraden alias Linien zu bestimmen. Ich habe mir bei der Darstellung die größte Mühe gegeben, die abstrakte Sprache der Mengenlehre und unsere räumliche Anschauung zu einer Einheit zu fügen, ohne dabei die algorithmischen Aspekte zu kurz kommen zu lassen. Für Korrekturen und Verbesserungen danke ich Ulrich Derenthal und Veronika Thierfelder, deren fundamentale allgemeine Ratschläge zur Darstellung mir sehr geholfen haben.

Inhalt

1 Gleichungssysteme und Vektorräume

1.1 Lösen linearer Gleichungssysteme

1.1.1. Sei k ein Körper im Sinne von I.3.3.1. Ich rate, sich hier zunächst einmal den Körper $k = \mathbb{Q}$ der rationalen Zahlen oder den Körper $k = \mathbb{R}$ der reellen Zahlen zu denken. Gegeben seien n Gleichungen in m Unbekannten in der Form

$$\begin{array}{rcl} a_{11}x_1 + a_{12}x_2 + & \dots & + a_{1m}x_m = b_1 \\ a_{21}x_1 + a_{22}x_2 + & \dots & + a_{2m}x_m = b_2 \\ \vdots & & \vdots \\ a_{n1}x_1 + a_{n2}x_2 + & \dots & + a_{nm}x_m = b_n \end{array}$$

mit $a_{ij}, b_i \in k$ fest vorgegeben und x_j gesucht. Man spricht dann auch von einem **linearen Gleichungssystem**. Linear heißt es, weil darin keine komplizierteren Terme wie x_1^2 oder $x_1x_2^7$ vorkommen. Sind alle b_i auf der rechten Seite unserer Gleichungen Null, so heißt unser System **homogen**. Das lineare Gleichungssystem, das aus einem inhomogenen System entsteht, indem man alle b_i zu Null setzt, heißt das zugehörige **homogenisierte** Gleichungssystem. Gesucht ist eine Beschreibung aller m-Tupel $(x_1, \dots, x_m)$ von Elementen von k derart, daß alle n Gleichungen gleichzeitig erfüllt sind. In der Begrifflichkeit und Notation, wie wir sie gleich in 1.2.2 einführen, bildet die Gesamtheit aller m-Tupel $(x_1, \dots, x_m)$ von Elementen von k eine neue Menge k^m, und wir suchen eine möglichst explizite Beschreibung der Teilmenge $L \subset k^m$ aller derjenigen m-Tupel, die alle unsere n Gleichungen erfüllen, der sogenannten **Lösungsmenge** unseres Gleichungssystems.

Ergänzung 1.1.2. In obigem Gleichungssystem ist a_{12} nicht als a-Zwölf zu verstehen, sondern als a-Eins-Zwei. Sicher wäre es präziser gewesen, stets die beiden Bestandteile unserer Doppelindizes durch ein Komma zu trennen und $a_{1,2}$ und dergleichen zu schreiben, aber das hätte unser Gleichungssystem dann auch wieder weniger übersichtlich gemacht. Man muß eben beim Schreiben und Verstehen von Mathematik immer einen Mittelweg zwischen einer präzisen aber unübersichtlichen und einer übersichtlichen aber unpräzisen Darstellung wählen, und an dieser Stelle schien mir das Weglassen der Kommata der bessere Weg. Insbesondere in der Physik ist es üblich, einen der Indizes hochzustellen, also a_1^2 und dergleichen zu schreiben, aber das kann auch wieder als das Quadrat $(a_1)^2$ von a_1 mißverstanden werden.

1.1.3. Um die Lösungsmenge eines linearen Gleichungssystems zu bestimmen, kann man den **Gauß-Algorithmus** anwenden. Er basiert auf der elementaren Erkenntnis, daß sich die Lösungsmenge nicht ändert, wenn wir in einer der beiden folgenden Weisen zu einem neuen Gleichungssystem übergehen:

SkriptenBilder/BildZstF.png

Ein System in Zeilenstufenform ist ein System der obigen Gestalt, bei dem im Teil mit den Koeffizienten a_{ij} wie angedeutet unterhalb solch einer "Treppe mit der Stufenhöhe Eins aber mit variabler Breite der Stufen" nur Nullen stehen, vorn an den Stufenabsätzen aber von Null verschiedene Einträge. An die durch den senkrechten Strich abgetrennte letzte Spalte mit den gewünschten Ergebnissen b_i werden hierbei keinerlei Bedingungen gestellt.

1. Wir ersetzen eine unserer Gleichungen durch ihre Summe mit einem Vielfachen einer anderen unserer Gleichungen;

2. Wir vertauschen zwei unserer Gleichungen.

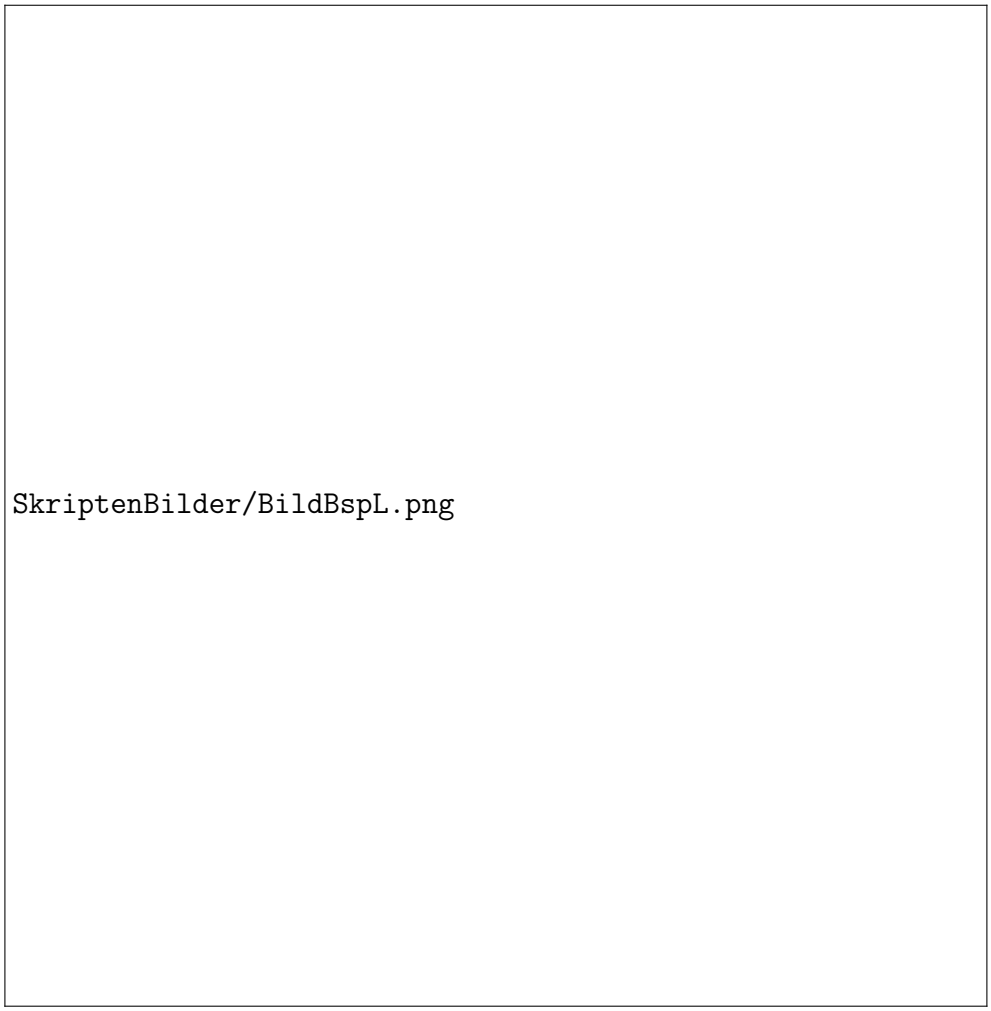
Der noch zu besprechende Gauß-Algorithmus beschreibt, wie wir mithilfe dieser beiden Operationen, also ohne die Lösungsmenge zu ändern, zu einem Gleichungssystem übergehen können, das **Zeilenstufenform** hat. Nebenstehendes Bild mag aufschlüsseln, was das anschaulich bedeuten soll. Formal sagen wir, ein Gleichungssystem sei "in Zeilenstufenform", genau dann, wenn man ein $r \geq 0$ und Indizes $1 \leq s(1) < s(2) < \ldots < s(r) \leq m$ so angeben kann, daß in unserem Gleichungssystem gilt $a_{i,s(i)} \neq 0$ für $1 \leq i \leq r$ und daß $a_{\nu\mu} \neq 0$ nur gelten kann, wenn es ein i gibt mit $\nu \leq i$ und $\mu \geq s(i)$. Es ist üblich und erspart viel Schreibarbeit, die Symbole x_j sowie die Pluszeichen und Gleichheitszeichen bei Rechnungen im Zusammenhang mit linearen Gleichungssystemen wegzulassen und stattdessen ein Gleichungssystem der oben beschriebenen Art abzukürzen durch seine **erweiterte Koeffizientenmatrix**

$$\left(\begin{array}{cccc|c} a_{11} & a_{12} & \ldots & a_{1m} & b_1 \\ a_{21} & a_{22} & & a_{2m} & b_2 \\ \vdots & & & \vdots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nm} & b_n \end{array}\right)$$

Die Spezifikation "erweitert" weist auf die letzte Spalte der b_i hin. Die Familie der a_{ij} für sich genommen heißt die **Koeffizientenmatrix** unseres Gleichungssystems.

1.1.4 (**Gauß-Algorithmus**). Der Gauß-Algorithmus zum Bestimmen der Lösungsmenge eines linearen Gleichungssystems funktioniert so: Sind alle Koeffizienten in der ersten Spalte Null, so ignorieren wir die erste Spalte und machen mit der auf diese Weise entstehenden Matrix weiter. Ist ein Koeffizient in der ersten Spalte von Null verschieden, so bringen wir ihn durch eine Zeilenvertauschung an die oberste Stelle. Ziehen wir dann geeignete Vielfache der ersten Zeile von den anderen Zeilen ab, so gelangen wir zu einem System, bei dem wie angedeutet in der ersten Spalte unterhalb des obersten Eintrags nur Nullen stehen. Für das weitere ignorieren wir dann die erste Zeile und die erste Spalte und machen mit der auf diese Weise entstehenden Matrix weiter. Offensichtlich können wir so jedes lineare Gleichungssystem auf Zeilenstufenform bringen, ohne seine Lösungsmenge zu ändern.

1.1.5. Die Lösungsmenge eines linearen Gleichungssystems in Zeilenstufenform ist schnell bestimmt: Ist eine der Zahlen $b_{r+1}, \ldots, b_n$ nicht Null, so besitzt es gar keine Lösung. Gilt dahingegen $b_{r+1} = \ldots = b_n = 0$, können wir Zahlen x_μ



Ein lineares Gleichungssystem mit drei Gleichungen und drei Unbekannten und seine Lösung mit dem Gauß-Algorithmus. Für gewöhnlich wird beim Anwenden des Gauß-Algorithmus ein Vertauschen der Zeilen gar nicht nötig sein. Gibt es weiter genausoviele Gleichungen wie Unbekannte, so werden wir für gewöhnlich so wie in obigem Beispiel genau eine Lösung erwarten dürfen.

für μ verschieden von den Spaltenindizes $s(1), \ldots, s(r)$ der Stufen beliebig vorgeben und finden für jede solche Vorgabe der Reihe nach eindeutig bestimmte $x_{s(r)}, x_{s(r-1)}, \ldots, x_{s(1)}$ derart, daß das entstehende m-Tupel $(x_1, \ldots, x_m)$ eine Lösung unseres Gleichungssystems ist.

1.1.6. Eine Abbildung der Produktmenge $\{1, \ldots, n\} \times \{1, \ldots, m\}$ in eine Menge Z heißt ganz allgemein eine $(n \times m)$**-Matrix mit Koeffizienten in** Z. Gegeben solch eine Matrix A schreibt man meist A_{ij} oder a_{ij} statt $A(i,j)$ und veranschaulicht sich dieses Datum als ein rechteckiges Arrangement von Elementen von Z wie eben im Fall $Z = k$. Das i heißt hierbei der **Zeilenindex**, da es angibt alias "indiziert", in welcher Zeile unser Eintrag a_{ij} steht, wohingegen man das j den **Spaltenindex** unseres Matrixeintrags nennt. Die Menge aller $(n \times m)$-Matrizen mit Koeffizienten in Z notieren wir

$$\mathrm{M}(n \times m; Z) := \mathrm{Ens}(\{1, \ldots, n\} \times \{1, \ldots, m\}, Z)$$

Im Fall $n = m$ sprechen wir von einer **quadratischen Matrix**. Manchmal werden wir sogar für beliebige Mengen X, Y, Z eine Abbildung $X \times Y \to Z$ als eine $(X \times Y)$**-Matrix mit Koeffizienten in** Z ansprechen.

Satz 1.1.7 (Lösungen inhomogener linearer Gleichungssysteme). *Ist die Lösungsmenge eines linearen Gleichungssystems nicht leer, so erhalten wir alle Lösungen, indem wir zu einer fest gewählten Lösung unseres Systems eine beliebige Lösung des zugehörigen homogenisierten Systems komponentenweise addieren.*

Beweis. Ist $c = (c_1, \ldots, c_m)$ eine Lösung unseres linearen Gleichungssystems und $d = (d_1, \ldots, d_m)$ eine Lösung des homogenisierten Systems, so ist offensichtlich die komponentenweise Summe $c \dot{+} d = (c_1 + d_1, \ldots, c_m + d_m)$ eine Lösung des ursprünglichen Systems. Ist andererseits $c' = (c'_1, \ldots, c'_m)$ eine weitere Lösung unseres linearen Gleichungssystems, so ist offensichtlich die komponentenweise Differenz $d = (c'_1 - c_1, \ldots, c'_m - c_m)$ eine Lösung des homogenisierten Systems, für die gilt $c' = c \dot{+} d$ mit unserer komponentenweisen Addition $\dot{+}$ aus I.1.2.7. □

1.1.8. Die vorstehenden Überlegungen zeigen, wie man die Lösungsmenge jedes linearen Gleichungssystems bestimmen kann. Man erhält dabei nach 1.1.5 im Fall einer nichtleeren Lösungsmenge durch die Transformation in Zeilenstufenform sogar eine ausgezeichnete Bijektion zwischen t-Tupeln von Elementen von k und besagter Lösungsmenge, für $t = m - r$ die Zahl der Variablen abzüglich der "Zahl der Stufen", die eben jeder Vorgabe von x_j für j verschieden von den "Spaltenindizes der Stufen" $j \neq s(1), \ldots, s(r)$ die durch diese Vorgabe eindeutig bestimmte Lösung zuordnet. Der Gauß-Algorithmus gibt uns allerdings nicht vor, welche Zeilenvertauschungen wir unterwegs verwenden sollen. Damit stellt sich

Ein lineares Gleichungssystem mit zwei Gleichungen und drei Unbekannten, dessen Lösungsmenge nach unser allgemeinen Theorie für jedes x_3 genau einen Punkt (x_1, x_2, x_3) enthält, und zwar haben wir wegen der zweiten Gleichung $x_2 = x_3/4$ und dann wegen der ersten Gleichung $x_1 = 1 - (3/4)x_3$, so daß die allgemeine Lösung lautet $(1 - (3/4)\lambda, \lambda/4, \lambda)$ für variables λ.

sofort die Frage, ob wir unabhängig von der Wahl dieser Zeilenvertauschungen stets bei derselben Matrix in Zeilenstufenform ankommen. Das ist nun zwar nicht richtig, aber dennoch sind die "Breiten der einzelnen Stufen" alias die Spaltenindizes $s(i)$ der Stufen unabhängig von allen Wahlen. In der Tat lassen sie sich auch direkt beschreiben, indem wir im zugehörigen homogenisierten Gleichungssystem unsere Variablen von hinten durchgehen und jeweils fragen: Gibt es für jedes $(x_{j+1}, x_{j+2}, \ldots, x_m)$, das zu einer Lösung $(x_1, x_2, \ldots, x_m)$ ergänzbar ist, nur ein x_j derart, daß auch $(x_j, x_{j+1}, x_{j+2}, \ldots, x_m)$ zu einer Lösung $(x_1, x_2, \ldots, x_m)$ ergänzbar ist? Genau dann lautet die Antwort "ja", wenn in der j-ten Spalte eine neue Stufe beginnt.

1.1.9. Nun könnten wir natürlich auch vor dem Anwenden des Gauß-Algorithmus zuerst unsere Variablen umnummerieren alias die Spalten unserer Koeffizientenmatrix vertauschen. Wir erhielten wieder eine Bijektion eines k^u mit der Lösungsmenge wie eben. Die Frage, der wir uns als nächstes zuwenden wollen, lautet nun: Gilt stets $u = t$, in anderen Worten, landen wir bei einer Zeilenstufenform mit derselben Zahl von Stufen, wenn wir zuerst die Spalten unseres Systems willkürlich vertauschen, bevor wir den Gauß-Algorithmus durchführen? Die Antwort lautet wieder "Ja", aber hierzu ist mir kein ganz elementares Argument mehr eingefallen, und darüber war ich sogar ganz froh: Diese Frage kann so nämlich zur Motivation der Entwicklung der abstrakten Theorie der Vektorräume dienen, mit der wir an dieser Stelle beginnen. Wir führen in diesem Rahmen den auch in vielen anderen Zusammenhängen äußerst nützlichen Begriff der "Dimension" eines "Vektorraums" ein, und zeigen in 1.5.11, daß die Stufenzahl unabhängig von allen Wahlen als die "Dimension des Lösungsraums" des zugehörigen homogenisierten Gleichungssystems beschrieben werden kann. Zunächst jedoch führen wir weitere Begriffe der Mengenlehre ein, die wir dabei und auch darüber hinaus noch oft brauchen werden.

1.2 Ergänzungen zur Mengenlehre

1.2.1. Bis jetzt hatten wir nur das kartesische Produkt $X \times Y$ von zwei Mengen X und Y betrachtet. Ebenso kann man jedoch auch für Mengen $X_1, \ldots, X_n$ das kartesische Produkt

$$X_1 \times \ldots \times X_n = \{(x_1, \ldots, x_n) \mid x_i \in X_i \text{ für } 1 \leq i \leq n\}$$

einführen. Die Elemente von so einem Produkt bezeichnet man als n**-Tupel**.

1.2.2. Gegeben drei Mengen X, Y, Z kann man sich natürlich die Frage stellen, inwieweit die drei Mengen $(X \times Y) \times Z$, $X \times (Y \times Z)$ und $X \times Y \times Z$ übereinstimmen und auch allgemeiner, inwieweit "das kartesische Produkt $\times$ assoziativ ist". Wir werden derartige Fragen später im Rahmen der Kategorientheorie ausführlich

diskutieren. Hier sei nur bemerkt, daß zum Beispiel alle unsere drei Tripelprodukte jedenfalls wohlbestimme Projektionen $\mathrm{pr}_X, \mathrm{pr}_Y$ und pr_Z auf X, Y und Z haben und daß es eindeutig bestimmte Bijektionen zwischen ihnen gibt, die mit diesen drei Projektionen verträglich sind. Wir werden derartige Bijektionen meist nicht explizit machen. Es ist auch sinnvoll und allgemeine Konvention, das Produkt von Null Mengen als "die" einelementige Menge zu verstehen. Das kartesische Produkt von n Kopien einer Menge X kürzt man meist mit

$$X^n$$

ab, die Elemente von X^n sind also n-Tupel von Elementen aus X und X^0 besteht aus genau einem Element, so daß wir für alle $n, m \geq 0$ eine kanonische Bijektion $X^n \times X^m \xrightarrow{\sim} X^{n+m}$ haben. Manchmal schreibe ich statt X^n auch ausführlicher $X^{\times n}$, insbesondere dann, wenn ich Verwechslungen mit anderen Notationen befürchte, die Sie noch kennenlernen werden.

1.2.3. Für ein kartesisches Produkt hat man stets die **Projektionsabbildungen** oder **Projektionen**

$$\begin{array}{rccc} \mathrm{pr}_i : & X_1 \times \ldots \times X_n & \to & X_i \\ & (x_1, \ldots, x_n) & \mapsto & x_i \end{array}$$

Wir erhalten dann für jede weitere Menge Z eine Bijektion

$$\begin{array}{ccc} \mathrm{Ens}(Z, X_1 \times \ldots \times X_n) & \xrightarrow{\sim} & \mathrm{Ens}(Z, X_1) \times \ldots \times \mathrm{Ens}(Z, X_n) \\ f & \mapsto & (\mathrm{pr}_1 \circ f, \ldots, \mathrm{pr}_n \circ f) \end{array}$$

Die Umkehrung dieser Bijektion notieren wir sozusagen gar nicht: Gegeben Abbildungen $f_i : Z \to X_i$ notieren wir die Abbildung $f : Z \to X_1 \times \ldots \times X_n$ von Z in das kartesische Produkt der X_i gegeben durch die Vorschrift $z \mapsto (f_1(z), \ldots, f_n(z))$ schlicht $f = (f_1, \ldots, f_n)$. In der exponentiellen Schreibweise geschrieben liest sich unsere Bijektion ganz suggestiv als eine kanonische Bijektion $(X_1 \times \ldots \times X_n)^Z \xrightarrow{\sim} X_1^Z \times \ldots \times X_n^Z$. Besonders wichtig ist die **diagonale Einbettung** oder **Diagonale**

$$\begin{array}{rccc} \Delta := \Delta_X := (\mathrm{id}, \mathrm{id}) : & X & \to & X \times X \\ & x & \mapsto & (x, x) \end{array}$$

1.2.4. Ist ein weiteres Produkt von der Form $Y = Y_1 \times \ldots \times Y_n$ gegeben sowie Abbildungen $f_i : X_i \to Y_i$, so können wir auch die Abbildung

$$\begin{array}{ccc} X_1 \times \ldots \times X_n & \to & Y_1 \times \ldots \times Y_n \\ (x_1, \ldots, x_n) & \mapsto & (f_1(x_1), \ldots, f_n(x_n)) \end{array}$$

erklären. Wir notieren diese Abbildung $f_1 \times \cdots \times f_n$. Man beachte jedoch, daß keineswegs alle Abbildungen $X_1 \times \ldots \times X_n \to Y_1 \times \cdots \times Y_n$ von dieser Form

sind. Man beachte allgemeiner, daß eine Abbildung $f : X_1 \times \ldots \times X_n \to Z$ von einem kartesischen Produkt in eine beliebige Menge Z sich keineswegs in ähnlicher Weise aus Abbildungen $X_i \to Z$ zusammensetzen läßt, wie wir das bei Abbildungen von einer beliebigen Menge in ein kartesisches Produkt gesehen hatten.

Definition 1.2.5. Gegeben eine Menge X erinnere ich an die Menge aller Teilmengen $\mathcal{P}(X) = \{U \mid U \subset X\}$ von X, die sogenannte **Potenzmenge** von X. Da es mich verwirrt, über Mengen von Mengen zu reden, werde ich Teilmengen von $\mathcal{P}(X)$ nach Möglichkeit als **Systeme von Teilmengen von** X ansprechen. Gegeben ein solches Mengensystem $\mathcal{U} \subset \mathcal{P}(X)$ bildet man zwei neue Teilmengen von X, den **Schnitt** und die **Vereinigung** der Mengen aus unserem System $\mathcal{U}$, durch die Vorschrift

$$\begin{aligned} \textstyle\bigcup_{U\in\mathcal{U}} U &= \{x \in X \mid \text{Es gibt } U \in \mathcal{U} \text{ mit } x \in U\} \\ \textstyle\bigcap_{U\in\mathcal{U}} U &= \{x \in X \mid \text{Für alle } U \in \mathcal{U} \text{ gilt } x \in U\} \end{aligned}$$

Insbesondere ist der Schnitt über das leere System von Teilmengen von X ganz X und die Vereinigung über das leere System von Teilmengen von X die leere Menge.

1.2.6. Wir würden nun gerne zum Beispiel die Erkenntnis, daß das Komplement eines derartigen Schnitts die Vereinigung der Komplemente ist, ausdrücken können in der Formel

$$X \setminus \left(\bigcap_{U\in\mathcal{U}} U \right) = \bigcup_{U\in\mathcal{U}} (X \setminus U)$$

Damit in dieser Formel auch die Bedeutung der rechten Seite unmißverständlich klar ist, führen wir weitere Notationen ein.

1.2.7. Gegeben Mengen A und I bezeichnet man eine Abbildung $I \to A$ ganz allgemein auch als eine **durch** I **indizierte Familie von Elementen von** A und benutzt die Notation

$$(a_i)_{i\in I}$$

Diese Sprechweise und Notation für Abbildungen verwendet man insbesondere dann, wenn man der Menge I eine untergeordnete Rolle zugedacht hat. Im Fall $I = \emptyset$ spricht man von der **leeren Familie** von Elementen von A.

Definition 1.2.8. Gegeben eine Familie $(X_i)_{i\in I}$ von Teilmengen einer Menge X erklärt man ihren **Schnitt** und ihre **Vereinigung** durch die Regeln

$$\begin{aligned} \textstyle\bigcap_{i\in I} X_i &= \{x \in X \mid \text{Für alle } i \in I \text{ gilt } x \in X_i\} \\ \textstyle\bigcup_{i\in I} X_i &= \{x \in X \mid \text{Es existiert ein } i \in I \text{ mit } x \in X_i\} \end{aligned}$$

Insbesondere ist der Schnitt über die leere Familie von Teilmengen von X ganz X und die Vereinigung über die leere Familie von Teilmengen von X ist die leere Menge.

Ergänzende Übung 1.2.9. Man verallgemeinere die Formeln aus I.2.1.15 auf diese Situation. Genauer schreibe man in Formeln und zeige, daß der Schnitt einer derartigen Vereinigung mit einer weiteren Menge die Vereinigung der Schnitte ist, die Vereinigung eines derartigen Schnitts mit einer weiteren Menge der Schnitt der Vereinigungen, das Komplement eines Schnitts die Vereinigung der Komplemente und das Komplement einer Vereinigung der Schnitt der Komplemente. Besonders Mutige versuchen, für eine durch ein Produkt indizierte Familie $(X_{ij})_{(i,j)\in I\times J}$ den Schnitt von Vereinigungen $\bigcap_{j\in J}\left(\bigcup_{i\in I} X_{ij}\right)$ als Vereinigung von Schnitten zu schreiben.

1.2.10. In 6.2 diskutieren wir allgemeiner Produkte und zusätzlich "disjunkte Vereinigungen" beliebiger nicht notwendig endlicher Mengensysteme.

1.3 Vektorräume und Untervektorräume

Definition 1.3.1. Ein **Vektorraum** V **über einem Körper** k ist ein Paar bestehend aus einer abelschen Gruppe $V = (V, \dot{+})$ und einer Abbildung

$$\begin{array}{ccc} k \times V & \to & V \\ (\lambda, \vec{v}) & \mapsto & \lambda\vec{v} \end{array}$$

derart, daß für alle $\lambda, \mu \in k$ und $\vec{v}, \vec{w} \in V$ die folgenden Identitäten gelten:

$$\begin{array}{rcl} \lambda(\vec{v} \dot{+} \vec{w}) & = & (\lambda\vec{v}) \dot{+} (\lambda\vec{w}) \\ (\lambda + \mu)\vec{v} & = & (\lambda\vec{v}) \dot{+} (\mu\vec{v}) \\ \lambda(\mu\vec{v}) & = & (\lambda\mu)\vec{v} \\ 1\vec{v} & = & \vec{v} \end{array}$$

In Analogie zu der Sprechweise bei der Axiomatik eines Körpers I.3.3.1 heißen die ersten beiden Gesetze die beiden **Distributivgesetze**. In Analogie zu der Sprechweise bei Mengen mit Verknüpfung heißt das dritte Gesetz wieder das **Assoziativgesetz**.

1.3.2. Die Elemente eines Vektorraums nennt man meist die **Vektoren** des Vektorraums. Die Elemente des Körpers heißen in diesem Zusammenhang oft **Skalare** und die Abbildung $(\lambda, \vec{v}) \mapsto \lambda\vec{v}$ die **Multiplikation mit Skalaren** und ist nicht zu verwechseln mit dem "Skalarprodukt", das wir in 4.1.6 einführen und das aus zwei Vektoren einen Skalar macht. Ich habe oben aus didaktischen Gründen die Addition von Vektoren $\dot{+}$ notiert, um sie von der Addition von Körperelementen

zu unterscheiden, aber das werde ich nicht lange durchhalten. Mit der auch in diesem Zusammenhang allgemein üblichen Konvention "Punkt vor Strich" und der zu $+$ vereinfachten Notation für die Addition von Vektoren lauten unsere Vektorraumaxiome dann etwas übersichtlicher

$$\begin{array}{rcl} \lambda(\vec{v}+\vec{w}) & = & \lambda\vec{v}+\lambda\vec{w} \\ (\lambda+\mu)\vec{v} & = & \lambda\vec{v}+\mu\vec{v} \\ \lambda(\mu\vec{v}) & = & (\lambda\mu)\vec{v} \\ 1\vec{v} & = & \vec{v} \end{array}$$

Ich habe aus didaktischen Gründen bis hierher Vektoren stets mit einem Pfeil notiert, das halte ich wohl etwas länger durch, aber auf Dauer werden Sie sich den Pfeil auch selbst dazudenken müssen. Das neutrale Element der abelschen Gruppe V notieren wir $\vec{0}$ und nennen es den **Nullvektor**. Die letzte Bedingung $1\vec{v} = \vec{v}$ schließt zum Beispiel den Fall aus, daß wir für V irgendeine von Null verschiedene abelsche Gruppe nehmen und dann einfach setzen $\lambda\vec{v} = \vec{0}$ für alle $\lambda \in k$ und $\vec{v} \in V$.

Ergänzung 1.3.3. Die Bezeichnung "Vektor" kommt von lateinisch "vehere" für "fahren, transportieren", und rührt von unserem Beispiel I.1.2.5 der Gesamtheit aller Parallelverschiebungen der Ebene oder des Raums her, deren Elemente ja in gewisser Weise Punkte transportieren. Auf Deutsch könnte man, um diese Intuition wiederzugeben, statt von Vektoren etwa von "Schiebern" reden. Beim Gedanken an eine Vorlesung über die "Lehre von der Schieberei" bin ich aber doch wieder glücklicher mit der gewohnten, vom Latein geprägten Terminologie. Die Bezeichnung "Skalare" für Elemente des zugrundeliegenden Körpers kommt von dem lateinischen Wort "scala" für "Leiter" und hat sich von dort über das Metermaß entwickelt zu einer Bezeichnung für das, was man auf einer Meßskala ablesen kann, als da heißt zu einer Bezeichnung für reelle Zahlen. In der Mathematik werden nun aber nicht nur reelle Vektorräume betrachtet, und so überträgt man dann dieses Wort weiter und verwendet es auch im allgemeinen als Bezeichnung für die Elemente des zugrundeliegenden Körpers.

1.3.4. Gegeben ein Vektorraum V und ein Vektor $\vec{v} \in V$ gilt $0\vec{v} = \vec{0}$. In der Tat finden wir mit der zweiten Formel aus der Definition $0\vec{v} = (0+0)\vec{v} = 0\vec{v} \dot{+} 0\vec{v}$ und Subtraktion von $0\vec{v}$ auf beiden Seiten liefert $\vec{0} = 0\vec{v}$, in Worten "Null mal ein Vektor ist stets der Nullvektor".

1.3.5. Gegeben ein Vektorraum V und ein Vektor $\vec{v} \in V$ gilt $(-1)\vec{v} = -\vec{v}$, das Negative von $\vec{v}$ in der abelschen Gruppe V. In der Tat finden wir mit der letzten und der zweiten Formel aus der Definition $\vec{v} \dot{+} (-1)\vec{v} = 1\vec{v} + (-1)\vec{v} = (1+(-1))\vec{v} = 0\vec{v} = \vec{0}$ und damit ist $(-1)\vec{v}$ in der Tat das additive Inverse von $\vec{v}$, in Formeln $(-1)\vec{v} = -\vec{v}$.

Ergänzende Übung 1.3.6. Gegeben ein Vektorraum V über einem Körper k zeige man für alle $\lambda \in k$ die Identität $\lambda\vec{0} = \vec{0}$. Weiter zeige man, daß aus $\lambda\vec{v} = \vec{0}$ folgt $\lambda = 0$ oder $\vec{v} = \vec{0}$.

Weiterführende Übung 1.3.7. Eine vorgegebene abelsche Gruppe kann auf höchstens eine Weise mit der Struktur eines $\mathbb{Q}$-Vektorraums versehen werden.

Beispiele 1.3.8. Einige Beispiele für Vektorräume wurden bereits in I.1.2 diskutiert. Besonders wichtig ist das Beispiel des Vektorraums

$$V = k^n$$

über einem vorgegebenen Körper k. Hier verwenden wir die Notation 1.2.2, die Elemente von k^n sind also n-Tupel von Elementen des Körpers k. Die Operationen seien gegeben durch

$$\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \dot{+} \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} := \begin{pmatrix} v_1 + w_1 \\ \vdots \\ v_n + w_n \end{pmatrix}$$

$$\lambda \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} := \begin{pmatrix} \lambda v_1 \\ \vdots \\ \lambda v_n \end{pmatrix}$$

für $\lambda, v_1, \ldots, v_n, w_1, \ldots, w_n \in k$. Wir haben unsere n-Tupel hier der Übersichtlichkeit halber untereinander geschrieben. Die erste dieser Gleichungen definiert die Summe zweier n-Tupel, also die Addition in unserem Vektorraum $V = k^n$, indem sie diese durch die Addition in k ausdrückt. Die zweite Gleichung leistet dasselbe für die Multiplikation mit Skalaren. Ich gebe nun einen ersten Teil meiner didaktischen Notation auf und schreibe von hier an $+$ statt $\dot{+}$. Gegeben $\vec{v} \in k^n$ schreibe ich seine Komponenten $v_1, v_2, \ldots, v_n$ und versehe sie nicht mit Pfeilen, da sie ja Elemente des Grundkörpers sind. Wenn irgendwo einmal $\vec{v}_1, \vec{v}_2, \ldots, \vec{v}_n$ stehen sollte, so sind nicht die n Komponenten eines n-Tupels $\vec{v}$ gemeint, sondern vielmehr n Vektoren eines Vektorraums. Sobald ich die Pfeil-Notation auch aufgegeben haben werde, muß der Leser aus dem Kontext erschließen, was jeweils gemeint ist.

Beispiel 1.3.9. Gegeben ein Körper k wird jede einelementige Menge V vermittels der offensichtlichen Operation zu einem k-Vektorraum. Wir sprechen dann von einem **Nullvektorraum**, weil er eben nur aus dem Nullvektor besteht, und verwenden oft auch den bestimmten Artikel und sprechen von *dem* Nullvektorraum, da er ja "im Wesentlichen" eindeutig bestimmt ist.

Übung 1.3.10. Gegeben ein Körper k und k-Vektorräume $V_1, \ldots, V_n$ können wir das kartesische Produkt $V_1 \times \ldots \times V_n$ zu einem k-Vektorraum machen, indem wir die Addition sowie die Multiplikation mit Skalaren komponentenweise definieren. In Formeln sieht das dann so aus wie 1.3.8, nur daß wir den v_i und w_i Pfeile aufsetzen und statt $v_i, w_i \in k$ wie dort nun $\vec{v}_i, \vec{w}_i \in V_i$ nehmen müssen. Den so entstehenden Vektorraum notieren wir auch

$$V_1 \oplus \ldots \oplus V_n$$

und nennen ihn die **direkte Summe** oder noch genauer die **externe direkte Summe**, wenn wir sie von der in 1.5.20 diskutierten "internen Summe von Untervektorräumen" abgrenzen wollen. Insbesondere ist also k^n sozusagen dasselbe wie die externe direkte Summe $k \oplus \ldots \oplus k$ von n Kopien des k-Vektorraums k.

Ergänzende Übung 1.3.11. Gegeben Gruppen G, H können wir das kartesische Produkt $G \times H$ zu einer Gruppe machen, indem wir darauf die komponentenweise Verknüpfung $(g, h)(g', h') = (gg', hh')$ betrachten. Analog versehen wir auch das Produkt einer beliebigen Familie von Gruppen mit der Struktur einer Gruppe.

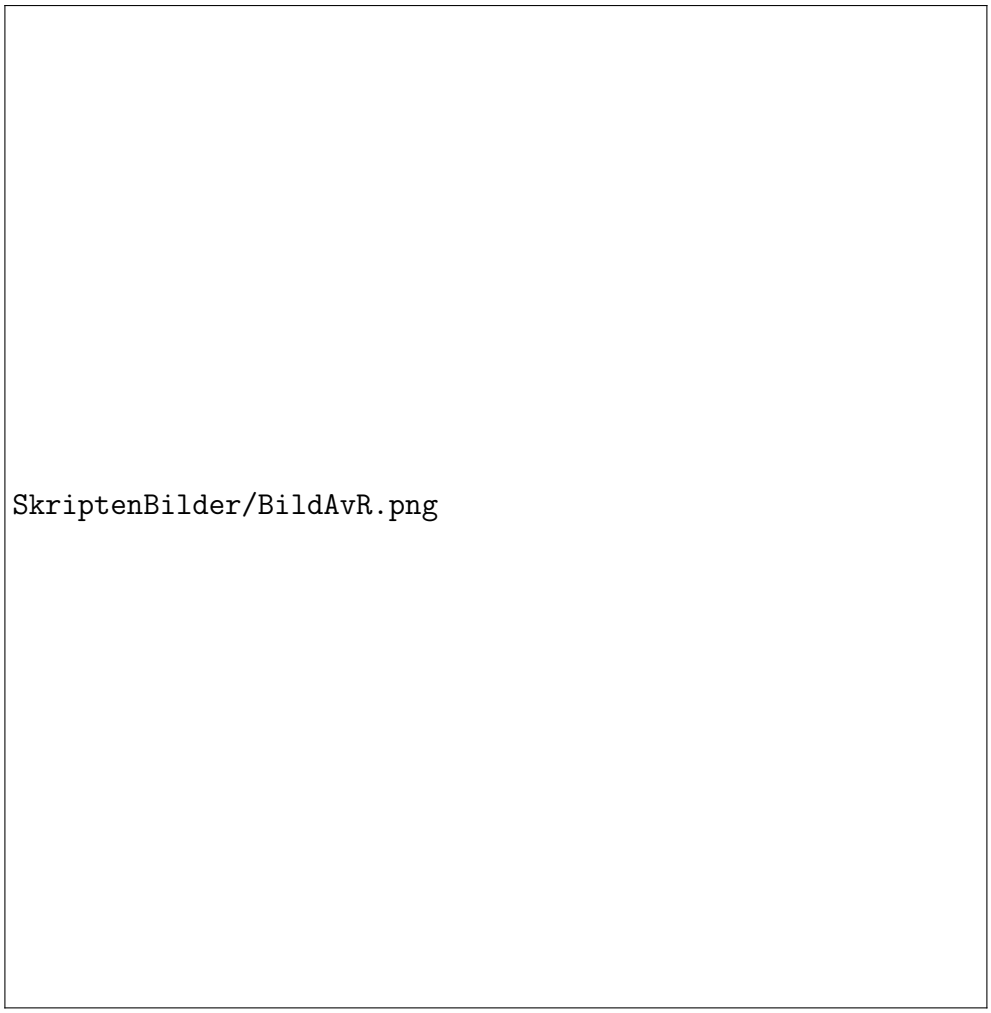
Definition 1.3.12. Eine Teilmenge U eines Vektorraums V heißt ein **Untervektorraum** oder **Teilraum** genau dann, wenn U den Nullvektor enthält und wenn aus $\vec{u}, \vec{v} \in U$ und $\lambda \in k$ folgt $\vec{u} + \vec{v} \in U$ sowie $\lambda\vec{u} \in U$.

Ergänzung 1.3.13. Die vom höheren Standpunkt aus "richtige" Definition eines Untervektorraums lautet eigentlich anders, und zwar so: Sei k ein Körper. Eine Teilmenge eines k-Vektorraums heißt ein Untervektorraum genau dann, wenn sie so mit der Struktur eines k-Vektorraums versehen werden kann, daß die Einbettung ein "Homomorphismus k-Vektorräumen" wird. Ich kann diese "bessere" Definition hier noch nicht geben, da wir Homomorphismen von k-Vektorräumen noch gar nicht kennengelernt haben. Sie scheint mir deshalb besser, da man in derselben Weise auch korrekte Definitionen von Untermonoiden, Untergruppen, Unterkörpern und Unter-was-nicht-noch-all-für-Strukturen erhält, die Sie erst später kennenlernen werden.

Beispiel 1.3.14. Unter einem homogenen linearen Gleichungssystem über einem gegebenen Körper k versteht man, wie bereits erwähnt, ein System von Gleichungen der Gestalt

$$\begin{array}{rcl} a_{11}x_1 + a_{12}x_2 + & \ldots & + a_{1m}x_m = 0 \\ a_{21}x_1 + a_{22}x_2 + & \ldots & + a_{2m}x_m = 0 \\ \vdots & & \vdots \\ a_{n1}x_1 + a_{n2}x_2 + & \ldots & + a_{nm}x_m = 0 \end{array}$$

bei dem also rechts nur Nullen stehen. Die Lösungsmenge eines solchen homogenenen Gleichungssystems ist offensichtlich ein Untervektorraum $L \subset k^m$.



Visualisierung eines Vektorraums ähnlich wie in 1.3.15 erläutert: Hier denke ich mir die Papierebene mit einem festen ausgezeichneten Punkt als Vektorraum. Die Elemente des Vektorraums entsprechen dann den Punkten der Papierebene, werden jedoch als Pfeile von unserem ausgewählten fetten Punkt zu besagtem Punkt der Papierebene gezeichnet.

Beispiel 1.3.15. Ich selber denke mir einen reellen Vektorraum meist als den "Raum der Anschauung" zusammen mit einem ausgezeichneten festen Punkt, obwohl a priori eher zweifelhaft ist, ob es sich bei den Punkten des "Raums unserer Anschauung" auch wirklich um im Cantor'schen Sinne "wohlunterschiedene Objekte unseres Denkens oder unserer Anschauung" handelt. Genauer denke ich mir Vektoren als Pfeile von besagtem festen Punkt zu irgendeinem anderen Punkt. Die Summe zweier solcher Pfeile erhält man, indem man den einen so parallel verschiebt, daß er beim Ende des anderen beginnt, und dann den Punkt nimmt, an dem der so verschobene Pfeil endet. Das Produkt eines Vektors mit einem positiven Skalar bedeutet, die Länge unseres Pfeils entsprechend zu ändern. Das Negative eines Pfeils ist der Pfeil derselben Länge in die Gegenrichtung. Den Nullvektor denke ich mir als den ausgezeichneten festen Punkt selber. In diesem Bild entsprechen die Untervektorräume dann den folgenden Teilmengen des Raums unserer Anschauung: (0) der einelementigen Teilmenge, die nur aus unserem festen Punkt besteht, (1) allen Geraden, die unseren festen Punkt enthalten, (2) allen Ebenen, die unseren festen Punkt enthalten, und (3) dem ganzen Raum der Anschauung. Sicher mag es natürlicher scheinen, sich eher die Gesamtheit aller Parallelverschiebungen des Raums der Anschauung I.1.2.6 als Vektorraum zu denken, da man dabei ohne die Wahl eines festen Punktes auskommt. Ich kann jedoch die Mengen von Verschiebungen, die darin Untervektorräume bilden, nicht so plastisch beschreiben und auch nicht so plastisch denken, weshalb ich das zuvor erklärte Modell vorziehe.

1.3.16. Ich rede hier bewußt vom "Raum der Anschauung" und nicht vom "Anschauungsraum", da ich mir letztere Bezeichnung für das in 4.1.15 erklärte Gebilde der Mengenlehre vorbehalten will, das zwar den Raum der Anschauung modellieren soll, das ich aber doch sprachlich von diesem absetzen will. Wann immer ich einen Begriff mit dem Zusatz "der Anschauung" oder "anschaulich" versehe, ist gemeint, daß er nicht im mathematisch definierten Sinne zu verstehen ist, also nicht als ein Gebilde der Mengenlehre, sondern eben anschaulich.

1.3.17. Jeder Schnitt von Untervektorräumen eines Vektorraums ist wieder ein Untervektorraum. Betrachten wir für eine Teilmenge T eines Vektorraums V über einem Körper k den Schnitt aller Untervektorräume von V, die T umfassen, so erhalten wir offensichtlich den kleinsten Untervektorraum von V, der T umfaßt. Insbesondere existiert stets solch ein kleinster Untervektorraum. Wir notieren ihn

$$\langle T \rangle = \langle T \rangle_k \subset V$$

und bezeichnen ihn als den **von** T **erzeugten** Untervektorraum oder den **von** T **aufgespannten** Untervektorraum oder auch das **Erzeugnis von** T oder den **Spann**

von T. Er kann explizit beschrieben werden als die Menge

$$\langle T\rangle = \left\{ \alpha_1\vec{v}_1 + \ldots + \alpha_r\vec{v}_r \;\middle|\; \begin{array}{l} \alpha_1,\ldots,\alpha_r \in k,\\ \vec{v}_1,\ldots,\vec{v}_r \in T,\\ r \geq 0 \end{array} \right\}$$

wobei die leere Summe mit $r = 0$ den Nullvektor meint. In der Tat ist die auf der rechten Seite dieser Gleichung beschriebene Menge offensichtlich ein Untervektorraum von V, und jeder Untervektorraum von V, der T umfaßt, muß auch die auf der rechten Seite dieser Gleichung beschriebene Menge umfassen. Einen Vektor der Gestalt $\alpha_1\vec{v}_1+\ldots+\alpha_r\vec{v}_r$ bezeichnen wir als eine **Linearkombination** der Vektoren $\vec{v}_1,\ldots,\vec{v}_r$. Die Elemente von $\langle T\rangle$ bezeichnen wir als **Linearkombinationen von Vektoren aus** T. Gemeint sind damit immer endliche Linearkombinationen, auch wenn die Menge T selbst unendlich sein sollte.

Ergänzung 1.3.18. Andere übliche Notationen für den von einer Teilmenge T eines Vektorraums erzeugten Untervektorraum sind $\mathrm{span}(T)$ und $\mathrm{lin}(T)$.

Definition 1.3.19. Eine Teilmenge eines Vektorraums heißt ein **Erzeugendensystem** unseres Vektorraums genau dann, wenn ihr Erzeugnis der ganze Vektorraum ist. Ein Vektorraum, der ein endliches Erzeugendensystem besitzt, heißt **endlich erzeugt**. Manche Autoren verwenden gleichbededeutend die vielleicht noch präzisere Terminologie **endlich erzeugbar**.

Beispiel 1.3.20. Denken wir uns wie in 1.3.15 den Raum der Anschauung mit einem ausgezeichneten festen Punkt als reellen Vektorraum, so denke man sich das Erzeugnis des Nullvektors nur aus dem Nullvektor alias unserem festen Punkt bestehend; das Erzeugnis eines von Null verschiedenen Vektors darf man sich als die anschauliche Gerade durch den festen Punkt und den Endpunkt unseres Pfeils denken; und das Erzeugnis zweier Vektoren, von denen keiner ein Vielfaches des anderen ist, als die anschauliche Ebene, auf der unser fester Punkt und die Endpunkte unserer beiden Pfeile liegen.

Definition 1.3.21. Sei X eine Menge und k ein Körper. Die Menge $\mathrm{Ens}(X,k)$ aller Abbildungen $f : X \to k$ mit der punktweisen Addition und Multiplikation mit Skalaren ist offensichtlich ein k-Vektorraum. Darin bilden alle Abbildungen, die nur an endlich vielen Stellen von Null verschiedene Werte annehmen, einen Untervektorraum

$$k\langle X\rangle \subset \mathrm{Ens}(X,k)$$

Dieser Untervektorraum heißt der **freie Vektorraum über der Menge** X. Ein Element $a \in k\langle X\rangle$ fassen wir als "formale Linearkombination von Elementen von

X" auf und notieren es statt $(a_x)_{x\in X}$ suggestiver $\sum_{x\in X} a_x x$. Im Fall der Menge $X = \{\sharp, \flat, \natural\}$ wäre ein typisches Element von $\mathbb{Q}\langle X\rangle$ etwa der Ausdruck

$$\frac{1}{2}\,\sharp - \frac{7}{5}\,\flat + 3\,\natural$$

Im Fall einer endlichen Menge $X = \{x_1, \ldots, x_n\}$ schreiben wir statt dem etwas umständlichen $k\langle\{x_1, \ldots, x_n\}\rangle$ auch abkürzend $k\langle x_1, \ldots, x_n\rangle$. Unseren Vektorraum von eben hätten wir also auch mit $\mathbb{Q}\langle\sharp, \flat, \natural\rangle$ bezeichnen können. Wenn wir betonen wollen, daß X für eine Menge von Erzeugern und nicht etwa einen einzigen Erzeuger steht, schreiben wir $k\langle X\rangle = k\langle{}_!X\rangle$. Manchmal lassen wir auch die eckigen Klammern weg und schreiben statt $k\langle X\rangle$ einfach kX.

Weiterführende Übung 1.3.22. Man zeige, daß für eine unendliche Menge X weder der Vektorraum $\mathrm{Ens}(X, k)$ noch der freie Vektorraum $k\langle X\rangle$ über X endlich erzeugt sind. Hinweis: Für den Fall $\mathrm{Ens}(X, k)$ sind dazu die Resultate des folgenden Abschnitts hilfreich.

Übung 1.3.23. Gegeben eine Menge X und ein k-Vektorraum V ist auch die Menge $\mathrm{Ens}(X, V)$ aller Abbildungen von $X \to V$ ein k-Vektorraum, wenn man sie mit der Addition gegeben durch $(f + g)(x) = f(x) + g(x)$ und mit der Multiplikation mit Skalaren gegeben durch $(\lambda f)(x) = \lambda(f(x))$ versieht. Insbesondere erhält so auch die Menge $\mathrm{M}(n \times m; k)$ aller $(n \times m)$-Matrizen mit Einträgen in einem Körper k aus 1.1.6 die Struktur eines k-Vektorraums.

Ergänzende Übung 1.3.24. Eine Teilmenge eines Vektorraums heißt ganz allgemein eine **Hyperebene** oder genauer **lineare Hyperebene** genau dann, wenn unsere Teilmenge ein echter Untervektorraum ist, der zusammen mit einem einzigen weiteren Vektor unseren ursprünglichen Vektorraum erzeugt. Man zeige, daß eine Hyperebene zusammen mit *jedem* Vektor außerhalb besagter Hyperebene unseren ursprünglichen Vektorraum erzeugt.

1.4 Lineare Unabhängigkeit und Basen

Definition 1.4.1. Eine Teilmenge L eines Vektorraums V heißt **linear unabhängig** genau dann, wenn für beliebige paarweise verschiedene Vektoren $\vec{v}_1, \ldots, \vec{v}_r \in L$ und beliebige Skalare $\alpha_1, \ldots, \alpha_r \in k$ aus $\alpha_1\vec{v}_1 + \ldots + \alpha_r\vec{v}_r = \vec{0}$ bereits folgt $\alpha_1 = \ldots = \alpha_r = 0$.

Definition 1.4.2. Eine Teilmenge L eines Vektorraums V heißt **linear abhängig** genau dann, wenn sie nicht linear unabhängig ist, wenn es also ausgeschrieben paarweise verschiedene Vektoren $\vec{v}_1, \ldots, \vec{v}_r \in L$ und Skalare $\alpha_1, \ldots, \alpha_r \in k$ gibt derart, daß nicht alle α_i Null sind und dennoch gilt $\alpha_1\vec{v}_1 + \ldots + \alpha_r\vec{v}_r = \vec{0}$.

Beispiel 1.4.3. Die leere Menge ist in jedem Vektorraum linear unabhängig.

Beispiel 1.4.4. Eine einelementige Teilmenge ist linear unabhängig genau dann, wenn sie nicht aus dem Nullvektor besteht: Für den Nullvektor gilt nämlich $1\vec{0} = \vec{0}$ und nach unseren Annahmen gilt in einem Körper stets $1 \neq 0$, also ist die aus dem Nullvektor bestehende Menge nicht linear unabhängig. Daß jede andere einelementige Teilmenge linear unabhängig ist, folgt andererseits aus 1.3.6.

Übung 1.4.5. Eine zweielementige Teilmenge eines Vektorraums ist linear unabhängig genau dann, wenn keiner ihrer beiden Vektoren ein Vielfaches des anderen ist.

Beispiel 1.4.6. Denken wir uns wie in 1.3.15 den Raum der Anschauung mit einem ausgezeichneten festen Punkt als reellen Vektorraum, so sind drei Vektoren salopp gesprochen linear unabhängig genau dann, wenn sie nicht "zusammen mit unserem festen Punkt in einer anschaulichen Ebene liegen".

Ergänzende Übung 1.4.7. Sei $(X, \leq)$ eine partiell geordnete Menge und k ein Körper. Seien für alle $x \in X$ Abbildungen $f_x : X \to k$ gegeben mit $f_x(x) \neq 0$ und $f_x(y) \neq 0 \Rightarrow y \geq x$. Man zeige, daß dann die Familie $(f_x)_{x\in X}$ linear unabhängig ist im Vektorraum $\mathrm{Ens}(X, k)$ aller Abbildungen von X nach k.

Definition 1.4.8. Eine **Basis eines Vektorraums** ist ein linear unabhängiges Erzeugendensystem.

Beispiel 1.4.9. Denken wir uns wie in 1.3.15 den Raum der Anschauung mit einem ausgezeichneten festen Punkt als reellen Vektorraum, so ist jede Menge von drei Vektoren, die nicht zusammen mit unserem festen Punkt in einer anschaulichen Ebene liegen, eine Basis.

1.4.10. Manchmal ist es praktisch und führt zu einer übersichtlicheren Darstellung, Varianten unserer Begriffe zu verwenden, die sich statt auf Teilmengen unseres Vektorraums auf Familien von Vektoren $(\vec{v}_i)_{i\in I}$ beziehen. Eine derartige Familie heißt ein Erzeugendensystem genau dann, wenn die Menge $\{\vec{v}_i \mid i \in I\}$ ein Erzeugendensystem ist. Sie heißt **linear unabhängig** oder ganz pedantisch **linear unabhängig als Familie** genau dann, wenn für beliebige paarweise verschiedene Indizes $i_1, \ldots, i_r \in I$ und beliebige Skalare $\alpha_1, \ldots, \alpha_r \in k$ aus $\alpha_1\vec{v}_{i_1} + \ldots + \alpha_r\vec{v}_{i_r} = \vec{0}$ bereits folgt $\alpha_1 = \ldots = \alpha_r = 0$. Der wesentliche Unterschied zur Begrifflichkeit für Teilmengen liegt darin, daß bei einer Familie ja für verschiedene Indizes die zugehörigen Vektoren durchaus gleich sein könnten, was aber durch die Bedingung der linearen Unabhängigkeit dann doch wieder ausgeschlossen wird. Eine Familie von Vektoren, die nicht linear unabhängig ist, nennen wir eine **linear abhängige Familie**. Eine erzeugende und linear unabhängige Familie nennt man wieder eine **Basis** oder ausführlicher eine **durch** $i \in I$ **indizierte Basis**.

1.4.11. Besonders oft werden wir später Basen betrachten, die durch eine Menge $\{1, \ldots, n\}$ mit $n \in \mathbb{N}$ indiziert sind. Hier ist dann der wesentliche Unterschied zu einer Basis im Sinne von 1.4.8, daß wir zusätzlich festlegen, welcher Basisvektor der erste, welcher der zweite und so weiter sein soll. In der Terminologie aus **??** bedeutet das gerade, daß wir eine Anordnung auf unserer Basis festlegen. Wollen wir das besonders hervorheben, so sprechen wir von einer **angeordneten Basis**.

Beispiel 1.4.12. Sei k ein Körper und $n \in \mathbb{N}$. Wir betrachten in k^n die Vektoren

$$\vec{e}_i = (0, \ldots, 0, 1, 0, \ldots, 0)$$

mit einer Eins an der i-ten Stelle und Nullen sonst. Dann bilden $\vec{e}_1, \ldots, \vec{e}_n$ eine angeordnete Basis von k^n, die sogenannte **Standardbasis** des k^n.

Satz 1.4.13 (über Linearkombinationen von Basiselementen). *Seien k ein Körper, V ein k-Vektorraum und $(\vec{v}_i)_{i\in I}$ eine Familie von Vektoren aus unserem Vektorraum V. So sind gleichbedeutend:*

1. *Die Familie $(\vec{v}_i)_{i\in I}$ ist eine Basis von V;*
2. *Für jeden Vektor $\vec{v} \in V$ gibt es genau eine Familie $(a_i)_{i\in I}$ von Elementen unseres Körpers k, in der für höchstens endlich viele i das a_i von Null verschieden ist und für die gilt*

$$\vec{v} = \sum_{i\in I} a_i \vec{v}_i$$

Beweis. $1 \Rightarrow 2$) Ist unsere Familie ein Erzeugendensystem, so gibt es schon einmal für jeden Vektor $\vec{v} \in V$ ein Darstellung als Linearkombination $\vec{v} = \sum_{i\in I} a_i\vec{v}_i$, in der für höchstens endlich viele i das a_i von Null verschieden ist. Ist unsere Familie linear unabhängig, so muß diese Darstellung eindeutig sein: Ist nämlich $\vec{v} = \sum_{i\in I} b_i\vec{v}_i$ eine weitere derartige Darstellung von $\vec{v}$, so folgt erst $\vec{0} = \sum_{i\in I}(a_i - b_i)\vec{v}_i$, und dann wegen der linearen Unabhängigkeit unserer Familie $a_i - b_i = 0$ für alle $i \in I$.

$2 \Rightarrow 1$) Aus 2 folgt sofort, daß die $(\vec{v}_i)_{i\in I}$ ein Erzeugendensystem bilden. Wenn sich weiter jeder Vektor nur auf genau eine Weise als Linearkombination der $\vec{v}_i$ schreiben läßt, so gilt das insbesondere auch für den Nullvektor, für den also $\vec{0} = \sum_{i\in I} 0\vec{v}_i$ die einzig mögliche Darstellung als Linearkombination der $\vec{v}_i$ ist. Das zeigt dann die lineare Unabhängigkeit der $\vec{v}_i$. □

1.4.14. Mit dem Begriff des freien Vektorraums $k\langle X\rangle$ über einer Menge X aus 1.3.21 können wir den vorhergehenden Satz 1.4.13 auch wie folgt umformulieren:

Gegeben ein k-Vektorraum V ist eine Familie $(\vec{v}_i)_{i\in I}$ von Vektoren eine Basis genau dann, wenn das "Auswerten formaler Ausdrücke"

$$\begin{array}{rccc} \Phi: & k\langle I\rangle & \to & V \\ & (a_i)_{i\in I} & \mapsto & \sum_{i\in I} a_i\vec{v}_i \end{array}$$

eine Bijektion des freien Vektorraums $k\langle I\rangle$ über I mit dem gegebenen Vektorraum V definiert. Ausführlicher gilt für diese Abbildung Φ sogar:

$$\begin{array}{lcll} (\vec{v}_i)_{i\in I} \text{ ist Erzeugendensystem} & \Leftrightarrow & \Phi \text{ ist eine Surjektion} & k\langle I\rangle \twoheadrightarrow V \\ (\vec{v}_i)_{i\in I} \text{ ist linear unabhängig} & \Leftrightarrow & \Phi \text{ ist eine Injektion} & k\langle I\rangle \hookrightarrow V \\ (\vec{v}_i)_{i\in I} \text{ ist eine Basis} & \Leftrightarrow & \Phi \text{ ist eine Bijektion} & k\langle I\rangle \xrightarrow{\sim} V \end{array}$$

Hier folgt die erste Äquivalenz direkt aus den Definitionen. Um bei der zweiten Äquivalenz die Implikation $\Leftarrow$ einzusehen, muß man nur bemerken, daß Φ den Nullvektor auf Null wirft und folglich kein anderer Vektor aus $k\langle I\rangle$ von Φ auf Null geworfen werden kann. Um bei der zweiten Äquivalenz die Implikation $\Rightarrow$ einzusehen, argumentiert man wie im Beweis von 1.4.13. Die letzte Äquivalenz schließlich ist eine direkte Konsequenz der ersten beiden. Als Variante bemerken wir, daß wir für jede angeordnete Basis $\mathcal{B} = (\vec{v}_1, \ldots, \vec{v}_n)$ eines k-Vektorraums V eine Bijektion

$$\Phi_{\mathcal{B}} : k^n \xrightarrow{\sim} V$$

erhalten durch die Abbildungsvorschrift $(\lambda_1, \ldots, \lambda_n) \mapsto \lambda_1\vec{v}_1 + \ldots + \lambda_n\vec{v}_n$. Der Beweis ist mutatis mutandis derselbe.

Satz 1.4.15 (Charakterisierungen von Basen). *Für eine Teilmenge eines Vektorraums sind gleichbedeutend:*

1. *Unsere Teilmenge ist eine Basis alias ein linear unabhängiges Erzeugendensystem.*
2. *Unsere Teilmenge ist minimal unter allen Erzeugendensystemen.*
3. *Unsere Teilmenge ist maximal unter allen linear unabhängigen Teilmengen.*

1.4.16. Die Begriffe minimal und maximal sind hier zu verstehen im Sinne von **??** in Bezug auf Inklusionen zwischen Teilmengen, nicht etwa in Bezug auf die Zahl der Elemente.

Beweis. $(1 \Leftrightarrow 2)$ Es gilt zu zeigen: Ein Erzeugendensystem ist linear unabhängig genau dann, wenn es minimal ist. Wir zeigen das durch Widerspruch. Ist $E \subset V$ ein Erzeugendensystem und ist E nicht linear unabhängig, so gilt eine Relation $\lambda_1\vec{v}_1 + \ldots + \lambda_n\vec{v}_n = \vec{0}$ mit $n \geq 1$, den $\vec{v}_i \in E$ paarweise verschieden und allen

$\lambda_i \neq 0$. Nach Multiplikation mit λ_1^{-1} dürfen wir hier sogar $\lambda_1 = 1$ annehmen. Wir folgern

$$\vec{v}_1 = -\lambda_1^{-1}\lambda_2\vec{v}_2 - \ldots - \lambda_1^{-1}\lambda_n\vec{v}_n \in \langle E\backslash\vec{v}_1\rangle$$

und damit ist auch $E\backslash\vec{v}_1$ bereits ein Erzeugendensystem und E war nicht minimal. Ist umgekehrt E nicht minimal, so gibt es $\vec{v} \in E$ derart, daß $E\backslash\vec{v}$ immer noch ein Erzeugendensystem ist, und insbesondere existiert eine Darstellung

$$\vec{v} = \lambda_1\vec{v}_1 + \ldots + \lambda_n\vec{v}_n$$

mit $n \geq 0$ und $\vec{v}_i \in E\backslash\vec{v}$. Dann existiert aber auch solch eine Darstellung mit den $\vec{v}_i$ paarweise verschieden, daraus folgt $\vec{v} - \lambda_1\vec{v}_1 - \ldots - \lambda_n\vec{v}_n = \vec{0}$, und E war nicht linear unabhängig.

$(1 \Leftrightarrow 3)$ Es gilt zu zeigen: Eine linear unabhängige Teilmenge ist ein Erzeugendensystem genau dann, wenn sie maximal ist. Wir argumentieren wieder durch Widerspruch. Ist $L \subset V$ linear unabhängig und kein Erzeugendensystem, so ist für jedes $\vec{v} \in V\backslash\langle L\rangle$ auch $L \cup \{\vec{v}\}$ linear unabhängig und L war nicht maximal. Ist umgekehrt L nicht maximal, so gibt es einen Vektor $\{\vec{v}\}$ derart, daß auch $L \cup \{\vec{v}\}$ linear unabhängig ist, und dann kann L kein Erzeugendensystem gewesen sein, denn dieser Vektor $\vec{v}$ kann nicht zu ihrem Erzeugnis gehört haben. □

Ergänzende Übung 1.4.17. Seien $L \subset E$ eine linear unabhängige Teilmenge in einem Erzeugendensystem eines Vektorraums. Ist A minimal unter allen Erzeugendensystemen unseres Vektorraums mit $L \subset A \subset E$, so ist A eine Basis. Ist A maximal unter allen linear unabhängigen Teilmengen unseres Vektorraums mit $L \subset A \subset E$, so ist A eine Basis.

1.4.18. Unser Satz 1.4.15 impliziert insbesondere, daß jeder endlich erzeugte Vektorraum eine endliche Basis besitzt: Wir lassen einfach aus einem endlichen Erzeugendensystem so lange Vektoren weg, bis wir bei einem unverkürzbaren Erzeugendensystem angekommen sind. Mit raffinierteren Methoden der Mengenlehre kann man sogar den sogenannten **Basisexistenzsatz** zeigen, nach dem überhaupt jeder Vektorraum eine Basis besitzt: Wir diskutieren das in 1.4.39 und recht eigentlich erst in **??**.

Satz 1.4.19. *In einem vorgegebenen Vektorraum hat eine linear unabhängige Teilmenge stets höchstens soviele Elemente wie ein Erzeugendensystem. Ist also V ein Vektorraum, $L \subset V$ eine linear unabhängige Teilmenge und $E \subset V$ ein Erzeugendensystem, so gilt in Formeln*

$$|L| \leq |E|$$

1.4.20. Wir verwenden hier unsere Konvention, nach der wir für alle unendlichen Mengen X schlicht $|X| = \infty$ setzen. In Worten besagt der Satz also, daß in einem endlich erzeugten Vektorraum eine linear unabhängige Teilmenge höchstens soviele Elemente haben kann wie ein beliebiges Erzeugendensystem. Der Satz gilt aber auch mit einer feineren Interpretation von $|X|$ als "Kardinalität". Genauer folgt aus dem Zorn'schen Lemma die Existenz einer Injektion $L \hookrightarrow E$, wie in 1.4.22 in größerer Allgemeinheit diskutiert wird.

Erster Beweis. Durch Widerspruch. Nehmen wir an, wir hätten ein Erzeugendensystem $E = \{\vec{w}_1, \ldots, \vec{w}_m\}$ und eine linear unabhängige Teilmenge $L = \{\vec{v}_1, \ldots, \vec{v}_n\}$ mit $n > m$. Dann könnten wir natürlich $a_{ij} \in k$ finden mit

$$\begin{array}{ccccccccc} \vec{v}_1 & = & a_{11}\vec{w}_1 & + & a_{21}\vec{w}_2 & + & \cdots & + & a_{m1}\vec{w}_m \\ \vdots & & \vdots & & \vdots & & & & \vdots \\ \vec{v}_n & = & a_{1n}\vec{w}_1 & + & a_{2n}\vec{w}_2 & + & \cdots & + & a_{mn}\vec{w}_m \end{array}$$

Jetzt betrachten wir das "vertikal geschriebene" homogene lineare Gleichungssystem

$$\begin{array}{ccccc} x_1a_{11} & & x_1a_{21} & & x_1a_{m1} \\ + & & + & & + \\ \vdots & & \vdots & \cdots & \vdots \\ + & & + & & + \\ x_na_{1n} & & x_na_{2n} & \cdots & x_na_{mn} \\ = & & = & & = \\ 0 & & 0 & \cdots & 0 \end{array}$$

das in der üblichen Form geschrieben die Gestalt

$$\begin{array}{ccccccc} a_{11}x_1 & + & \cdots & + & a_{1n}x_n & = & 0 \\ a_{21}x_1 & + & \cdots & + & a_{2n}x_n & = & 0 \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{m1}x_1 & + & \cdots & + & a_{mn}x_n & = & 0 \end{array}$$

annimmt. Da unser Gleichungssystem weniger Gleichungen hat als Unbekannte, liefert der Gauß-Algorithmus 1.1.4 dafür mindestens eine von Null verschiedene Lösung $(x_1, \ldots, x_n) \neq (0, \ldots, 0)$. Für jede solche Lösung gilt aber

$$x_1\vec{v}_1 + \cdots + x_n\vec{v}_n = 0$$

im Widerspruch zur linearen Unabhängigkeit der $\vec{v}_i$. □

Zweiter Beweis. Unser Satz folgt auch sofort aus dem Austauschsatz 1.4.21, den wir im Anschluß formulieren und beweisen. □

Satz 1.4.21 (Austauschsatz von Steinitz). *Ist V ein Vektorraum, $E \subset V$ ein Erzeugendensystem und $L \subset V$ eine endliche linear unabhängige Teilmenge, so gibt es eine Injektion $\varphi : L \hookrightarrow E$ derart, daß auch $(E\backslash\varphi(L)) \cup L$ ein Erzeugendensystem von V ist.*

1.4.22. Wir können in anderen Worten die Vektoren unserer linear unabhängigen Teilmenge so in unser Erzeugendensystem hineintauschen, daß es ein Erzeugendensystem bleibt. Mit raffinierteren Methoden der Mengenlehre kann unser Austauschsatz auch ohne die Voraussetzung L endlich gezeigt werden. Der Beweis in dieser Allgemeinheit wird in **??** skizziert.

Beweis. Sei $M \subset L$ eine maximale Teilmenge von L, für die es eine Injektion $\varphi : M \hookrightarrow E$ gibt mit der Eigenschaft, daß auch $(E\backslash\varphi(M)) \cup M$ ein Erzeugendensystem von V ist. Es gilt zu zeigen $M = L$. Sei sonst $\vec{w} \in L \setminus M$. Schreiben wir $\vec{w}$ als eine Linearkombination von Vektoren aus $(E\backslash\varphi(M)) \cup M$, genauer als

$$\vec{w} = \lambda_1\vec{v}_1 + \ldots + \lambda_r\vec{v}_r + \mu_1\vec{w}_1 + \ldots + \mu_s\vec{w}_s$$

mit $\vec{v}_1, \ldots, \vec{v}_r \in E\backslash\varphi(M)$ paarweise verschieden und $\vec{w}_1, \ldots, \vec{w}_s \in M$ paarweise verschieden, so muß in dieser Linearkombination mindestens ein Vektor $\vec{v}_i \in E\backslash\varphi(M)$ mit einem von Null verschiedenen Koeffizienten $\lambda_i \neq 0$ auftreten, da ja L linear unabhängig war und $\vec{w}$ auf die andere Seite gebracht mit dem Koeffizienten $(-1) \neq 0$ auftritt. Dann erhält man jedoch wieder ein Erzeugendensystem, wenn man zusätzlich diesen Vektor $\vec{v}_i$ durch unser $\vec{w}$ austauscht, denn es gilt ja

$$\vec{v}_i = -\lambda_i^{-1}\lambda_1\vec{v}_1 - \ldots - \widehat{\lambda_i^{-1}\lambda_i\vec{v}_i} - \ldots - \lambda_i^{-1}\lambda_r\vec{v}_r - \lambda_i^{-1}\mu_1\vec{w}_1 - \ldots - \lambda_i^{-1}\mu_s\vec{w}_s + \lambda_i^{-1}\vec{w}$$

mit einem Hut über dem wegzulassenden Summanden und damit liegt liegt $\vec{v}_i$ im Erzeugnis von $((E\backslash(\varphi(M))\backslash\vec{v}_i) \cup (M \cup \{\vec{w}\})$, das folglich immer noch der ganze Raum ist. Widerspruch zur Maximalität von M! □

Korollar 1.4.23 (Kardinalitäten von Basen). *Jeder endlich erzeugte Vektorraum besitzt eine endliche Basis, und je zwei seiner Basen haben gleich viele Elemente.*

Ergänzung 1.4.24. In **??** wird mit raffinierteren Methoden der Mengenlehre gezeigt, daß es auch im Fall eines nicht notwendig endlich erzeugten Vektorraums für je zwei seiner Basen eine Bijektion zwischen der einen Basis und der anderen Basis gibt.

Beweis. Wie bereits in 1.4.18 erwähnt, erhalten wir nach 1.4.15 eine endliche Basis, wenn wir ein beliebiges endliches Erzeugendensystem durch das Streichen von Vektoren zu einem minimalen Erzeugendensystem verkleinern. Gegeben zwei Basen B und B' eines Vektorraums haben wir nach 1.4.19 außerdem stets $|B| \leq |B'| \leq |B|$. □

Definition 1.4.25. Die Kardinalität einer und nach 1.4.23 jeder Basis eines endlich erzeugten Vektorraums V heißt die **Dimension** von V und wird $\dim V$ notiert. Ist k ein Körper und wollen wir betonen, daß wir die Dimension als k-Vektorraum meinen, so schreiben wir

$$\dim V = \dim_k V$$

Ist der Vektorraum nicht endlich erzeugt, so schreiben wir $\dim V = \infty$ und nennen V **unendlichdimensional** und ignorieren für gewöhnlich die durchaus möglichen feineren Unterscheidungen zwischen verschiedenen Unendlichkeiten. Derartige Feinheiten werden in **??** besprochen.

1.4.26. In der Physik wird der Begriff "Dimension" leider auch noch in einer völlig anderen Bedeutung verwendet: Physikalische Dimensionen wären in diesem Sinne etwa die Länge, die Zeit, die Masse, die Frequenz und dergleichen mehr. In der hier entwickelten Sprache würde man so eine physikalische Dimension wohl am ehesten als einen "eindimensionalen reellen Vektorraum" modellieren. Ich kann nur hoffen, daß der Leser aus dem Kontext erschließen kann, welcher Dimensionsbegriff im Einzelfall jeweils gemeint ist.

1.4.27. Der Nullraum hat als Basis die leere Menge. Seine Dimension ist folglich Null. Allgemeiner haben wir nach 1.4.12 offensichtlich

$$\dim_k k^n = n$$

Korollar 1.4.28. *Sei V ein endlich erzeugter Vektorraum.*

1. *Jede linear unabhängige Teilmenge $L \subset V$ hat höchstens $\dim V$ Elemente und im Fall $|L| = \dim V$ ist L bereits eine Basis.*
2. *Jedes Erzeugendensystem $E \subset V$ hat mindestens $\dim V$ Elemente und im Fall $|E| = \dim V$ ist E bereits eine Basis.*

Beweis. Nach 1.4.19 haben wir für L eine linear unabhängige Teilmenge, B eine Basis und E ein Erzeugendensystem stets

$$|L| \leq |B| \leq |E|$$

Gibt es ein endliches Erzeugendensystem, so muß im Fall $|L| = |B|$ mithin L eine maximale linear unabhängige Teilmenge und damit nach 1.4.15 eine Basis sein. Im Fall $|B| = |E|$ muß E in derselben Weise ein minimales Erzeugendensystem und damit nach 1.4.15 eine Basis sein. □

Korollar 1.4.29. *Ein echter Untervektorraum eines endlichdimensionalen Vektorraums hat stets eine echt kleinere Dimension. Ist allgemeiner und in Formeln $U \subset V$ ein Untervektorraum, so gilt $\dim U \leq \dim V$ und aus $\dim U = \dim V < \infty$ folgt $U = V$.*

Beweis. Ist V nicht endlich erzeugt, so ist nichts zu zeigen. Ist V endlich erzeugt, so gibt es nach 1.4.28 in U eine maximale linear unabhängige Teilmenge, und jede derartige Teilmenge hat höchstens $\dim V$ Elemente. Jede derartige Teilmenge ist aber nach 1.4.15 notwendig eine Basis von U und das zeigt $\dim U \leq \dim V$. Gilt hier Gleichheit und ist V endlichdimensional, so ist wieder nach 1.4.28 jede Basis von U auch eine Basis von V und das zeigt $U = V$. □

Übung 1.4.30. Man zeige, daß jeder eindimensionale Vektorraum genau zwei Untervektorräume besitzt.

Satz 1.4.31 (Dimensionssatz). *Gegeben ein Vektorraum V und Teilräume $U, W \subset V$ mit endlichdimensionalem Schnitt gilt*

$$\dim(U + W) = \dim U + \dim W - \dim(U \cap W)$$

Bemerkung 1.4.32. Wir beweisen diesen Satz in 1.6.15 noch ein zweites Mal als Korollar der Dimensionsformel.

Beispiel 1.4.33. Denken wir uns wie in 1.3.15 den Raum der Anschauung mit einem ausgezeichneten festen Punkt als Vektorraum, so entsprechen die zweidimensionalen Untervektorräume den anschaulichen Ebenen durch unseren festen Punkt und je zwei verschiedene zweidimensionale Untervektorräume U, W spannen den ganzen Raum auf, $\dim(U + W) = 3$. Zwei verschiedene Ebenen durch unseren festen Punkt schneiden sich nun offensichtlich in einer anschaulichen Geraden, und das entspricht genau der Aussage unseres Satzes, die in diesem Fall zur Identität $3 = 2 + 2 - 1$ spezialisiert.

Beweis. Sind U oder W unendlichdimensional, so ist das eh klar. Sonst wählen wir eine Basis $s_1, \ldots, s_d$ von $U \cap W$ und ergänzen sie erst durch $u_1, \ldots, u_r \in U$ zu einer Basis von U und dann weiter durch $w_1, \ldots, w_t \in W$ zu einer Basis von $U+W$. Wir haben gewonnen, wenn wir zeigen können, daß bei derartigen Wahlen bereits $s_1, \ldots, s_d, w_1, \ldots, w_t$ eine Basis von W ist. Dazu reicht es zu zeigen, daß diese Menge W erzeugt. Sicher können wir jedes $w \in W$ schreiben als Linearkombination

$$\begin{aligned} w \quad = \quad & \lambda_1 u_1 + \ldots + \lambda_r u_r \\ & + \mu_1 s_1 + \ldots + \mu_d s_d \\ & + \nu_1 w_1 + \ldots + \nu_t w_t \end{aligned}$$

Dabei gilt jedoch offensichtlich $\lambda_1 u_1 + \ldots + \lambda_r u_r \in W \cap U$. Dieser Ausdruck läßt sich damit auch als Linearkombination der s_i schreiben, so daß w selbst auch als Linearkombination der s_i und der w_j geschrieben werden kann, was zu zeigen war. Im übrigen muß dann auch bei der obigen Darstellung bereits gelten $\lambda_1 = \ldots = \lambda_r = 0$, aber das ist für unseren Beweis schon gar nicht mehr von Belang. □

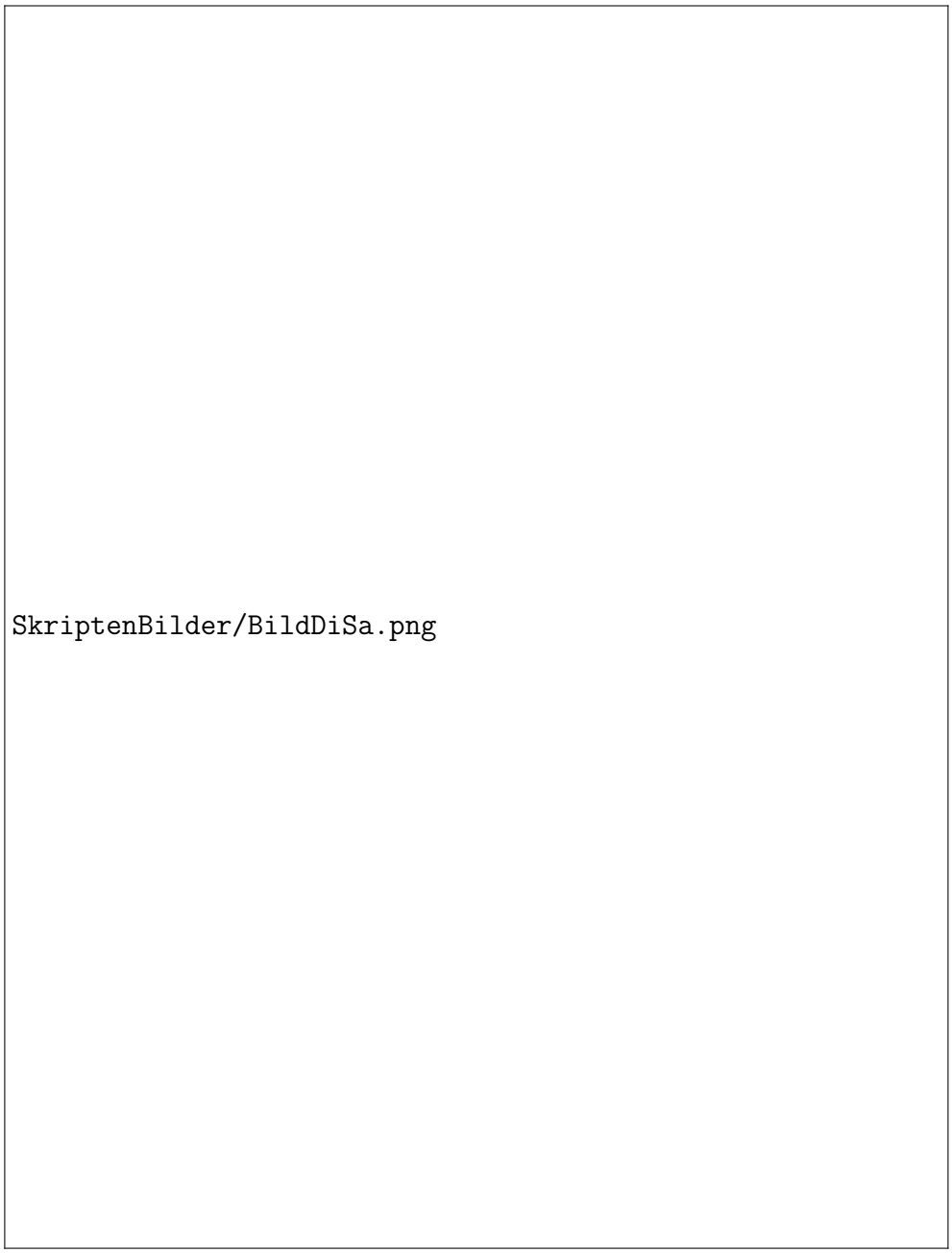


Illustration zum Dimensionssatz nach 1.4.33: Zwei verschiedene Ebenen im Raum, die beide einen ausgezeichneten festen Punkt enthalten, schneiden sich in einer Geraden.

Ergänzende Übung 1.4.34. Eine Gruppe, in der jedes Element sein eigenes Inverses ist, kann auf genau eine Weise mit der Struktur eines Vektorraums über dem Körper mit zwei Elementen versehen werden, und ihre Untergruppen sind dann genau die Untervektorräume.

Übung 1.4.35. Gegeben k-Vektorräume $V_1, \ldots, V_n$ zeige man für die Dimension ihres kartesischen Produkts im Sinne von 1.3.10 die Formel

$$\dim(V_1 \oplus \ldots \oplus V_n) = \dim(V_1) + \ldots + \dim(V_n)$$

Ergänzende Übung 1.4.36. Wir erinnern die Körper $\mathbb{R} \subset \mathbb{C}$ aus I.3.3.15. Natürlich kann jeder $\mathbb{C}$-Vektorraum V auch als $\mathbb{R}$-Vektorraum aufgefaßt werden. Man zeige $\dim_{\mathbb{R}} V = 2 \dim_{\mathbb{C}} V$.

Satz 1.4.37 (Basisergänzungssatz). *Ist in einem endlich erzeugten Vektorraum L eine linear unabhängige Teilmenge und E ein Erzeugendensystem, so läßt sich L durch Hinzunahme von Vektoren aus E zu einer Basis unseres Vektorraums ergänzen.*

Beweis. Nach 1.4.17 ist jede linear unabhängige Teilmenge B unseres Vektorraums, die maximal ist unter allen linear unabhängigen Teilmengen A mit $L \subset A \subset (L \cup E)$, bereits eine Basis. Nach 1.4.19 gibt es auch tatsächlich maximale Teilmengen B mit dieser Eigenschaft. □

1.4.38. Der Basisergänzungssatz gilt unverändert auch für nicht notwendig endlich erzeugte Vektorräume. Der Beweis in dieser Allgemeinheit wird in **??** gegeben. Er verwendet tieferliegende Methoden der Mengenlehre und paßt schlecht in eine Grundvorlesung. Um dennoch einige der im folgenden bewiesenen Sätze nicht durch unnötig einschränkende Endlichkeitsannahmen zu verkomplizieren, werde ich für die Zwecke dieser Vorlesung den Basisergänzungssatz für nicht notwendig endlich erzeugte Vektorräume ohne Beweis hinnehmen. Damit Sie nicht den Überlick verlieren, was nun im allgemeinen und was nur für endlich erzeugte Vektorräume vollständig bewiesen ist, will ich den Basisergänzungssatz in dieser Allgemeinheit sozusagen als Axiom behandeln. Wir nehmen also ohne Beweis die folgende Aussage hin:

> **Axiom:** Ist V ein Vektorraum, $L \subset V$ eine linear unabhängige Teilmenge und $E \subset V$ ein Erzeugendensystem von V, so läßt sich L durch Hinzunahme von Vektoren aus E zu einer Basis von V ergänzen.

Ich verspreche, daß es das einzige Axiom dieser Art bleiben soll, so daß wir zumindest mit klaren Spielregeln weiterarbeiten. Ich werde auch mein möglichstes tun, an jeder Stelle klarzumachen, welche der im folgenden bewiesenen Aussagen im unendlichdimensionalen Fall auf der allgemeinen Form des Basisergänzungssatzes beruhen. Ein erstes Beispiel ist der bereits erwähnte Basisexistenzsatz.

Satz 1.4.39 (Basisexistenzsatz). *Jeder Vektorraum besitzt eine Basis.*

Beweis. Die leere Menge ist stets linear unabhängig, der ganze Vektorraum ist stets ein Erzeugendensystem. Nun wende man den allgemeinen Basisergänzungssatz 1.4.38 an. □

1.5 Lineare Abbildungen

Definition 1.5.1. Seien V, W Vektorräume über einem Körper k. Eine Abbildung $f : V \to W$ heißt **linear** oder genauer **k-linear** oder ein **Homomorphismus von k-Vektorräumen** genau dann, wenn für alle $\vec{v}, \vec{w} \in V$ und $\lambda \in k$ gilt

$$\begin{aligned} f(\vec{v} + \vec{w}) &= f(\vec{v}) + f(\vec{w}) \\ f(\lambda\vec{v}) &= \lambda f(\vec{v}) \end{aligned}$$

Eine bijektive lineare Abbildung heißt ein **Isomorphismus** von Vektorräumen. Gibt es zwischen zwei Vektorräumen einen Isomorphismus, so heißen sie **isomorph**. Ein Homomorphismus von einem Vektorraum in sich selber heißt ein **Endomorphismus** unseres Vektorraums. Ein Isomorphismus von einem Vektorraum in sich selber heißt ein **Automorphismus** unseres Vektorraums. Die Terminologie geht auf griechisch $\mu o \rho \varphi \eta$ für deutsch "Gestalt" mit griechisch $o \mu \upsilon o$ für deutsch "zusammen", griechisch $\iota \sigma o \varsigma$ für deutsch "gleich", griechisch $\varepsilon \nu \delta o \nu$ für deutsch "drinnen", und griechisch $\alpha \upsilon \tau o \varsigma$ für deutsch "selbst" zurück.

Beispiel 1.5.2. Die Projektionen auf die Faktoren $\mathrm{pr}_i : k^n \to k$ sind linear. Das Quadrieren $k \to k$ ist nicht linear, es sei denn, k ist ein Körper mit zwei Elementen.

Beispiel 1.5.3. Gegeben Vektorräume V, W sind die Projektionsabbildungen $\mathrm{pr}_V : (V \oplus W) \to V$ und $\mathrm{pr}_W : (V \oplus W) \to W$ linear. Dasselbe gilt allgemeiner für die Projektionen $\mathrm{pr}_i : V_1 \oplus \ldots \oplus V_n \to V_i$. Ebenso sind die **kanonischen Injektionen** $\mathrm{in}_V : V \to (V \oplus W)$, $v \mapsto (v, 0)$ und $\mathrm{in}_W : W \to (V \oplus W)$, $w \mapsto (0, w)$ linear und dasselbe gilt allgemeiner für die analog definierten Injektionen $\mathrm{in}_i : V_i \to V_1 \oplus \ldots \oplus V_n$.

Übung 1.5.4. Jede Verknüpfung von Vektorraumhomomorphismen ist wieder ein Vektorraumhomomorphismus. Sind also in Formeln $f : V \to W$ und $g : U \to V$ Vektorraumhomomorphismen, so ist auch $f \circ g : U \to W$ ein Vektorraumhomomorphismus.

Übung 1.5.5. Ist $f : V \to W$ ein Vektorraumisomorphismus, so ist auch die Umkehrabbildung $f^{-1} : W \to V$ ein Vektorraumisomorphismus. Insbesondere

bilden die Automorphismen eines Vektorraums V eine Untergruppe seiner Permutationsgruppe. Sie heißt die **allgemeine lineare Gruppe** oder auch die **Automorphismengruppe** unseres Vektorraums V und wird notiert

$$\mathrm{GL}(V) = \mathrm{Aut}(V) \subset \mathrm{Ens}^\times(V)$$

nach der englischen Bezeichnung **general linear group**.

Übung 1.5.6. Das Bild eines Untervektorraums unter einer linearen Abbildung ist ein Untervektorraum. Das Urbild eines Untervektorraums unter einer linearen Abbildung ist ein Untervektorraum.

Übung 1.5.7. Wieviele Untervektorräume besitzt der $\mathbb{R}^2$, die unter der Spiegelung $(x, y) \mapsto (x, -y)$ in sich selber überführt werden? Welche Untervektorräume des $\mathbb{R}^3$ werden unter der Spiegelung $(x, y, z) \mapsto (x, y, -z)$ in sich selber überführt?

Definition 1.5.8. Ein Punkt, der unter einer Abbildung auf sich selbst abgebildet wird, heißt ein **Fixpunkt** besagter Abbildung. Gegeben eine Abbildung $f : X \to X$ notiert man die Menge ihrer Fixpunkte auch

$$X^f = \{x \in X \mid f(x) = x\}$$

Übung 1.5.9. Gegeben ein Vektorraum V und ein Endomorphismus $f \in \mathrm{End}\, V$ bildet die Menge der von f festgehaltenen Vektoren einen Untervektorraum $V^f \subset V$.

Satz 1.5.10. *Gegeben eine natürliche Zahl n ist ein Vektorraum über einem Körper k genau dann isomorph zu k^n, wenn er die Dimension n hat.*

Beweis. Natürlich gehen unter einem Vektorraumisomorphismus Erzeugendensysteme in Erzeugendensysteme, linear unabhängige Teilmengen in linear unabhängige Teilmengen und Basen in Basen über. Sind also zwei Vektorräume isomorph, so haben sie auch dieselbe Dimension. Hat umgekehrt ein Vektorraum V eine angeordnete Basis $B = (\vec{v}_1, \ldots, \vec{v}_n)$ aus n Vektoren, so liefert die Vorschrift $(\lambda_1, \ldots, \lambda_n) \mapsto \lambda_1\vec{v}_1 + \ldots + \lambda_n\vec{v}_n$ etwa nach 1.4.14 einen Vektorraumisomorphismus $k^n \xrightarrow{\sim} V$. □

1.5.11. Nun können wir auch unsere Ausgangsfrage 1.1.9 lösen, ob die "Zahl der freien Parameter" bei unserer Darstellung der Lösungsmenge eines linearen Gleichungssystems eigentlich wohlbestimmt ist oder präziser, ob beim Anwenden des Gauss-Algorithmus dieselbe Zahl von Stufen entsteht, wenn wir zuvor die Variablen umnummerieren alias die Spalten vertauschen. Wenn wir das für homogene Systeme zeigen können, folgt es offensichtlich für beliebige Systeme.

Illustration zu Übung 1.5.9, nach der die Fixpunktmenge jedes Endomorphismus eines Vektorraums ein Untervektorraum ist. Zum Beispiel ist die Spiegelung an einer Ursprungsgerade eine lineare Abbildung und ihre Fixpunktmenge ist in der Tat ein Untervektorraum, nämlich besagte Ursprungsgerade.

Bei homogenen Systemen ist jedoch die Lösungsmenge $L \subset k^m$ ein Untervektorraum und wir erhalten einen Vektorraumisomorphismus $L \xrightarrow{\sim} k^{m-r}$ durch "Streichen aller Einträge, bei denen eine neue Stufe beginnt", also durch Weglassen von $x_{s(1)}, x_{s(2)}, \ldots, x_{s(r)}$ aus einem m-Tupel $(x_1, \ldots, x_m) \in L$. Damit erhalten wir für die Zahl r der Stufen die von allen Wahlen unabhängige Beschreibung als Zahl der Variablen abzüglich der Dimension des Lösungsraums, in Formeln $r = m - \dim_k L$.

1.5.12. Seien V, W Vektorräume über einem Körper k. Die Menge aller Homomorphismen von V nach W notieren wir

$$\mathrm{Hom}_k(V, W) = \mathrm{Hom}(V, W) \subset \mathrm{Ens}(V, W)$$

Lemma 1.5.13 (Lineare Abbildungen und Basen). *Seien V, W Vektorräume über einem Körper k und $B \subset V$ eine Basis. So liefert das Einschränken von Abbildungen eine Bijektion*

$$\mathrm{Hom}_k(V, W) \xrightarrow{\sim} \mathrm{Ens}(B, W)$$

Jede lineare Abbildung ist also in Worten festgelegt und festlegbar durch ihre Werte auf einer Basis.

Erster Beweis. Seien $f, g : V \to W$ linear. Gilt $f(\vec{v}) = g(\vec{v})$ für alle $\vec{v} \in B$, so folgt $f(\lambda_1\vec{v}_1 + \ldots + \lambda_r\vec{v}_r) = g(\lambda_1\vec{v}_1 + \ldots + \lambda_r\vec{v}_r)$ für alle $\lambda_1, \ldots, \lambda_r \in k$ und $\vec{v}_1, \ldots, \vec{v}_r \in B$ und damit $f(\vec{v}) = g(\vec{v})$ für alle $\vec{v}$ im Erzeugnis von B alias für alle $\vec{v} \in V$. Das zeigt die Injektivität der im Lemma betrachteten Einschränkungsabbildung sogar für jedes Erzeugendensystem B von V. Ist B sogar eine Basis und ist umgekehrt eine Abbildung von Mengen $g : B \to W$ gegeben, so können wir sie zu einer linearen Abbildung $\tilde{g} : V \to W$ ausdehnen wie folgt: Jeder Vektor $\vec{v} \in V$ läßt sich ja nach 1.4.13 eindeutig als Linearkombination der Basisvektoren schreiben, etwa $\vec{v} = \lambda_1\vec{v}_1 + \ldots + \lambda_r\vec{v}_r$ mit paarweise verschiedenen $\vec{v}_i \in B$, und wenn wir nun schlicht

$$\tilde{g}(\vec{v}) = \lambda_1 g(\vec{v}_1) + \ldots + \lambda_r g(\vec{v}_r)$$

setzen, so erhalten wir die gesuchte lineare Ausdehnung von g. □

1.5.14. Der vorstehende Beweis befriedigt mich nicht vollständig, da wir darin doch einiges nicht ganz sauber ausgeführt haben: So muß eigentlich die Eindeutigkeit der Darstellung als Linearkombination von Basisvektoren sorgfältiger formuliert werden, und die Linearität unserer Ausdehnung $\tilde{g}$ könnte auch noch eine sorgfältigere Argumentation vertragen. Wir wiederholen deshalb unsere Argumentation nocheinmal in einer abstrakteren Sprache.

1.5.15. Wir erinnern an Begriff des freien k-Vektorraums $k\langle I\rangle$ über einer Menge I und erklären die **kanonische Einbettung** $\mathrm{can} : I \hookrightarrow k\langle I\rangle$ dadurch, daß sie jedem Punkt $i \in I$ die charakteristische Funktion der einelementigen Menge $\{i\}$ zuordnen möge. In anderen Worten ist also $\mathrm{can}(i)$ die formale Linearkombination von Elementen von I, in der i selbst mit dem Koeffizienten Eins auftritt und alle anderen $j \in I$ mit dem Koeffizienten Null. Offensichtlich ist das Bild $\mathrm{can}(I)$ der Menge I unter dieser kanonischen Einbettung eine Basis des freien Vektorraums über I.

Satz 1.5.16 (Universelle Eigenschaft freier Vektorräume). *Seien I eine Menge, k ein Körper, $k\langle I\rangle$ der freie Vektorraum über I und $\mathrm{can} : I \to k\langle I\rangle$ die kanonische Einbettung. So liefert für jeden k-Vektorraum W das Vorschalten von can eine Bijektion*

$$\mathrm{Hom}_k(k\langle I\rangle, W) \xrightarrow{\sim} \mathrm{Ens}(I, W)$$

Beweis. Stimmen zwei lineare Abbildungen auf einer Teilmenge eines Vektorraums überein, so auch auf dem von dieser Teilmenge erzeugten Untervektorraum. Da nun das Bild von can den ganzen freien Vektorraum $k\langle I\rangle$ erzeugt, folgt für lineare Abbildungen $f, g : k\langle I\rangle \to W$ aus $f \circ \mathrm{can} = g \circ \mathrm{can}$ bereits $f = g$ und die Injektivität unserer Bijektion in spe ist gezeigt. Ist andererseits irgendeine Abbildung $\varphi : I \to W$ gegeben, etwa $\varphi : i \mapsto \vec{w}_i$, so können wir die lineare Abbildung

$$\begin{array}{rccc} \tilde{\varphi} & : & k\langle I\rangle & \to & W \\ & & (a_i)_{i\in I} & \mapsto & \sum a_i\vec{w}_i \end{array}$$

bilden, für die per definitionem gilt $\tilde{\varphi} \circ \mathrm{can} = \varphi$. Das zeigt dann auch die Surjektivität unserer Bijektion in spe. □

Zweiter Beweis von Lemma 1.5.13. Da $B \subset V$ eine Basis ist, liefert das Auswerten formaler Ausdrücke nach 1.4.14 einen Vektorraumisomorphismus $\Phi : k\langle B\rangle \xrightarrow{\sim} V$. Per definitionem ist seine Komposition mit $\mathrm{can} : B \to kB$ schlicht die Einbettung $i : B \hookrightarrow V$. Wir erhalten nun Bijektionen

$$\mathrm{Hom}_k(V, W) \overset{\circ\Phi}{\xrightarrow{\sim}} \mathrm{Hom}_k(k\langle B\rangle, W) \overset{\circ\,\mathrm{can}}{\xrightarrow{\sim}} \mathrm{Ens}(B, W)$$

da Φ ein Isomorphismus ist und wegen 1.5.16. Das Lemma 1.5.13 folgt. □

Übung 1.5.17. Man zeige, daß $\mathrm{Hom}_k(V, W)$ ein Untervektorraum der Menge aller Abbildungen $\mathrm{Ens}(V, W)$ von V nach W mit ihrer Vektorraumstruktur aus 1.3.21 ist. Man zeige für die Dimension von $\mathrm{Hom}_k(V, W)$ unter der Konvention $0 \cdot \infty = \infty \cdot 0 = 0$ die Formel

$$\dim \mathrm{Hom}_k(V, W) = (\dim V)(\dim W)$$

Diese Formel ist insofern mit Vorsicht zu genießen, als sie bei einer feineren Interpretation der Dimension als Kardinalität im Fall unendlichdimensionaler Räume ihre Gültigkeit verliert. Hinweis: 1.5.13.

Übung 1.5.18. Man zeige: Gegeben Vektorräume $V_1, \ldots, V_n, W$ und lineare Abbildungen $f_i : V_i \to W$ erhalten wir auch eine lineare Abbildung $f : V_1 \oplus \ldots \oplus V_n \to W$ durch die Vorschrift $f(v_1, \ldots, v_n) = f_1(v_1) + \ldots + f_n(v_n)$. Auf diese Weise ergibt sich sogar einen Isomorphismus

$$\mathrm{Hom}(V_1, W) \oplus \ldots \oplus \mathrm{Hom}(V_n, W) \xrightarrow{\sim} \mathrm{Hom}(V_1 \oplus \ldots \oplus V_n, W)$$

dessen Umkehrabbildung wir auch in der Form $f \mapsto (f \circ \mathrm{in}_i)_i$ schreiben können.

Übung 1.5.19. Man zeige: Gegeben Vektorräume $V, W_1, \ldots, W_n$ und lineare Abbildungen $g_i : V \to W_i$ erhalten wir auch eine lineare Abbildung $g : V \to W_1 \oplus \ldots \oplus W_n$ durch die Vorschrift $g(v) = (g_1(v), \ldots, g_n(v))$. Auf diese Weise ergibt sich sogar einen Isomorphismus

$$\mathrm{Hom}(V, W_1) \oplus \ldots \oplus \mathrm{Hom}(V, W_n) \xrightarrow{\sim} \mathrm{Hom}(V, W_1 \oplus \ldots \oplus W_n)$$

dessen Umkehrabbildung wir auch in der Form $f \mapsto (\mathrm{pr}_i \circ f)_i$ schreiben können.

Definition 1.5.20. Zwei Teilräume U, W eines Vektorraums V heißen **komplementär** genau dann, wenn die Addition eine Bijektion

$$U \times W \xrightarrow{\sim} V$$

liefert. Nach 1.5.18 ist diese Abbildung dann unter Verwendung der in 1.3.10 eingeführten Notation sogar ein Vektorraumisomorphismus $U \oplus W \xrightarrow{\sim} V$. Man schreibt in diesem Fall auch abkürzend $V = U \oplus W$ und sagt, der Vektorraum V sei die **direkte Summe** oder genauer die **innere direkte Summe** der Teilräume U und W. Ebenso kürzt man allgemeiner auch für Teilräume $V_1, \ldots, V_n \subset V$ die Aussage, daß die Addition einen Isomorphismus $V_1 \oplus \ldots \oplus V_n \xrightarrow{\sim} V$ liefert, ab mit

$$V = V_1 \oplus \ldots \oplus V_n$$

und sagt dann, der Vektorraum V sei die **direkte Summe** oder genauer die **innere direkte Summe** der Teilräume V_i.

Übung 1.5.21. Man zeige, daß es in einem endlichdimensionalen Vektorraum zu jedem Untervektorraum einen, ja im allgemeinen sogar verschiedene komplementäre Untervektorräume gibt. Mutige zeigen es auch für nicht notwendig endlichdimensionale Vektorräume. Das benötigt jedoch den Basisergänzungssatz in seiner vollen Allgemeinheit 1.4.38, in der wir ihn nicht bewiesen, sondern als Axiom hingenommen haben.

Proposition 1.5.22. *1. Für jede injektive lineare Abbildung $f : V \hookrightarrow W$ existiert ein* **Linksinverses***, als da heißt eine lineare Abbildung $g : W \to V$ mit $g \circ f = \mathrm{id}_V$.*

2. Für jede surjektive lineare Abbildung $f : V \twoheadrightarrow W$ existiert ein **Rechtsinverses***, als da heißt eine lineare Abbildung $g : W \to V$ mit $f \circ g = \mathrm{id}_W$.*

Ergänzung 1.5.23. Einen unabhängigen Beweis noch allgemeinerer Aussagen diskutieren wir in 9.2.10.

Beweis. Der Beweis beider Aussagen benötigt den Basisergänzungssatz 1.4.38, den wir im unendlichdimensionalen Fall nicht bewiesen, sondern als Axiom hingenommen haben. Um Teil 1 zu zeigen, wählen wir mit 1.5.21 ein Komplement $U \subset W$ von $f(V)$ und definieren $g : W \to V$ durch die Vorschrift $g(u + f(v)) = v \quad \forall u \in U, v \in V$: Das ist erlaubt, da nach unsern Annahmen die Abbildung $(u, v) \mapsto u + f(v)$ eine Bijektion $U \times V \xrightarrow{\sim} W$ induziert. Um Teil 1 zu zeigen, wählen wir mithilfe des Basisexistenzsatzes 1.4.39 eine Basis $B \subset W$, finden $\tilde{g} : B \to V$ mit $f(\tilde{g}(b)) = b$ für alle $b \in B$ und erklären $g : W \to V$ als die eindeutig bestimmte lineare Abbildung mit $g(b) = \tilde{g}(b) \quad \forall b \in B$. Dann folgt $f(g(b)) = b \quad \forall b \in B$ und damit sofort $f(g(w)) = w \quad \forall w \in W$. □

Übung 1.5.24. Jede lineare Abbildung von einem Untervektorraum U eines Vektorraums V in einen weiteren Vektorraum $f : U \to W$ läßt sich zu einer linearen Abbildung $\tilde{f} : V \to W$ auf dem ganzen Raum fortsetzen. Hinweis: 1.5.22.

1.5.25. Die folgenden Übungen sind dazu gedacht, die Diskussion der Determinante und allgemeinerer multilinearer Abbildungen vorzubereiten. Sie stehen nur deshalb an dieser Stelle, da sie eben nicht mehr als die bis hierher erworbenen Kenntnisse voraussetzen.

Definition 1.5.26. Seien V, X, U Vektorräume über einem Körper k. Eine Abbildung $F : V \times X \to U$ heißt **bilinear** genau dann, wenn sie für jedes feste $v \in V$ linear ist in $x \in X$ und für jedes feste $x \in X$ linear in $v \in V$, in Formeln

$$\begin{aligned} F(v + w, x) &= F(v, x) + F(w, x) \\ F(\lambda v, x) &= \lambda F(v, x) \\ F(v, x + y) &= F(v, x) + F(v, y) \\ F(v, \mu x) &= \mu F(v, x) \end{aligned}$$

für alle $\lambda, \mu \in k$ und $v, w \in V$ und $x, y \in X$. Die Menge aller solchen bilinearen Abbildungen notieren wir

$$\mathrm{Hom}_k^{(2)}(V \times X, U) \subset \mathrm{Ens}(V \times X, U)$$

Diese Notation befriedigt mich unter formalen Aspekten nicht vollständig, da das Symbol $\times$ darin nicht als kartesisches Produkt, sondern vielmehr als ein Trenner aufzufassen ist. Ich habe sie dennoch gewählt in der Hoffnung, daß sie sich leichter merken und lesen läßt als eine unter formalen Aspekten bessere Notation wie zum Beispiel $\mathrm{Hom}_k^{(2)}(V, X; U)$.

Übung 1.5.27. Seien U, V, W Vektorräume und $A \subset U$ sowie $B \subset V$ jeweils Basen. So liefert die Einschränkung eine Bijektion

$$\mathrm{Hom}_k^{(2)}(U \times V, W) \xrightarrow{\sim} \mathrm{Ens}(A \times B, W)$$

In Worten ist also eine bilineare Abbildung festgelegt und festlegbar durch ihre Werte auf Paaren von Basisvektoren. Hinweis: Man orientiere sich am Beweis von 1.5.13.

Übung 1.5.28. Man zeige, daß für je drei Vektorräume U, V, W die Verknüpfung von linearen Abbildungen $\mathrm{Hom}(U, V) \times \mathrm{Hom}(V, W) \to \mathrm{Hom}(U, W)$ bilinear ist. Hier sind unsere Homomorphismenräume zu verstehen mit ihrer in 1.5.17 erklärten Vektorraumstruktur.

Übung 1.5.29. Gegeben Vektorräume U, V, W induziert die kanonische Identifikation $\mathrm{Ens}(U \times V, W) \xrightarrow{\sim} \mathrm{Ens}(U, \mathrm{Ens}(V, W))$ aus I.2.2.26 einen Isomorphismus $\mathrm{Hom}^{(2)}(U \times V, W) \xrightarrow{\sim} \mathrm{Hom}(U, \mathrm{Hom}(V, W))$ zwischen dem Raum der bilinearen Abbildungen $U \times V \to W$ und dem Raum der linearen Abbildungen $U \to \mathrm{Hom}(V, W)$.

1.6 Dimensionsformel

Definition 1.6.1. Das **Bild** einer linearen Abbildung $f : V \to W$ notiert man auch

$$\mathrm{im}(f) := f(V) = \{w \in W \mid \exists v \in V \text{ mit } f(v) = w\}$$

für französisch und englisch **image**. Es ist nach 1.5.6 ein Untervektorraum von W. Das Urbild des Nullvektors unter einer linearen Abbildung $f : V \to W$ notiert man auch

$$\ker(f) := f^{-1}(0) = \{v \in V \mid f(v) = 0\}$$

und nennt es den **Kern** der linearen Abbildung f. Der Kern ist nach 1.5.6 ein Untervektorraum von V.

Übung 1.6.2. Der Kern einer von Null verschiedenen linearen Abbildung in den Grundkörper ist stets eine Hyperebene im Sinne von 1.3.24.

Lemma 1.6.3. *Eine lineare Abbildung $f : V \to W$ ist injektiv genau dann, wenn ihr Kern Null ist.*

1.6.4. Etwas allgemeiner werden wir dies Resultat in 2.2.14 nocheinmal für beliebige Gruppenhomomorphismen zeigen.

Beweis. Liegen im Kern außer dem Nullvektor von V noch andere Vektoren, so werden verschieden Vektoren aus V unter f auf den Nullvektor von W abgebildet und unsere Abbildung ist nicht injektiv. Ist umgekehrt unsere Abbildung nicht injektiv, so gibt es $v \neq v_1$ in V mit $f(v) = f(v_1)$ und es folgt $f(v - v_1) = 0$ aber $v - v_1 \neq 0$. Mit $v - v_1$ liegt also ein von Null verschiedener Vektor im Kern, der folglich nicht der Nullraum sein kann. □

Ergänzende Übung 1.6.5. Die idempotenten Endomorphismen eines Vektorraums entsprechen eineindeutig seinen Zerlegungen in eine direkte Summe von zwei komplementären Teilräumen. Gegeben ein Vektorraum V liefert genauer die Abbildung $f \mapsto (\operatorname{im} f, \ker f)$ eine Bijektion

$$\{f \in \operatorname{End} V \mid f^2 = f\} \xrightarrow{\sim} \left\{ (I,K) \in \mathcal{P}(V)^2 \;\middle|\; \begin{array}{c} I, K \subset V \text{ sind Teilräume} \\ \text{mit } I \oplus K = V \end{array} \right\}$$

Ein Endomorphismus f eines Vektorraums mit der Eigenschaft $f^2 = f$ heißt auch **idempotent**. Für die Umkehrabbildung sagt man, sie ordne einer Zerlegung $V = I \oplus K$ die **Projektion von** V **auf** I **längs** K zu.

Übung 1.6.6. Gegeben eine lineare Abbildung $f : V \to W$ gilt für alle $v \in V$ die Identität $f^{-1}(f(v)) = v + \ker f$ von Teilmengen von V.

Definition 1.6.7. Eine Teilmenge T eines Vektorraums V heißt ein **affiner Teilraum** genau dann, wenn es einen Vektor $v \in V$ und einen Untervektorraum $U \subset V$ gibt mit $T = v + U$.

1.6.8. Manche Autoren definieren affine Teilräume abweichend so, daß auch die leere Menge ein affiner Teilraum ist.

1.6.9. Ist $f : V \to W$ eine lineare Abbildung, so ist also für alle $w \in W$ die Faser $f^{-1}(w)$ entweder leer oder aber ein affiner Teilraum von V. Wir diskutieren in 1.7.18 affine Teilräume beliebiger "affiner Räume". Der hier definierte Begriff wird sich dann als ein Spezialfall erweisen.

Übung 1.6.10. Ist $f : V \to W$ eine lineare Abbildung, so ist für jeden affinen Teilraum $A \subset W$ sein Urbild $f^{-1}(A)$ entweder leer oder aber ein affiner Teilraum von V.

Übung 1.6.11. Sei $p : V \twoheadrightarrow W$ eine surjektive lineare Abbildung. Genau dann ist ein Teilraum $U \subset V$ komplementär zu $\ker p$, wenn p einen Isomorphismus $p : U \xrightarrow{\sim} W$ induziert.

Satz 1.6.12. *Für jede lineare Abbildung $f : V \to W$ von Vektorräumen gilt die* **Dimensionsformel**

$$\dim V = \dim(\ker f) + \dim(\operatorname{im} f)$$

Beweis. Ist V endlich erzeugt, so ist auch $(\operatorname{im} f)$ endlich erzeugt, da ja für jedes Erzeugendensystems $E \subset V$ sein Bild $f(E)$ ein Erzeugendensystem von $f(V) = \operatorname{im} f$ ist. Ebenso ist mit V auch $(\ker f)$ endlich erzeugt, nach dem Korollar 1.4.29 ist ja sogar jeder Untervektorraum eines endlich erzeugten Vektorraums endlich erzeugt. Gilt also umgekehrt $\dim(\ker f) = \infty$ oder $\dim(\operatorname{im} f) = \infty$, so folgt $\dim V = \infty$ und unser Satz gilt. Wir brauchen ihn also nur noch in dem Fall zu zeigen, daß $(\ker f)$ und $(\operatorname{im} f)$ beide endlichdimensional sind. In diesem Fall folgt er aus dem anschließenden präziseren Lemma 1.6.13. Alternativ kann man auch mit Übung 1.6.14 argumentieren. □

Lemma 1.6.13. *Sei $f : V \to W$ eine lineare Abbildung. Ist A eine Basis ihres Kerns, B eine Basis ihres Bildes und $g : B \to V$ eine Wahl von Urbildern unserer Basis des Bildes, so ist $g(B) \cup A$ eine Basis von V.*

Beweis. Gegeben $\vec{v} \in V$ haben wir $f(\vec{v}) = \lambda_1\vec{w}_1 + \ldots + \lambda_r\vec{w}_r$ mit $\vec{w}_i \in B$. Offensichtlich liegt dann $\vec{v} - \lambda_1 g(\vec{w}_1) - \ldots - \lambda_r g(\vec{w}_r)$ im Kern von f und so folgt, daß $g(B) \cup A$ ganz V erzeugt. Um die lineare Unabhängigkeit zu zeigen nehmen wir an, es gelte

$$\lambda_1 g(\vec{w}_1) + \ldots + \lambda_r g(\vec{w}_r) + \mu_1\vec{v}_1 + \ldots + \mu_s\vec{v}_s = 0$$

mit den $\vec{v}_i \in A$ und $\vec{w}_j \in B$ paarweise verschieden. Wenden wir f an, so folgt $\lambda_1\vec{w}_1 + \ldots + \lambda_r\vec{w}_r = 0$ und damit $\lambda_1 = \ldots = \lambda_r = 0$ wegen der linearen Unabhängigkeit der $\vec{w}_i$. Setzen wir diese Erkenntnis in die ursprüngliche Gleichung ein, so folgt weiter $\mu_1 = \ldots = \mu_s = 0$ wegen der linearen Unabhängigkeit der Vektoren $\vec{v}_j$. □

Übung 1.6.14. Sei $f : V \to W$ eine lineare Abbildung. Man zeige: Ist $\vec{v}_1, \ldots, \vec{v}_s$ eine Basis des Kerns $\ker f$ und $\vec{v}_{s+1}, \ldots, \vec{v}_n$ eine Erweiterung zu einer linear unabhängigen Teilmenge von V, so ist die Familie $f(\vec{v}_{s+1}), \ldots, f(\vec{v}_n)$ linear unabhängig in W. Ist unsere Erweiterung sogar eine Basis von V, so ist unsere Familie eine Basis des Bildes von f.

Korollar 1.6.15 (Dimensionssatz). *Gegeben ein Vektorraum V und Teilräume $U, W \subset V$ mit endlichdimensionalem Schnitt gilt*

$$\dim(U + W) = \dim U + \dim W - \dim(U \cap W)$$

Beweis. Wir haben diesen Satz bereits in 1.4.31 sozusagen zu Fuß bewiesen. Mit unserer Dimensionsformel 1.6.12 können wir nun noch einen alternativen Beweis geben. Betrachtet man nämlich die lineare Abbildung

$$f : U \oplus W \to V$$

gegeben durch $f(u, w) = u + w$, so gilt $(\operatorname{im} f) = U + W$ und die Abbildung $d \mapsto (d, -d)$ definiert einen Isomorphismus $(U \cap W) \xrightarrow{\sim} \ker f$. Die Formel 1.4.35 für die Dimension der direkten Summe in Verbindung mit der Dimensionsformel liefert so

$$\dim U + \dim W = \dim(U \oplus W) = \dim(U \cap W) + \dim(U + W) \qquad \square$$

Übung 1.6.16. Man zeige: Zwei Untervektorräume U, W eines Vektorraums V sind komplementär genau dann, wenn gilt $V = U + W$ und $U \cap W = 0$.

Übung 1.6.17. Man zeige: Zwei Untervektorräume U, W eines endlichdimensionalen Vektorraums V sind komplementär genau dann, wenn gilt $V = U + W$ und $\dim U + \dim W \leq \dim V$. Hinweis: 1.4.35.

Ergänzende Übung 1.6.18. Sei $\varphi : V \to V$ ein Endomorphismus eines endlichdimensionalen Vektorraums. Man zeige, daß $\ker(\varphi^2) = \ker \varphi$ gleichbedeutend ist zu $V = \ker \varphi \oplus \operatorname{im} \varphi$.

1.7 Affine Räume

Definition 1.7.1. Ein **affiner Raum** oder kurz **Raum** über einem Körper k ist ein Tripel

$$E = (E, \vec{E}, a)$$

bestehend aus einer nichtleeren Menge E, einer abelschen Untergruppe $\vec{E} \subset \operatorname{Ens}^\times E$ der Gruppe der Permutationen von E, von der man fordert, daß für alle $p \in E$ das Anwenden auf p eine Bijektion $\vec{E} \xrightarrow{\sim} E, \vec{v} \mapsto \vec{v}(p)$ besagter Gruppe mit unserem Raum liefert, sowie einer Abbildung $a : k \times \vec{E} \to \vec{E}$, die die abelsche Gruppe $\vec{E}$ zu einem k-Vektorraum macht. Die Elemente von $\vec{E}$ heißen die **Translationen** oder **Richtungsvektoren** unseres affinen Raums und den Vektorraum $\vec{E}$ selbst nennen wir den **Richtungsraum** unseres affinen Raums E. Die Operation von k auf $\vec{E}$ mag man die **Reskalierung von Translationen** nennen. Unter der **Dimension** eines affinen Raums verstehen wir die Dimension seines Richtungsraums. Das Resultat der Operation von $\vec{v} \in \vec{E}$ auf $p \in E$ notieren wir $\vec{v} + p := \vec{v}(p)$ oder manchmal auch $p + \vec{v}$.

1.7.2. Einen affinen Raum über dem Körper $\mathbb{R}$ der reellen Zahlen nenne ich auch einen **reellen affinen Raum** oder kurz **reellen Raum**.

1.7.3. Hier entsteht leider ein Konflikt mit der Notation aus **??**, nach der mit Pfeilen versehene Mannigfaltigkeiten orientierte Mannigfaltigkeiten andeuten sollen. Was im Einzelfall jeweils gemeint ist, muß der Leser aus dem Kontext erschließen. Die leere Menge kann in meinen Konventionen nie ein affiner Raum sein. Es gibt hier jedoch auch andere Konventionen. Unser Richtungsraum wird in manchen Quellen auch der **Differenzraum** des affinen Raums genannt.

1.7.4. Ein affiner Raum hat die Dimension Null genau dann, wenn er aus einem einzigen Punkt besteht. Affine Räume der Dimensionen Eins bzw. Zwei heißen **affine Geraden** bzw. **affine Ebenen**.

1.7.5. Ist E ein affiner Raum, so liefert nach Annahme für jedes $p \in E$ das Anwenden der Richtungsvektoren auf besagten Punkt eine Bijektion $\vec{E} \xrightarrow{\sim} E$, $\vec{v} \mapsto \vec{v}+p$ und es gilt $\vec{0}+p = p$ sowie $\vec{u}+(\vec{v}+p) = (\vec{u}+\vec{v})+p$ für alle $\vec{u},\vec{v} \in \vec{E}$ und $p \in E$. Flapsig gesprochen ist also ein affiner Raum schlicht ein "Vektorraum, bei dem man den Ursprung vergessen hat". Gegeben $p, q \in E$ definieren wir $p - q$ als denjenigen Richtungsvektor $\vec{u} \in \vec{E}$ mit $p = \vec{u} + q$. In Schulbüchern verwendet man auch oft Großbuchstaben $A, B, C, \ldots$ für die Punkte eines affinen Raums und notiert den Richtungsvektor, der A nach B schiebt und den wir hier $B - A$ schreiben, als $\overrightarrow{AB}$.

1.7.6 (**Vektorräume als affine Räume**). Jeder Vektorraum V kann als ein affiner Raum aufgefaßt werden, indem wir als Translationen die durch die Addition von festen Vektoren gegebenen Abbildungen nehmen, so daß unsere Gruppe von Translationen das Bild des injektiven Gruppenhomomorphismus $V \to \mathrm{Ens}^{\times}(V)$, $v \mapsto (v+\ )$ wird, und die Reskalierung von Translationen dadurch erklären, daß dieser Gruppenhomomorphismus einen Vektorraumisomorphismus auf sein Bild liefern soll. Insbesondere erhalten wir damit eine kanonische Identifikation $\mathrm{trans} : V \xrightarrow{\sim} \vec{V}$ zwischen unserem Vektorraum und dem Richtungsraum des aus unserem Vektorraum gebildeten affinen Raums. Diese Identifikation scheint mir derart kanonisch, daß ich sie von nun an in Sprache und Notation oft so behandeln werde, als seien diese beiden Vektorräume schlicht gleich.

Beispiel 1.7.7. Es scheint mir besonders sinnfällig, den "Raum unserer Anschauung" mathematisch als einen dreidimensionalen reellen affinen Raum

$$\mathbb{E}$$

zu modellieren. Dieses Modell werden wir in 4.1 noch um die Vorgabe einer ausgezeichneten "Bewegungsgruppe" und "Orientierung" erweitern und dann in 4.1.15 den "Anschauungsraum" formal als ein Gebilde der Mengenlehre definieren. Diese endgültige Definition muß aber noch auf die Einführung der fehlenden Begriffe warten. Der Buchstabe $\mathbb{E}$ soll an das französische Wort "éspace" für "Raum" erinnern. Mit dem "Raum unserer Anschauung" meine ich den "Raum

der klassischen Mechanik". Manche Punkte dieses Raums können wir uns direkt als Kirchturmspitzen, Zimmerecken und dergleichen denken, die Übrigen gilt es sich vorzustellen. Wir ignorieren dabei, daß die Erde sich um sich selber dreht und dabei gleichzeitig um die Sonne rast, die sich hinwiederum mit unvorstellbarer Geschwindigkeit um das Zentrum der Milchstraße bewegt, und damit ist es auch noch nicht zu Ende. Den zum Raum unserer Anschauung gehörigen Richtungsraum denkt man sich dann als die Gesamtheit aller "Parallelverschiebungen des Raums der Anschauung". In 1.7.34 werden wir lernen, in welchem Sinne die Bedingung, daß unsere Sichtlinien gerade den "affinen Geraden" entsprechen sollen, die Struktur als reeller affiner Raum bereits eindeutig festlegt. Daß wir als Grundkörper für die Modellierung des Raums der Anschauung den Körper der reellen Zahlen nehmen, hat analytische Gründe: Im Kern liegen sie darin, daß für diesen Körper der Zwischenwertsatz **??** gilt. Deshalb modellieren reelle Vektorräume, insbesondere wenn es später auch um Drehungen, Winkel im Bogenmaß und dergleichen gehen wird, unsere geometrische Anschauung besser als etwa Vektorräume über den rationalen Zahlen oder allgemeineren Teilkörpern von $\mathbb{R}$.

Beispiel 1.7.8. Man mag sich in ähnlicher Weise auch die Schreibfläche einer in jeder Richtung unbegrenzten Tafel als einen zweidimensionalen reellen affinen Raum denken.

Beispiel 1.7.9. Die Menge aller **Zeitpunkte** der klassischen Mechanik mag man mathematisch als einen eindimensionalen reellen affinen Raum

$$\mathbb{T}$$

modellieren. Dieses Modell werden wir zu gegebener Zeit noch durch die Vorgabe einer ausgezeichneten Orientierung erweitern und Zeit erst in 3.2.9 fertig werden, wo wir den Begriff der Orientierung diskutieren. Der Buchstabe $\mathbb{T}$ soll an das lateinische Wort "tempus" für "Zeit" erinnern. Eine mögliche Translation in diesem Raum wäre etwa die Vorschrift: Man warte von einem vorgegebenen Zeitpunkt sieben Ausschläge eines bestimmten Pendels ab, dann erreicht man den um diese Translation verschobenen Zeitpunkt. Die Elemente des Richtungsraums $\vec{\mathbb{T}}$ dieses affinen Raums hätte man sich als "Zeitspannen" zu denken, wobei jedoch auch "negative Zeitspannen" zuzulassen wären. Die Flugbahn einer Fliege etwa würden wir durch eine Abbildung $\mathbb{T} \to \mathbb{E}$ oder genauer, da Fliegen ja sterblich sind, durch die Abbildung einer geeigneten Teilmenge $I \subset \mathbb{T}$ nach $\mathbb{E}$ beschreiben.

Ergänzung 1.7.10. Ein Vektor des Homomorphismenraums $\mathrm{Hom}(\vec{\mathbb{T}}, \vec{\mathbb{E}})$ nach 1.5.17 modelliert, was man in der Physik eine **vektorielle Geschwindigkeit** nennt.

1.7.11. Vielfach findet man die begriffliche Variante eines **affinen Raums über einem vorgegebenen Vektorraum**: Darunter versteht man dann eine Menge E mit einer "freien transitiven Wirkung" des vorgegebenen Vektorraums. Ich ziehe die oben gegebene Definition vor, da sie jeden Bezug auf einen vorgegebenen

Vektorraum vermeidet und den Anschauungsraum meines Erachtens besser modelliert.

Definition 1.7.12. Eine Abbildung $\varphi : E \to E'$ zwischen affinen Räumen heißt eine **affine Abbildung** genau dann, wenn es eine lineare Abbildung zwischen den zugehörigen Richtungräumen $\vec{\varphi} : \vec{E} \to \vec{E}'$ gibt mit

$$\varphi(p) - \varphi(q) = \vec{\varphi}(p - q) \quad \forall p, q \in E$$

Diese lineare Abbildung $\vec{\varphi}$ ist dann durch φ eindeutig bestimmt und heißt der **lineare Anteil** unserer affinen Abbildung. Eine bijektive affine Abbildung heißt auch ein **Isomorphismus von affinen Räumen**, ein Isomorphismus von einem affinen Raum auf sich selbst heißt ein **Automorphismus** von besagtem affinen Raum. Die Menge aller affinen Abbildungen von einem affinen Raum E in einen affinen Raum F notieren wir

$$\mathrm{Aff}(E, F) = \mathrm{Aff}_k(E, F)$$

Beispiel 1.7.13. Eine Abbildung $\varphi : V \to W$ zwischen Vektorräumen ist affin genau dann, wenn es eine lineare Abbildung $\vec{\varphi} : V \to W$ und einen Punkt $w \in W$ gibt mit $\varphi(v) = w + \vec{\varphi}(v)$ für alle $v \in V$.

Übung 1.7.14. Die Verknüpfung affiner Abbildungen ist affin und der lineare Anteil einer Verknüpfung affiner Abbildungen ist die Verknüpfung ihrer linearen Anteile.

Übung 1.7.15. Beschreiben Sie in Worten eine affine Abbildung $\mathbb{T} \to \mathbb{E}$ des affinen Raums der Zeiten in den Anschauungsraum. Natürlich ist das keine mathematische Übung im eigentlichen Sinne!

Übung 1.7.16. Man zeige: Gegeben affine Räume $X_1, \ldots, X_n$ gibt es auf ihrem kartesischen Produkt $X_1 \times \ldots \times X_n$ genau eine Struktur als affiner Raum derart, daß die Projektionen pr_i affin sind. Des weiteren liefern dann die linearen Anteile der Projektionen mit 1.5.19 einen Isomorphismus zwischen dem Richtungsraum des Produkts und dem Produkt der Richtungsräume der Faktoren.

Bemerkung 1.7.17. Nach der reinen Lehre sollte eine Teilmenge eines affinen Raums ein "affiner Teilraum" heißen genau dann, wenn sie so mit der Struktur eines affinen Raums versehen werden kann, daß die Einbettung eine affine Abbildung wird. Da diese Definition jedoch für Anwendungen erst aufgeschlüsselt werden muß, nehmen wir als unsere Definition gleich die aufgeschlüsselte Fassung und überlassen dem Leser den Nachweis der Äquivalenz zur Definition aus der reinen Lehre als Übung 1.7.20.

Definition 1.7.18. Eine Teilmenge $F \subset E$ eines affinen Raums heißt ein **affiner Teilraum** genau dann, wenn es einen Punkt $p \in E$ und einen Untervektorraum $W \subset \vec{E}$ gibt mit

$$F = p + W$$

Die durch Restriktion gegebene Abbildung $W \to \mathrm{Ens}^\times F$ ist dann eine Injektion und wir erklären wir auf F die Struktur eines affinen Raums, indem wir als Richtungsraum $\vec{F}$ das Bild von W in $\mathrm{Ens}^\times F$ nehmen und diese abelsche Gruppe mit derjenigen Struktur eines k-Vektorraums versehen, für die Restriktion $W \xrightarrow{\sim} \vec{F}$ ein Vektorraumisomorphismus ist.

Beispiel 1.7.19. Die affinen Teilräume des $\mathbb{R}^3$ sind genau: Alle einelementigen Teilmengen, alle Geraden $G = p + \mathbb{R}\vec{v}$ mit $\vec{v} \neq \vec{0}$, alle Ebenen $P = p + \mathbb{R}\vec{v} + \mathbb{R}\vec{w}$ mit $\vec{v}, \vec{w}$ linear unabhängig, und der ganze $\mathbb{R}^3$.

Ergänzende Übung 1.7.20. Sei E ein affiner Raum. Genau dann ist eine Teilmenge $F \subset E$ ein affiner Teilraum im Sinne von 1.7.18, wenn F eine Struktur als affiner Raum $(F, \vec{F}, b)$ besitzt derart, daß die Einbettung eine affine Abbildung ist. Die fragliche affine Struktur auf F ist dadurch dann eindeutig bestimmt.

1.7.21. Eine Teilmenge eines affinen Raums heißt eine **Gerade** oder genauer eine **affine Gerade** genau dann, wenn sie ein affiner Teilraum der Dimension Eins ist. Eine Teilmenge eines affinen Raums heißt eine **Ebene** oder genauer eine **affine Ebene** genau dann, wenn sie ein affiner Teilraum der Dimension Zwei ist.

1.7.22 (**Anschauliche Interpretation linearer Gleichungssysteme**). Wählen wir im Anschauungsraum $\mathbb{E}$ einen festen Punkt p als **Ursprung** und eine Basis $\vec{v}_1$, $\vec{v}_2$, $\vec{v}_3$ seines Richtungsraums, so erhalten wir eine Bijektion

$$\mathbb{R}^3 \xrightarrow{\sim} \mathbb{E}$$

vermittels der Abbildungsvorschrift $(x, y, z) \mapsto p + x\vec{v}_1 + y\vec{v}_2 + z\vec{v}_3$. Die Abbildungen $\mathbb{E} \to \mathbb{R}$, die jedem Punkt die Komponenten seines Urbilds unter dieser Identifikation zuordnen, heißen auch **Koordinaten** und in ihrer Gesamtheit ein **Koordinatensystem auf** $\mathbb{E}$. Unter jeder derartigen Identifikation des $\mathbb{R}^3$ mit dem Raum unserer Anschauung kann man sich die Lösungsmenge einer homogenen linearen Gleichung in drei Unbekannten als eine Ebene durch den Ursprung denken, wenn man einmal von der "Nullgleichungen" absieht, und die Lösungsmenge einer nicht notwendig homogenen linearen Gleichung in drei Unbekannten als eine affine Ebene, wenn man wieder von dem Fall der "Nullgleichung" absieht, bei denen die Koeffizienten von x, y, z alle drei verschwinden. Die Lösungsmenge eines linearen Gleichungssystems ohne Nullgleichung kann man sich demnach veranschaulichen als den Schnitt einiger affiner Ebenen, eben der Lösungsmengen seiner einzelnen Gleichungen. So sieht man auch anschaulich ein, daß die

Lösungsmenge eines linearen Gleichungssystems ohne Nullgleichung mit zwei Gleichungen in drei Veränderlichen im Allgemeinen einen eindimensionalen Lösungsraum haben wird, da sich eben zwei Ebenen im Raum im Allgemeinen in einer Gerade schneiden, daß aber als Lösungsraum auch die leere Menge in Frage kommt, als Schnitt zweier paralleler Ebenen, und eine Ebene, wenn nämlich die Lösungsräume unserer beiden Gleichungen übereinstimmen.

1.7.23. Eine Teilmenge eines affinen Raums heißt eine **Hyperebene** oder genauer eine **affine Hyperebene** genau dann, wenn sie ein echter affiner Teilraum ist, dessen Richtungsraum im Sinne von 1.3.24 eine lineare Hyperebene im Richtungsraum unseres ursprünglichen affinen Raums ist.

1.7.24. Gegeben ein affiner Raum E mit einem affinen Teilraum $F \subset E$ verwenden wir von nun an das Symbol $\vec{F}$ auch für den Untervektorraum von $\vec{E}$, den wir als das Bild des Richtungsraums $\vec{F}$ von F unter dem linearen Anteil der Einbettung erhalten.

1.7.25. Ein nichtleerer Schnitt von affinen Teilräumen eines affinen Raums ist stets wieder ein affiner Teilraum, und der Richtungsraum des Schnitts ist der Schnitt der Richtungsräume, zumindest wenn wir alle diese Räume wie in 1.7.24 als Teilmengen des Richtungsraums unseres ursprünglichen Raums betrachten.

Definition 1.7.26. Zwei affine Teilräume $T, S \subset E$ eines affinen Raums E heißen **parallel** genau dann, wenn in $\vec{E}$ gilt $\vec{T} \subset \vec{S}$ oder $\vec{S} \subset \vec{T}$.

1.7.27. Die Konventionen scheinen in der Literatur nicht ganz eindeutig zu sein. Die hier gegebene Definition von Parallelität hat den Vorteil, die üblichen Definitionen für die Parallelität von Geraden oder Ebenen im zweidimensionalen wie im dreidimensionalen Raum zu liefern bis auf das Detail, daß damit auch ein Enthaltensein als Parallelität gilt. Allerdings hat sie den Nachteil, daß ein Punkt zu jedem weiteren Teilraum parallel ist, was meinem Sprachempfinden zuwiderläuft.

Definition 1.7.28. Gegeben eine nichtleere Teilmenge eines affinen Raums gibt es nach 1.7.25 einen kleinsten affinen Teilraum, der sie umfaßt. Wir bezeichnen ihn als den **von unserer Teilmenge erzeugten** affinen Teilraum. Ein **Erzeugendensystem** eines affinen Raums ist eine Teilmenge, die ihn erzeugt.

Übung 1.7.29. Durch je zwei verschiedene Punkte eines affinen Raums geht genau eine Gerade, als da heißt, es gibt genau einen affinen Teilraum der Dimension Eins, der unsere beiden Punkte enthält. Bringt man also Kimme und Korn in eine Sichtlinie mit dem Ziel, so ist das Gewehr bereits auf das Ziel ausgerichtet.

Übung 1.7.30. Durch je drei Punkte eines affinen Raums, die nicht auf einer Geraden liegen, geht genau eine Ebene. Insbesondere wird also ein dreibeiniger Hocker nie kippeln.

Übung 1.7.31. Der von einer nichtleeren endlichen Teilmenge T eines affinen Raums erzeugte Teilraum hat höchstens die Dimension $|T| - 1$.

Übung 1.7.32. Gegeben zwei endlichdimensionale affine Teilräume A, B eines affinen Raums E gilt für die Dimension des affinen Erzeugnisses C ihrer Vereinigung die Formel

$$\dim C = \begin{cases} \dim A + \dim B - \dim(A \cap B) & \text{falls } A \cap B \neq \emptyset; \\ \dim A + \dim B - \dim(\vec{A} \cap \vec{B}) + 1 & \text{falls } A \cap B = \emptyset. \end{cases}$$

Satz 1.7.33 (Charakterisierung affiner Abbildungen). *Eine injektive Abbildung von einem mindestens zweidimensionalen reellen affinen Raum in einen weiteren reellen affinen Raum ist affin genau dann, wenn das Bild jeder Geraden unter unserer Abbildung wieder eine Gerade ist.*

1.7.34. Die affinen Geraden des Raums unserer Anschauung denken wir uns als Sichtlinien. Der vorhergehende Satz 1.7.33 zeigt, daß im Fall reeller affiner Räume ab der Dimension Zwei die Kenntnis aller Geraden auch umgekehrt bereits die Struktur als reeller affiner Raum festlegt: Haben nämlich zwei Strukturen als affiner reeller Raum auf derselben Menge dieselben Geraden, und gibt es in besagtem Raum mehr als nur eine Gerade, so ist nach 1.7.33 die Identität auf unserer Menge ein Morphismus zwischen ihr einmal mit der einen Struktur als affiner Raum und ein andermal mit der anderen Struktur als affiner Raum. Dann aber müssen diese beiden Strukturen bereits übereinstimmen. Anschaulich gesprochen legt also im Raum unserer Anschauung “die Kenntnis der Sichtlinien bereits fest, welche Abbildungen als Parallelverschiebungen anzusehen sind”. Explizit kann man das wie folgt einsehen: Zunächst legt die Kenntnis der Sichtlinien alias Geraden fest, welche Teilmengen die Bezeichung als “Ebene” verdienen; Dann vereinbart man, zwei Geraden “parallel” zu nennen, wenn sie in einer Ebene liegen und sich nicht schneiden; Und schließlich kann man dann Parallelverschiebungen charakterisieren als diejenigen bijektiven Abbildungen, die jede Gerade bijektiv auf sich selbst oder aber bijektiv in eine parallele Gerade überführen. An dieser Stelle möchte ich Sie am liebsten wieder einmal davon überzeugen, daß das Abstrakte das eigentlich Konkrete ist.

Beweis. Wir zeigen den Satz zunächst unter der Annahme, daß sowohl unser Ausgangsraum als auch der Raum, in den abgebildet wird, beide die Dimension Zwei haben. Ohne Beschränkung der Allgemeinheit dürfen wir dann annehmen, daß es sich bei beiden Räumen um den $\mathbb{R}^2$ handelt, und indem wir unsere Abbildung noch mit einer geeigneten Verschiebung verknüpfen, dürfen wir sogar annehmen, daß sie den Ursprung festhält. Diesen Fall behandeln wir als eigenständiges Lemma.

Lemma 1.7.35. *Eine injektive Abbildung $\Phi : \mathbb{R}^2 \to \mathbb{R}^2$ mit $\Phi(0) = 0$, unter der das Bild jeder affinen Geraden wieder eine affine Gerade ist, muß linear sein.*

Beweis. Halten wir eine geeignete lineare Abbildung dahinter, so erkennen wir, daß wir ohne Beschränkung der Allgemeinheit annehmen dürfen, daß unser Φ die Vektoren e_1 und e_2 der Standardbasis festhält. Unter dieser Zusatzannahme gilt es nun zu zeigen, daß Φ die Identität ist. Zunächst gibt es sicher Abbildungen $\psi_1, \psi_2 : \mathbb{R} \to \mathbb{R}$ mit $\Phi(a\mathrm{e}_i) = \psi_i(a)\,\mathrm{e}_i$. Da wir Φ injektiv angenommen haben, müssen unter Φ parallele alias sich nicht schneidende Geraden parallel bleiben. Die Gerade durch $a\mathrm{e}_1$ und $a\mathrm{e}_2$ für $a \neq 0, 1$ ist parallel zu der durch e_1 und e_2, also ist für $a \neq 0, 1$ auch die Gerade durch $\Phi(a\mathrm{e}_1) = \psi_1(a)\,\mathrm{e}_1$ und $\Phi(a\mathrm{e}_2) = \psi_2(a)\,\mathrm{e}_2$ parallel zu der durch $\Phi(\mathrm{e}_1) = \mathrm{e}_1$ und $\Phi(\mathrm{e}_2) = \mathrm{e}_2$. Es folgt $\psi_1(a) = \psi_2(a)$ für $a \neq 0, 1$. Für $a = 0, 1$ ist das eh klar und wir notieren diese Abbildung nun ψ. Natürlich gilt $\psi(0) = 0$ und $\psi(1) = 1$. Da man die Addition von linear unabhängigen Vektoren durch Parallelogramme darstellen kann, gilt $\Phi(v + w) = \Phi(v) + \Phi(w)$ falls v und w linear unabhängig sind. Wir erhalten für $a \in \mathbb{R}$ damit

$$\Phi(\mathrm{e}_1 + a\,\mathrm{e}_2) \;=\; \mathrm{e}_1 + \psi(a)\,\mathrm{e}_2$$

im Fall $a \neq 0$ wegen der linearen Unabhängigkeit und im Fall $a = 0$ wegen $\psi(0) = 0$. Daraus folgern wir

$$\begin{aligned}\Phi(\mathrm{e}_1 + (a+b)\,\mathrm{e}_2) &= \mathrm{e}_1 + \psi(a+b)\,\mathrm{e}_2\\ \Phi(\mathrm{e}_1 + a\,\mathrm{e}_2 + b\,\mathrm{e}_2) &= \mathrm{e}_1 + \psi(a)\,\mathrm{e}_2 + \psi(b)\,\mathrm{e}_2\end{aligned}$$

indem wir bei der zweiten Gleichung ohne Beschränkung der Allgemeinheit $b \neq 0$ annehmen und erst den letzten Summanden abspalten. Es folgt sofort $\psi(a + b) = \psi(a) + (b)$. Da für $a, b \in \mathbb{R}$ mit $a \neq 0$ und $b \neq 0, 1$ die Gerade durch e_1 und $a\mathrm{e}_2$ parallel ist zu der durch $b\mathrm{e}_1$ und $ab\mathrm{e}_2$ folgt auch $\psi(ab) = \psi(a)\psi(b)$ erst für alle $a, b \neq 0, 1$, dann aber wegen $\psi(0) = 0$ und $\psi(1) = 1$ sogar für alle $a, b \in \mathbb{R}$. Da nach **??.??** oder besser **??** die Identität der einzige Körperhomomorphismus $\psi : \mathbb{R} \to \mathbb{R}$ ist, folgt $\psi = \mathrm{id}$. Da wie bereits erwähnt gilt $\Phi(v+w) = \Phi(v)+\Phi(w)$ falls v und w linear unabhängig sind, folgt sofort $\Phi = \mathrm{id}$. □

Um nun Satz 1.7.33 zu zeigen, sei $\Phi : E \hookrightarrow F$ unsere injektive Abbildung von reellen affinen Räumen, unter der das Bild jeder Geraden eine Gerade ist. Sei ein Punkt $e \in E$ fest gewählt und seien $\vec{v}, \vec{w} \in \vec{E}$ linear unabhängig. Die Bilder von $e, e + \vec{v}$ und $e + \vec{w}$ können nicht auf einer Geraden liegen, da sonst zwei verschiedene Geraden auf dieselbe Gerade abgebildet würden im Widerspruch zur Injektivität von Φ. Folglich erzeugen diese Bilder eine affine Ebene. Die von $e, e+\vec{v}, e + \vec{w}$ aufgespannte affine Ebene kann beschrieben werden als die Vereinigung aller Geraden, die durch einen von e verschiedenen Punkt der Gerade $e + \mathbb{R}\vec{v}$

sowie durch einen Punkt der Geraden $e+\mathbb{R}\vec{w}$ laufen. Diese Ebene wird dann von Φ bijektiv abgebildet auf die von $\Phi(e), \Phi(e+\vec{w}), \Phi(e+\vec{w})$ aufgespannte Ebene, denn diese kann in derselben Weise beschrieben werden. Mit unserem Lemma 1.7.35 folgt, daß Φ eine affine Abbildung zwischen diesen Ebenen induzieren muß. Die Abbildung $\Psi : \vec{E} \to \vec{F}$ gegeben durch $\Phi(e + \vec{v}) = \Phi(e) + \Psi(\vec{v})$ ist nun linear, da nach dem Vorhergehenden ihre Restriktion auf jeden zweidimensionalen Teilraum von $\vec{E}$ linear ist. Das hinwiederum zeigt, daß Φ affin ist. □

Ergänzung 1.7.36. Geht man den Beweis von Lemma 1.7.35 nocheinmal durch, so erkennt man, daß er auch die folgende feinere Aussage zeigt: Sind K, L Körper und ist $\Phi : K^2 \hookrightarrow L^2$ eine Injektion mit $\Phi(0) = 0$, unter der das Bild jeder affinen Geraden wieder eine affine Gerade ist, so ist Φ ein Gruppenhomomorphismus und es gibt einen Körperisomorphismus $\psi : K \xrightarrow{\sim} L$ mit $\Phi(\lambda\vec{v}) = \psi(\lambda)\Phi(\vec{v})$ für alle $\lambda \in K$ und $\vec{v} \in K^2$. Salopp gesprochen ist also unsere Abbildung Φ "linear bis auf einen Körperisomorphismus".

Ergänzung 1.7.37. Geht man den Beweis 1.7.33 im Lichte von 1.7.36 nocheinmal durch, so erkennt man, daß er auch die folgende feinere Aussage zeigt: Haben zwei Strukturen $(E, \vec{E}, a)$ und $(E, \vec{E}', a')$ auf ein- und derselben Menge E als zweidimensionaler affiner Raum über Körpern k bzw. k' dieselben Geraden, so gilt $\vec{E} = \vec{E}'$ und es gibt genau einen Körperisomorphismus $\varphi : k \xrightarrow{\sim} k'$ mit $a(\lambda, \vec{v}) = a'(\varphi(\lambda), \vec{v})$ für alle $\lambda \in k$ und $\vec{v} \in \vec{E}$. Salopp gesprochen kennt also ein weißes Blatt Papier zusammen mit einem Lineal bereits den Körper $\mathbb{R}$ der reellen Zahlen! Gegeben eine Menge E von "Punkten" und eine Teilmenge $\mathcal{G} \subset \mathcal{P}(E)$ ihrer Potenzmenge, deren Elemente $G \in \mathcal{G}$ "Geraden" heißen, kann man auch eine Liste von geometrisch sinnvollen Forderungen angeben, die genau dann erfüllt sind, wenn unsere Menge E so mit der Struktur eines zweidimensionalen affinen Raums über einem Körper versehen werden kann, daß $\mathcal{G}$ aus allen zugehörigen affinen Geraden besteht. Die einfachsten dieser Forderungen sind, daß durch je zwei verschiedene Punkte genau eine Gerade gehen soll und daß sich je zwei Geraden in höchstens einem Punkt schneiden. In dieser Weise lassen sich dann unsere Körperaxiome I.3.3.1 auch geometrisch rechtfertigen.

1.7.38. Gegeben ein affiner Raum E über einem Körper k und darin Punkte $e_1, \ldots, e_n \in E$ und Skalare $\lambda_1, \ldots, \lambda_n \in k$ mit $\lambda_1 + \ldots + \lambda_n \neq 0$ definiert man den **Schwerpunkt** s **der** e_i **mit den Gewichten** λ_i durch die Bedingung

$$\lambda_1(e_1 - s) + \ldots + \lambda_n(e_n - s) = \vec{0}$$

Daß höchstens ein Punkt $s \in E$ diese Bedingung erfüllen kann, folgt daraus, daß für jedes weitere s', das unsere Bedingung erfüllt, gelten muß

$$(\lambda_1 + \ldots + \lambda_n)(s - s') = \vec{0}$$

Wie man auf einer Gerade der Papierebene mit zwei verschiedenen als Null und Eins ausgezeichneten Punkten zwei beliebige Punkte multipliziert, wenn man nur ein Lineal zur Verfügung hat, das aber “unendlich lang” ist in dem Sinne, daß man durch einen gegebenen Punkt die zu einer gegebenen Gerade parallele Gerade zeichnen kann.

Daß es überhaupt ein s gibt, das unsere Bedingung erfüllt, erkennt man, indem man einen beliebigen Punkt $p \in E$ wählt und $\lambda = \lambda_1 + \ldots + \lambda_n$ setzt und den Punkt

$$s = p + \frac{\lambda_1}{\lambda}(e_1 - p) + \ldots + \frac{\lambda_n}{\lambda}(e_n - p)$$

betrachtet. Für diesen Punkt $s \in E$ gilt ja

$$\lambda(s - p) = \lambda_1(e_1 - p) + \ldots + \lambda_n(e_n - p)$$

und daraus folgt dann leicht

$$\vec{0} = \lambda_1(e_1 - s) + \ldots + \lambda_n(e_n - s)$$

Übung 1.7.39. Ist E ein n-dimensionaler affiner Raum und $e_0, \ldots, e_n$ ein Erzeugendensystem von E, so gibt es für jeden Punkt $s \in E$ genau ein Tupel von Gewichten $(\lambda_0, \ldots, \lambda_n) \in k^{n+1}$ so daß gilt $\lambda_0 + \ldots + \lambda_n = 1$ und daß s der Schwerpunkt der e_i mit den Gewichten λ_i ist. Die λ_i heißen dann die **baryzentrischen Koordinaten von** s **in Bezug auf die** e_i, nach griechisch "$\beta\alpha\rho\upsilon\varsigma$" für "schwer".

Ergänzung 1.7.40. Eine Teilmenge eines affinen Raums heißt **affin unabhängig** genau dann, wenn sich keiner ihrer Punkte als gewichteter Schwerpunkt von endlich vielen anderen ihrer Punkte schreiben läßt.

Ergänzende Übung 1.7.41. Der von einer nichtleeren Menge von Punkten eines affinen Raums erzeugte affine Teilraum kann auch beschrieben werden als die Menge aller Schwerpunkte zu endlichen mit Gewichten versehenen Teilmengen unserer Menge.

Definition 1.7.42. Gegeben Punkte p, q in einem affinen Raum E über einem angeordneten Körper schreiben wir

$$[p, q] := \{p + t(q - p) \mid 0 \leq t \leq 1\}$$

und nennen diese Menge im Fall $p \neq q$ das die Punkte p und q verbindende **Geradensegment**.

Definition 1.7.43. Eine Teilmenge eines affinen Raums über einem angeordneten Körper heißt **konvex** genau dann, wenn sie mit je zwei Punkten auch das ganze diese verbindende Geradensegment enthält.

Definition 1.7.44. Sei E ein affiner Raum über einem angeordneten Körper. Offensichtlich ist der Schnitt einer beliebigen Familie konvexer Teilmengen von E wieder konvex. Gegeben eine Teilmenge $T \subset E$ bezeichnet man die kleinste

Zwei fette Punkte der Gewichte 3 und 1 und ihr Schwerpunkt s nebst seiner Bestimmung mithilfe eines beliebigen weiteren Punktes p.

Eine nicht konvexe Teilmenge der Ebene und eine endliche Teilmenge der Ebene, dargestellt durch fette Punkte, mit ihrer konvexen Hülle, dargestellt als schraffierter Bereich.

konvexe Teilmenge des fraglichen affinen Raums, die T umfaßt, auch als die **konvexe Hülle von** T. Natürlich existiert solch eine kleinste konvexe Teilmenge, wir können sie etwa konstruieren als den Schnitt aller konvexen Teilmengen, die T umfassen. Wir verwenden für die konvexe Hülle von T die Notation

$$\mathrm{konv}(T)$$

Beispiel 1.7.45. Gegeben zwei Punkte in einem affinen Raum über einem angeordneten Körper ist ihre konvexe Hülle genau das verbindende Geradensegment, in Formeln $[p, q] = \mathrm{konv}(p, q)$.

Ergänzende Übung 1.7.46. Gegeben ein affiner Raum E über einem angeordneten Körper und eine Teilmenge $T \subset E$ ist die konvexe Hülle von T genau die Menge aller Schwerpunkte zu endlichen mit positiven Gewichten versehenen Teilmengen von T.

1.8 Lineare Abbildungen $K^n \to K^m$ und Matrizen

1.8.1. Wir bezeichnen in diesem Abschnitt unseren Körper mit K statt wie bisher mit k, weil das kleine k eine neue Aufgabe als Index übernehmen soll.

Satz 1.8.2 (Lineare Abbildungen $K^n \to K^m$ und Matrizen). *Gegeben ein Körper K und natürliche Zahlen $m, n \in \mathbb{N}$ erhalten wir eine Bijektion zwischen dem Raum der Homomorphismen $K^n \to K^m$ und der Menge der K-wertigen Matrizen mit m Zeilen und n Spalten*

$$\begin{array}{rccc} M: & \mathrm{Hom}_K(K^n, K^m) & \xrightarrow{\sim} & \mathrm{M}(m \times n; K) \\ & f & \mapsto & [f] \end{array}$$

indem wir jeder linearen Abbildung f ihre **darstellende Matrix** $M(f) := [f]$ *zuordnen, die dadurch erklärt wird, daß in ihren Spalten die Bilder unter f der Vektoren der Standardbasis des K^n stehen, in Formeln*

$$[f] := (f(\mathrm{e}_1)|f(\mathrm{e}_2)|\ldots|f(\mathrm{e}_n))$$

Beweis. Das folgt unmittelbar aus unserer Erkenntnis 1.5.13, daß eine lineare Abbildung festgelegt und festlegbar ist durch ihre Werte auf den Vektoren einer Basis. □

Übung 1.8.3. Man zeige, daß die Abbildung M aus 1.8.2 sogar ein Vektorraumisomorphismus ist für die Vektorraumstruktur 1.5.17 auf dem Raum der Homomorphismen und die Vektorraumstruktur 1.3.23 auf der Menge der Matrizen.

Beispiel 1.8.4. Die Matrix der Identität auf K^n ist die **Einheitsmatrix**

$$I = I_n := [\mathrm{id}] = \begin{pmatrix} 1 & & 0 \\ & 1 & \\ & & \ddots \\ 0 & & 1 \end{pmatrix}$$

mit Einträgen $I_{i,j} = \delta_{i,j}$ in der unter der Bezeichnung **Kroneckerdelta** bekannten und allgemein gebräuchlichen Konvention

$$\delta_{i,j} = \begin{cases} 1 & i = j; \\ 0 & \text{sonst.} \end{cases}$$

Ist allgemeiner $n \geq m$, so ist die Matrix des "Weglassens der überzähligen Koordinaten" $f : (x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_m)$ gerade

$$[f] = \begin{pmatrix} 1 & & 0 & & 0 \ldots 0 \\ & \ddots & & & \\ & & \ddots & & \\ 0 & & & 1 & 0 \ldots 0 \end{pmatrix}$$

Die Matrix des "Vertauschens der Koordinaten" $g : K^2 \to K^2$ schließlich ist

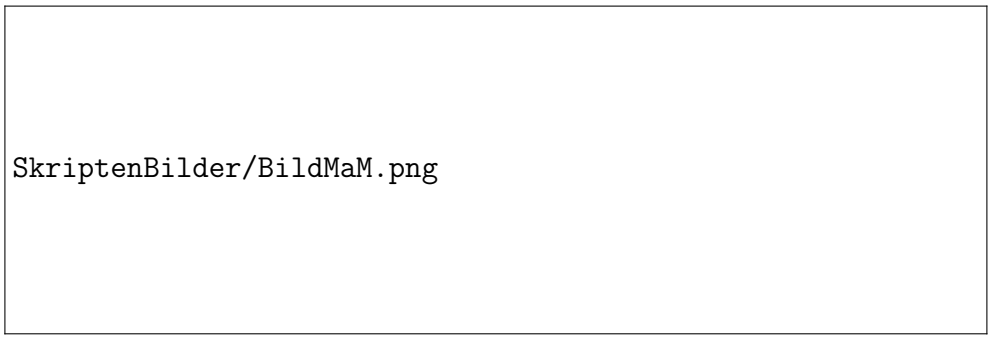
$$[g] = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Definition 1.8.5. Gegeben natürliche Zahlen $m, n, l \in \mathbb{N}$ und ein Körper K und Matrizen $A \in \mathrm{M}(n \times m; K)$ und $B \in \times \mathrm{M}(m \times l; K)$ definieren wir ihr **Produkt** $A \circ B = AB \in \mathrm{M}(n \times l; K)$ durch die Formel

$$(AB)_{ik} = \sum_{j=1}^{m} A_{ij} B_{jk}$$

die den Eintrag der Produktmatrix AB in der i-ten Zeile und k-ten Spalte durch die Einträge der Matrizen A und B ausdrückt. In Worten gilt es, jeweils den j-ten Eintrag der i-ten Zeile von A mit dem j-ten Eintrag der k-ten Spalte von B zu multiplizieren, und die Summe dieser m Produkte ist dann der Eintrag der Produktmatrix AB in der i-ten Zeile und k-ten Spalte. Manchmal schreiben wir die Produktmatrix auch ausführlicher $AB = A \circ B$. Die **Matrixmultiplikation** liefert eine Abbildung

$$\begin{array}{ccc} \mathrm{M}(n \times m; K) \times \mathrm{M}(m \times l; K) & \to & \mathrm{M}(n \times l; K) \\ (A \quad , \quad B) & \mapsto & AB \end{array}$$



Produkt zweier Matrizen. Der gestrichelt eingekringelte Eintrag 4 in der zweiten Zeile und dritten Spalte auf der rechten Seite etwa ergibt sich aus der gestrichelt eingekringelten zweiten Zeile des ersten Faktors und der gestrichelt eingekringelten dritten Spalte des zweiten Faktors vermittels der Rechnung $4 = 2 \cdot 2 + 0 \cdot 6$.

Den Ursprung dieser auf den ersten Blick vielleicht absonderlich anmutenden Definition des Produkts zweier Matrizen und unserer leicht mit dem Verknüpfen von Abbildungen zu verwechselnden alternativen Notation $AB = A \circ B$ erklärt der folgende Satz.

Satz 1.8.6 (Verknüpfen von Abbildungen und Matrixprodukt). *Gegeben lineare Abbildungen $g : K^l \to K^m$ und $f : K^m \to K^n$ ist die Matrix ihrer Verknüpfung das Produkt der zugehörigen Matrizen, in Formeln*

$$[f \circ g] = [f] \circ [g]$$

Beweis. Sei (a_{ij}) die Matrix $[f]$ und (b_{jk}) die Matrix $[g]$. Wir notieren die Standardbasen von K^n, K^m und K^l als $\vec{u}_i, \vec{v}_j$ und $\vec{w}_k$ in der Hoffnung, daß die folgende Rechnung dadurch transparenter wird, daß wir nicht für die Standardbasis in allen drei Räumen die sonst eigentlich übliche Notation $\vec{e}_r$ verwenden. In unserer Notation haben wir also

$$\begin{array}{rcccl} g(\vec{w}_k) & = & (b_{*k}) & = & b_{1k}\vec{v}_1 + \ldots + b_{mk}\vec{v}_m \\ f(\vec{v}_j) & = & (a_{*j}) & = & a_{1j}\vec{u}_1 + \ldots + a_{nj}\vec{u}_n \end{array}$$

und folgern

$$\begin{array}{rcl} (f \circ g)(\vec{w}_k) & = & f(b_{1k}\vec{v}_1 + \ldots + b_{mk}\vec{v}_m) \\ & = & b_{1k}f(\vec{v}_1) + \ldots + b_{mk}f(\vec{v}_m) \\ & = & \sum_{j=1}^m b_{jk} f(\vec{v}_j) \\ & = & \sum_{j=1}^m b_{jk} \sum_{i=1}^n a_{ij}\vec{u}_i \\ & = & \sum_{i=1}^n \left(\sum_{j=1}^m a_{ij}b_{jk} \right) \vec{u}_i \end{array}$$

Andererseits sind ja die Einträge (c_{ik}) der Matrix $[f \circ g]$ gerade definiert durch die Identität $(f \circ g)(\vec{w}_k) = c_{1k}\vec{u}_1 + \ldots + c_{nk}\vec{u}_n$, und durch einen Koeffizientenvergleich folgt für die Einträge c_{ik} von $[f \circ g]$ wie gewünscht $c_{ik} = \sum_{j=1}^m a_{ij}b_{jk}$. □

Proposition 1.8.7. *Für die Matrixmultiplikation gelten die folgenden Rechenregeln:*

$$\begin{array}{rcl} (A + A')B & = & AB + A'B \\ A(B + B') & = & AB + AB' \\ IB & = & B \\ AI & = & A \\ (AB)C & = & A(BC) \end{array}$$

für beliebige $k, l, m, n \in \mathbb{N}$ und $A, A' \in \mathrm{M}(n \times m; K)$, $B, B' \in \mathrm{M}(m \times l; K)$, $C \in \mathrm{M}(l \times k; K)$ und $I = I_m$ die $(m \times m)$-Einheitsmatrix.

Erster Beweis. Stures Rechnen, ich führe nur zwei Teile beispielhaft aus. Wir haben $(AI)_{ij} = \sum A_{ik} I_{kj} = \sum A_{ik}\delta_{kj} = A_{ij}$ und das zeigt $AI = A$. Für die nächste Rechnung verwende ich einmal andere Notationen und nehme $\kappa, \lambda, \mu, \nu$ als Laufindizes. Dann haben wir

$$\begin{aligned}
((AB)C)_{\nu\kappa} &= \textstyle\sum_{\lambda=1}^{l} (AB)_{\nu\lambda} C_{\lambda\kappa} \\
&= \textstyle\sum_{\lambda=1}^{l} \left(\sum_{\mu=1}^{m} A_{\nu\mu} B_{\mu\lambda} \right) C_{\lambda\kappa} \\
&= \textstyle\sum_{\lambda,\mu=1}^{l,m} A_{\nu\mu} B_{\mu\lambda} C_{\lambda\kappa} \\
(A(BC))_{\nu\kappa} &= \textstyle\sum_{\mu=1}^{m} A_{\nu\mu} (BC)_{\mu\kappa} \\
&= \textstyle\sum_{\mu=1}^{m} A_{\nu\mu} \left(\sum_{\lambda=1}^{l} B_{\mu\lambda} C_{\lambda\kappa} \right) \\
&= \textstyle\sum_{\mu,\lambda=1}^{m,l} A_{\nu\mu} B_{\mu\lambda} C_{\lambda\kappa}
\end{aligned}$$

und das zeigt $(AB)C = A(BC)$. □

Zweiter Beweis. Wir können unsere Rechenregeln für Matrizen auch mit 1.8.2 und 1.8.6 auf die entsprechenden Regeln für lineare Abbildungen zurückführen. Um zum Beispiel $(AB)C = A(BC)$ zu zeigen, betrachten wir die linearen Abbildungen a, b, c mit den entsprechenden Matrizen im Sinne von 1.8.2, finden mit 1.8.6 sofort

$$\begin{aligned}
(AB)C &= ([a] \circ [b]) \circ [c] \\
&= [a \circ b] \circ [c] \\
&= [(a \circ b) \circ c] \\
A(BC) &= [a] \circ ([b] \circ [c]) \\
&= [a] \circ [b \circ c] \\
&= [a \circ (b \circ c)]
\end{aligned}$$

und die Behauptung ergibt sich aus der für die Verknüpfung von Abbildungen offensichtlichen Identität $(a \circ b) \circ c = a \circ (b \circ c)$. □

1.8.8. In der Terminologie aus 1.5.26 ist unsere Matrixmultiplikation eine bilineare Abbildung, wie man unschwer einsieht.

1.8.9. Mit dem Formalismus der Matrixmultiplikation können wir auch die Umkehrung unserer Bijektion $\mathrm{Hom}_K(K^m, K^n) \xrightarrow{\sim} \mathrm{M}(n \times m; K)$, $f \mapsto [f]$ aus 1.8.2, bei der jeder linearen Abbildung ihre darstellende Matrix zugeordnet wird, elegant beschreiben, indem wir die Elemente von K^m bzw. K^n als Spaltenvektoren auffassen und einer Matrix $A \in \mathrm{M}(n \times m; K)$ die durch Matrixmultiplikation gegebene Abbildung $(A\circ) : \mathrm{M}(m \times 1; K) \to \mathrm{M}(n \times 1; K)$ alias

$$(A\circ) : K^m \to K^n$$

zuordnen. Das folgt unmittelbar aus den Definitionen. Statt $A \circ x$ schreibt man dann einfacher auch schlicht Ax. Die Umkehrabbildung zu $f \mapsto [f]$ kann mit diesen Konventionen also in der Form $A \mapsto (x \mapsto Ax)$ für $x \in K^m$ dargestellt werden, oder noch knapper in der Form $A \mapsto (A\circ)$. Auf die Dauer geht einem diese Identifikation von linearen Abbildungen $K^m \to K^n$ und Matrizen eh so in Fleisch und Blut über, daß man schlicht unterschiedslos A schreibt und damit beides gleichzeitig meint.

1.8.10. Gegeben ein Körper K liefert für jeden K-Vektorraum V das Auswerten auf dem Element $1 \in K$ eine Bijektion $\mathrm{Hom}(K,V) \xrightarrow{\sim} V$. Deren Umkehrabbildung kann explizit beschrieben werden als die Abbildung

$$V \xrightarrow{\sim} \mathrm{Hom}(K,V)$$

gegeben durch $\vec{v} \mapsto (\cdot\vec{v})$ mit $(\cdot\vec{v}) : \lambda \mapsto \lambda\vec{v}$. Im Spezialfall $V = K^m$ ist für $\vec{v} \in K^m$ die darstellende Matrix $[\cdot\vec{v}]$ von $(\cdot\vec{v}) : K \to K^m$ offensichtlich gerade $\vec{v}$ selber, aufgefaßt als Spaltenmatrix. Wir notieren diese Spaltenmatrix abkürzend

$$[\vec{v}]$$

oder später auch einfach nur noch $\vec{v}$. Ist nun $f : V \to W$ linear, so gilt auch ganz allgemein sicher $f \circ (\cdot\vec{v}) = (\cdot f(\vec{v}))$, denn diese beiden linearen Abbildungen $K \to W$ nehmen auf dem Erzeuger $1 \in K$ denselben Wert $f(\vec{v})$ an. Im Spezialfall $W = K^n$ folgern wir für das Produkt der darstellenden Matrizen aus der vorhergehenden Bemerkung 1.8.9 nocheinmal die Identität

$$[f] \circ [\vec{v}] = [f(\vec{v})]$$

von Spaltenvektoren, diesmal aber als Konsequenz unseres Satzes 1.8.6 über die Matrix einer Verknüpfung.

Übung 1.8.11. Sei $f : \mathbb{R}^2 \to \mathbb{R}^2$ die Spiegelung $(x,y) \mapsto (x,-y)$. Man zeige, daß die linearen Abbildungen $g : \mathbb{R}^2 \to \mathbb{R}^2$ mit der Eigenschaft $fg = gf$ einen Untervektorraum des Homomorphismenraums $\mathrm{Hom}_{\mathbb{R}}(\mathbb{R}^2,\mathbb{R}^2)$ bilden und gebe eine Basis dieses Untervektorraums des Homomorphismenraums an.

Übung 1.8.12. Gegeben eine Matrix $A \in \mathrm{M}(n\times m;K)$ definiert man die **transponierte Matrix** $A^\top \in \mathrm{M}(m \times n;K)$ durch die Vorschrift $(A^\top)_{ij} = A_{ji}$. Anschaulich gesprochen entsteht also $A^\top$ aus A durch "Spiegeln an der Hauptdiagonalen". Zum Beispiel ist die Transponierte eines Spaltenvektors alias einer $(n \times 1)$-Matrix ein **Zeilenvektor** alias eine $(1 \times n)$-Matrix. Natürlich gilt $(A^\top)^\top = A$. Man zeige

$$(AB)^\top = B^\top A^\top$$

Die transponierte Matrix erhält man durch eine “Spiegelung an der Hauptdiagonalen”.

Ergänzung 1.8.13. Viele Autoren verwenden für die transponierte Matrix auch die alternative Notation ${}^tA$.

1.8.14. An dieser Stelle will ich kurz auf die Frage eingehen, "ob denn Elemente eines K^n nun eigentlich Zeilenvektoren oder Spaltenvektoren sein sollen". A priori sind Elemente eines K^n halt n-Tupel, und wie wir sie schreiben ist egal. Wenn wir jedoch eine Matrix davormultiplizieren wollen, ist es wichtig, unsere n-Tupel als Spaltenvektoren alias Spaltenmatrizen aufzufassen. Da das oft vorkommt, plädiere ich dafür, sich n-Tupel grundsätzlich als Spalten zu denken. Allerdings ist es in einen durchlaufenden Text ungeschickt, Spaltenvektoren auch als solche zu schreiben. Da fügen sich Zeilenvektoren einfach viel besser ein. Wenn ich dennoch auf Spaltenvektoren bestehen will, schreibe ich sie im Text als "zu transponierende Zeilenvektoren", als da heißt, in der Form $(x_1, \ldots, x_n)^\top$. Oft schreibe ich aber auch einfach $(x_1, \ldots, x_n)$ und der Leser muß aus dem Kontext erschließen, was genau gemeint ist, wenn es denn darauf überhaupt ankommen sollte.

Ergänzung 1.8.15. Gegeben Vektorräume $V_1, \ldots, V_m$ und $W_1, \ldots, W_n$ über einem Körper k liefern 1.5.18 und 1.5.19 zusammen eine natürliche Identifikation

$$\begin{array}{ccc} \operatorname{Hom}(V_1 \oplus \ldots \oplus V_m, W_1 \oplus \ldots \oplus W_n) & \xrightarrow{\sim} & \prod_{i,j} \operatorname{Hom}_R(V_j, W_i) \\ f & \mapsto & (\mathrm{pr}_i \circ f \circ \mathrm{in}_j)_{ij} \end{array}$$

Wir werden die Elemente einer endlichen direkten Summe oft als Spaltenvetoren auffassen und die Homomorphismen zwischen direkten Summen als Matrizen von Homomorphismen zwischen den Summanden. So fassen wir ein Element (f_{ij}) des rechten Produkts oben auf als eine Matrix von Homomorphismen, mit $f_{11}, f_{21}, \ldots, f_{n1}$ als erster Spalte, $f_{12}, f_{22}, \ldots, f_{n2}$ als zweiter Spalte und so weiter. Diese Darstellung als Matrix erlaubt es dann, die Komposition solcher Homomorphismen mit dem Formalismus der Matrixmultiplikation zu berechnen: Entspricht genauer einer weiteren linearen Abbildung $g : U_1 \oplus \ldots \oplus U_l \to V_1 \oplus \ldots \oplus V_m$ die Matrix der $g_{jk} = \mathrm{pr}_j \circ g \circ \mathrm{in}_k : U_k \to V_j$, so entspricht der Verknüpfung $f \circ g$ die Matrix mit Einträgen

$$\left(\sum_j f_{ij} \circ g_{jk} \right) : U_k \to W_i$$

Sind speziell alle unsere Vektorräume irgendwelche k^a, so erhalten wir insbesondere, daß das Produkt zweier multiplizierbarer Matrizen auch berechnet werden kann, indem man sie "in verträglicher Weise" als Blockmatrizen auffaßt und dann diese Blockmatrizen nach den Regeln der Matrixmultiplikation "multipliziert, als ob die Blöcke Zahlen wären".

Ergänzende Übung 1.8.16. Eine quadratische Block-obere Dreiecksmatrix ist invertierbar genau dann, wenn alle Blöcke auf der Diagonalen invertierbar sind.

1.9 Einige Eigenschaften von Matrizen

1.9.1. Eine Matrix A heißt **invertierbar** genau dann, wenn es weitere Matrizen B, C gibt mit $BA = I$ und $AC = I$. Das ist nach 1.8.6 gleichbedeutend dazu, daß die durch A gegebene lineare Abbildung $A : K^m \to K^n$ invertierbar alias ein Isomorphismus ist. Das ist nach 1.5.10 nur möglich für $n = m$, es können also nur quadratische Matrizen invertierbar sein. Für eine quadratische Matrix A sind des weiteren gleichbedeutend:

1. Es gibt eine quadratische Matrix B mit $BA = I$;
2. Es gibt eine quadratische Matrix C mit $AC = I$;
3. Die quadratische Matrix A ist invertierbar.

In der Tat folgt aus (1), daß die durch A gegebene lineare Abbildung injektiv ist, also ist sie bijektiv nach Dimensionsvergleich. Ebenso folgt aus (2), daß die durch A gegebene lineare Abbildung surjektiv ist, also ist sie bijektiv nach Dimensionsvergleich. Ist A invertierbar und $a : K^n \xrightarrow{\sim} K^n$ der zugehörige Vektorraumisomorphismus, so ist die Matrix $[a^{-1}]$ der Umkehrabbildung die einzige quadratische Matrix B mit $AB = I$ und auch die einzige quadratische Matrix B mit $BA = I$. Die invertierbaren $(n \times n)$-Matrizen sind insbesondere genau die invertierbaren Elemente im Sinne von I.3.2.2 des Monoids der $(n \times n)$-Matrizen mit der Matrixmultiplikation als Verknüpfung. Im Einklang mit unseren allgemeinen Konventionen für multiplikativ notierte Monoide notieren wir diese Matrix A^{-1} und nennen sie die **inverse Matrix zu** A. Die invertierbaren $(n \times n)$-Matrizen mit Einträgen in einem Körper K bilden mit der Matrixmultiplikation eine Gruppe, die **allgemeine lineare Gruppe der** $(n \times n)$**-Matrizen**, die man notiert als

$$\mathrm{M}(n \times n; K)^\times = \mathrm{GL}(n; K)$$

in Anlehnung an die englische Bezeichnung **general linear group**.

Ergänzende Übung 1.9.2. Die Automorphismengruppe eines zweidimensionalen Vektorraums über einem zweielementigen Körper ist isomorph zur Gruppe der Permutationen von drei Elementen, in Formeln $\mathrm{GL}(2; \mathbb{F}_2) \cong \mathcal{S}_3$.

1.9.3. Unser lineares Gleichungssystem

$$\begin{array}{rcl} a_{11}x_1 + a_{12}x_2 + & \ldots & + a_{1m}x_m = b_1 \\ a_{21}x_1 + a_{22}x_2 + & \ldots & + a_{2m}x_m = b_2 \\ \vdots & & \vdots \\ a_{n1}x_1 + a_{n2}x_2 + & \ldots & + a_{nm}x_m = b_n \end{array}$$

können wir in unseren neuen Notationen zur Gleichung von Spaltenvektoren

$$Ax = b$$

abkürzen, wobei links das Produkt der Koeffizientenmatrix mit dem Spaltenvektor x gemeint ist. Gesucht ist das Urbild von $b \in K^n$ unter der linearen Abbildung $(A\circ) : K^m \to K^n$. Die Lösung des homogenisierten Systems ist genau der Kern dieser linearen Abbildung, und die Erkenntnis 1.1.7, nach der die allgemeine Lösung eines inhomogenen Systems die Summe einer speziellen Lösung des inhomogenen Systems mit einer allgemeinen Lösung des homogenisierten Systems ist, erweist sich als ein Spezialfall von 1.6.6. Die Operationen des Gauß-Algorithmus können wir in diesem Rahmen wie folgt interpretieren: Bezeichnet

$$E_{ij}$$

die **Basismatrix** mit dem Eintrag Eins in der i-ten Zeile und j-ten Spalte und Nullen sonst, so kann für $i \neq j$ das Gleichungssystem, das durch Addition des λ-fachen der j-ten Zeile zur i-ten Zeile entsteht, in Matrixschreibweise dargestellt werden als

$$(I + \lambda E_{ij})Ax = (I + \lambda E_{ij})b$$

Wegen $(I - \lambda E_{ij})(I + \lambda E_{ij}) = I$ hat es offensichtlich dieselbe Lösungsmenge wie das ursprüngliche System. Bezeichnet weiter P_{ij} für $i \neq j$ die Matrix zu der linearen Abbildung $K^m \xrightarrow{\sim} K^m$, die die i-te Koordinate mit der j-ten Koordinate vertauscht und sonst alles so läßt wie es ist, so kann das Gleichungssystem, das durch Vertauschen der i-ten Zeile mit der j-ten Zeile entsteht, in Matrixschreibweise dargestellt werden als

$$P_{ij}Ax = P_{ij}b$$

Wegen $P_{ij}P_{ij} = I$ hat es offensichtlich dieselbe Lösungsmenge wie das ursprüngliche System.

1.9.4. Unter einer **Elementarmatrix** verstehen wir eine quadratische Matrix, die sich in höchstens einem Eintrag von der Einheitsmatrix unterscheidet. Alle Elementarmatrizen mit Einträgen in einem Körper sind invertierbar mit Ausnahme der Matrizen, die entstehen, wenn man in der Einheitsmatrix eine Eins durch eine Null ersetzt.

Bemerkung 1.9.5. Es herrscht in der Literatur keine Einigkeit in der Frage, was genau unter einer Elementarmatrix zu verstehen sein soll. Manche Quellen bezeichnen zusätzlich zu unseren Elementarmatrizen auch noch die Permutationsmatrizen P_{ij} als Elementarmatrizen, andere Quellen hinwiederum lassen nur solche Matrizen zu, die sich von der Einheitsmatrix in höchstens einem Eintrag außerhalb der Diagonale unterscheiden. Ich schlage vor, diese letzteren Matrizen **spezielle Elementarmatrizen** zu nennen, da sie genau die Elementarmatrizen sind, die zur speziellen linearen Gruppe 3.4.5 gehören.

Satz 1.9.6. *Jede quadratische Matrix mit Einträgen in einem Körper läßt sich als ein Produkt von Elementarmatrizen darstellen.*

Beweis. Zunächst einmal gilt das für die Permutationsmatrizen P_{ij}, die wir schreiben können als

$$P_{ij} = \mathrm{diag}(1, \ldots, 1, -1, 1, \ldots, 1)(I + E_{ij})(I - E_{ji})(I + E_{ij})$$

Hier soll die (-1) an der j-ten Stelle stehen und $\mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ meint die **Diagonalmatrix** mit Einträgen $a_{ij} = 0$ für $i \neq j$ und $a_{ii} = \lambda_i$. Nun beachten wir, daß das Inverse jeder invertierbaren Elementarmatrix wieder eine Elementarmatrix ist. Gegeben eine beliebige Matrix A finden wir nun nach dem Gauß-Algorithmus invertierbare Elementarmatrizen $S_1, \ldots, S_n$ derart, daß $S_n \ldots S_1 A$ Zeilenstufenform hat. Nun überzeugt man sich leicht, daß wir durch Daranmultiplizieren invertierbarer Elementarmatrizen von rechts alle Spaltenoperationen erhalten können, als da heißt, das Addieren des Vielfachen einer Spalte zu einer anderen, das Vertauschen zweier Spalten, sowie das Multiplizieren einer Spalte mit einem von Null verschiedenen Skalar. Wir können also weiter invertierbare Elementarmatrizen $T_1, \ldots, T_m$ finden derart, daß $S_n \ldots S_1 A T_1 \ldots T_m$ die Gestalt $\mathrm{diag}(1, \ldots, 1, 0, \ldots, 0)$ hat. Diese Matrix schreiben wir leicht als Produkt von nun nicht mehr invertierbaren diagonalen Elementarmatrizen $S_n \ldots S_1 A T_1 \ldots T_m = D_1 \ldots D_r$ und folgern

$$A = S_1^{-1} \ldots S_n^{-1} D_1 \ldots D_r T_m^{-1} \ldots T_1^{-1}$$ □

1.9.7. Eine Matrix, die nur auf der Diagonalen von Null verschiedene Einträge hat, und zwar erst einige Einsen und danach nur noch Nullen, nennen wir auch eine Matrix in **Smith-Normalform**.

Satz 1.9.8. *Für jede Matrix $A \in \mathrm{M}(n \times m; K)$ mit Einträgen in einem Körper K gibt es invertierbare Matrizen P, Q derart, daß PAQ eine Matrix in Smith-Normalform ist.*

Beweis. Wie beim Beweis von 1.9.6 finden wir nach dem Gauß-Algorithmus erst invertierbare Elementarmatrizen $S_1, \ldots, S_n$ derart, daß $S_n \ldots S_1 A$ Zeilenstufenform hat, und dann invertierbare Elementarmatrizen $T_1, \ldots, T_m$ derart, daß $S_n \ldots S_1 A T_1 \ldots T_m$ Smith-Normalform hat. □

Definition 1.9.9. Gegeben eine Matrix $A \in \mathrm{M}(n \times m; K)$ heißt die Dimension des von ihren Spaltenvektoren aufgespannten Untervektorraums von K^n der **Spaltenrang** unserer Matrix. Analog heißt die Dimension des von ihren Zeilenvektoren aufgespannten Untervektorraums von K^m der **Zeilenrang** unserer Matrix.

Eine Matrix in Smith-Normalform

Satz 1.9.10. *Für jede Matrix stimmen Zeilenrang und Spaltenrang überein.*

1.9.11. Diese gemeinsame Zahl heißt dann der **Rang** unserer Matrix und wird $\mathrm{rk}\, A$ notiert nach der englischen Bezeichnung **rank**. Ist der Rang einer Matrix so groß wie für Matrizen derselben Gestalt möglich, sind also entweder die Spalten oder die Zeilen linear unabhängig, so sagt man, unsere Matrix habe **vollen Rang**.

Beweis. Der Spaltenrang einer Matrix $A \in \mathrm{M}(n \times m; K)$ kann interpretiert werden als die Dimension des Bildes von

$$(A\circ) : K^m \to K^n$$

Diese Interpretation zeigt sofort, daß PAQ denselben Spaltenrang hat wie A für beliebige invertierbare Matrizen P, Q. Durch Transponieren erkennen wir, daß PAQ auch denselben Zeilenrang hat wie A für beliebige invertierbare Matrizen P, Q. Nun finden wir jedoch nach 1.9.8 invertierbare Matrizen P, Q mit PAQ in Smith-Normalform. Dann stimmen natürlich Zeilenrang und Spaltenrang von PAQ überein, und dasselbe folgt für unsere ursprüngliche Matrix A. □

Definition 1.9.12. Ganz allgemein nennt man die Dimension des Bildes einer linearen Abbildung auch den **Rang** unserer linearen Abbildung. Dieser Rang kann unendlich sein, es gibt aber auch zwischen unendlichdimensionalen Vektorräumen durchaus von Null verschiedene Abbildungen endlichen Ranges.

Übung 1.9.13. Gegeben lineare Abbildungen $f : U \to V$ und $g : V \to W$ zeige man, daß der Rang ihrer Verknüpfung $g \circ f$ sowohl beschränkt ist durch den Rang von f als auch durch den Rang von g.

Übung 1.9.14. Man gebe eine ganzzahlige (3×3)-Matrix vom Rang zwei ohne Eintrag Null an, bei der je zwei Spalten linear unabhängig sind.

1.9.15 (**Invertieren von Matrizen**). Um die Inverse einer $(n \times n)$-Matrix A zu berechnen, kann man wie folgt vorgehen: Man schreibt die Einheitsmatrix I daneben und wendet dann auf die $(n \times 2n)$-Matrix $(A|I)$ Zeilenoperationen an, einschließlich des Multiplizierens einer Zeile mit einem von Null verschiedenene Skalar, bis man A erst in Zeilenstufenform und dann sogar zur Einheitsmatrix gemacht hat. Dann steht in der rechten Hälfte unserer $(n \times 2n)$-Matrix die Inverse zu A. In der Tat, sind unsere Zeilenumformungen etwa gegeben durch das Davormultiplizieren der Matrizen $S_1, S_2, \ldots, S_t$, so steht nach diesen Umformungen da

$$(S_t \ldots S_2 S_1 A | S_t \ldots S_2 S_1 I)$$

und wenn dann gilt $S_t \ldots S_2 S_1 A = I$, so folgt $S_t \ldots S_2 S_1 I = S_t \ldots S_2 S_1 = A^{-1}$. Dasselbe Verfahren funktioniert auch, wenn wir statt mit Zeilen- mit Spaltenumformungen arbeiten. Es ist nur nicht erlaubt, diese zu mischen, denn aus $S_t \ldots S_1 A T_1 \ldots T_r = I$ folgt keineswegs $S_t \ldots S_1 T_1 \ldots T_r = A^{-1}$.

1.10 Abstrakte lineare Abbildungen und Matrizen

1.10.1. Die im folgenden verwendeten Notationen ${}_{\mathcal{B}}[v]$ und ${}_{\mathcal{A}}[f]_{\mathcal{B}}$ habe ich Urs Hartl abgeschaut. Ähnlich wie die geschickt gewählten Steckverbindungen, die man bei Computerzubehör gewohnt ist, sorgen sie auch hier dafür, daß man fast nichts mehr falsch machen kann.

Satz 1.10.2 (Abstrakte lineare Abbildungen und Matrizen). *Seien gegeben ein Körper k sowie k-Vektorräume V, W mit angeordneten Basen $\mathcal{A} = (\vec{v}_1, \ldots, \vec{v}_m)$ und $\mathcal{B} = (\vec{w}_1, \ldots, \vec{w}_n)$. Ordnen wir jeder linearen Abbildung $f : V \to W$ die* **darstellende Matrix** ${}_{\mathcal{B}}[f]_{\mathcal{A}}$ *zu mit Einträgen a_{ij} gegeben durch die Identitäten $f(\vec{v}_j) = a_{1j}\vec{w}_1 + \ldots + a_{nj}\vec{w}_n$, so erhalten wir eine Bijektion, ja sogar einen Vektorraumisomorphismus*

$$\begin{array}{ccc} \mathrm{Hom}_k(V,W) & \xrightarrow{\sim} & \mathrm{M}(n \times m; k) \\ f & \mapsto & {}_{\mathcal{B}}[f]_{\mathcal{A}} \end{array}$$

1.10.3. Wir nennen ${}_{\mathcal{B}}[f]_{\mathcal{A}}$ die **darstellende Matrix der Abbildung f in Bezug auf die Basen $\mathcal{A}$ und $\mathcal{B}$**. In Worten ausgedrückt stehen in ihren Spalten die Koordinaten der Bilder der Vektoren der Basis $\mathcal{A}$ des Ausgangsraums in Bezug auf die Basis $\mathcal{B}$ des Zielraums. Beliebt ist statt ${}_{\mathcal{B}}[f]_{\mathcal{A}}$ auch die alternative Notation $M^{\mathcal{A}}_{\mathcal{B}}(f)$ oder noch ausführlicher $\mathrm{Mat}^{\mathcal{A}}_{\mathcal{B}}(f)$. Die Matrix einer linearen Abbildung $f : K^m \to K^n$ in Bezug auf die jeweiligen Standardbasen $\mathcal{S}(m)$, $\mathcal{S}(n)$ nach 1.4.12 ist genau unsere darstellende Matrix $[f]$ aus 1.8.2, in Formeln gilt also

$$[f] = {}_{\mathcal{S}(n)}[f]_{\mathcal{S}(m)}$$

Beweis. Wir könnten hier eine Variation unseres Beweises von 1.8.6 nochmal ausschreiben, aber stattdessen erinnern wir einfacher unsere Isomorphismen $\Phi_{\mathcal{A}} : k^m \xrightarrow{\sim} V$ und $\Phi_{\mathcal{B}} : k^n \xrightarrow{\sim} W$ aus 1.4.14 und beachten die Identität

$${}_{\mathcal{B}}[f]_{\mathcal{A}} = [\Phi_{\mathcal{B}}^{-1} f \Phi_{\mathcal{A}}]$$

Damit können wir unsere Abbildung dann schreiben als die Komposition von Bijektionen

$$\begin{array}{ccccc} \mathrm{Hom}_k(V,W) & \xrightarrow{\sim} & \mathrm{Hom}_k(k^m, k^n) & \overset{M}{\xrightarrow{\sim}} & \mathrm{M}(n \times m; k) \\ f & \mapsto & \Phi_{\mathcal{B}}^{-1} f \Phi_{\mathcal{A}} & & \end{array}$$

mit unserer Abbildung $M : g \mapsto [g]$ aus 1.8.2, die eben jeder Abbildung $g : k^m \to k^n$ ihre darstellende Matrix zuordnet. □

Die Matrix der anschaulichen Spiegelung $s : \mathbb{R}^2 \to \mathbb{R}^2$ hat die Gestalt

$$[s] = \begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix}$$

mit den Bildern der Vektoren der Standardbasis in den Spalten. Zum Beispiel hat $s(\vec{e}_1)$ die x-Koordinate $\cos 2\alpha$ und die y-Koordinate $\sin 2\alpha$ und das erklärt bereits die erste Spalte unserer Matrix. Bei $s(\vec{e}_2)$ scheint mir einsichtig, daß die x-Koordinate von $s(\vec{e}_2)$ die y-Koordinate von $s(\vec{e}_1)$ ist und die y-Koordinate von $s(\vec{e}_2)$ das Negative der x-Koordinate von $s(\vec{e}_1)$. Das erklärt dann auch die zweite Spalte unserer Matrix.

Satz 1.10.4 (Darstellende Matrix einer Verknüpfung). *Gegeben ein Körper k und endlichdimensionale k-Vektorräume U, V, W mit angeordneten Basen $\mathcal{A}, \mathcal{B}, \mathcal{C}$ und lineare Abbildungen $f : U \to V$ und $g : V \to W$ ist die darstellende Matrix der Verknüpfung das Produkt der darstellenden Matrizen, in Formeln*

$$_{\mathcal{C}}[g \circ f]_{\mathcal{A}} = {}_{\mathcal{C}}[g]_{\mathcal{B}} \circ {}_{\mathcal{B}}[f]_{\mathcal{A}}$$

Erster Beweis. Wir können die Behauptung nach Erinnern aller Notationen umschreiben zu $[\Phi_{\mathcal{C}}^{-1} g f \Phi_{\mathcal{A}}] = [\Phi_{\mathcal{C}}^{-1} g \Phi_{\mathcal{B}}] \circ [\Phi_{\mathcal{B}}^{-1} f \Phi_{\mathcal{A}}]$, und das folgt offensichtlich aus 1.8.6. □

Zweiter Beweis. Wir könnten auch expliziter vorgehen und den Beweis von 1.8.6 nocheinmal wiederholen mit der alternativen Interpretation von $\vec{u}_i, \vec{v}_j$ und $\vec{w}_k$ als den Vektoren unserer angeordneten Basen $\mathcal{A}, \mathcal{B}, \mathcal{C}$. □

Definition 1.10.5. Gegeben ein endlichdimensionaler Vektorraum V mit einer angeordneten Basis $\mathcal{A} = (\vec{v}_1, \ldots, \vec{v}_n)$ notieren wir die inverse Abbildung zur Abbildung $\Phi_{\mathcal{A}} : k^n \xrightarrow{\sim} V$ mit $\Phi_{\mathcal{A}} : (\lambda_1, \ldots, \lambda_n) \mapsto \lambda_1 \vec{v}_1 + \ldots + \lambda_n \vec{v}_n$ in der Form

$$\vec{v} \mapsto {}_{\mathcal{A}}[\vec{v}]$$

und nennen ${}_{\mathcal{A}}[\vec{v}]$ die **Darstellung des Vektors $\vec{v}$ in der Basis $\mathcal{A}$**.

Satz 1.10.6 (Darstellungen des Bildes eines Vektors). *Gegeben endlichdimensionale Räume V, W mit angeordneten Basen $\mathcal{A}, \mathcal{B}$ und eine lineare Abbildung $f : V \to W$ gilt für jeden Vektor $v \in V$, wenn wir ${}_{\mathcal{A}}[v]$ und ${}_{\mathcal{B}}[f(v)]$ für die Zwecke der Matrixmultiplikation als Spaltenmatrizen auffassen, die Identität*

$${}_{\mathcal{B}}[f(v)] = {}_{\mathcal{B}}[f]_{\mathcal{A}} \circ {}_{\mathcal{A}}[v]$$

Beweis. Hier wird bei genauerer Betrachtung nur die Gleichheit von Spaltenvektoren $\Phi_{\mathcal{B}}^{-1}(f(v)) = [(\Phi_{\mathcal{B}}^{-1} f \Phi_{\mathcal{A}})] \circ [\Phi_{\mathcal{A}}^{-1} v]$ behauptet, die aus 1.8.9 folgt. □

1.10.7. Betrachtet man zu einem beliebigen Vektor $v \in V$ die lineare Abbildung $(\cdot v) : k \to V$, $\lambda \mapsto \lambda v$, und bezeichnet mit (1) die angeordnete Basis (1) des k-Vektorraums k, so ergibt sich die Identität ${}_{\mathcal{A}}[v] = {}_{\mathcal{A}}[\cdot v]_{(1)}$. Wegen $(\cdot f(v)) = f \circ (\cdot v)$ können wir damit den vorhergehenden Satz 1.10.6 auch auffassen als den Spezialfall ${}_{\mathcal{B}}[\cdot f(v)]_{(1)} = {}_{\mathcal{B}}[f]_{\mathcal{A}} \circ {}_{\mathcal{A}}[\cdot v]_{(1)}$ von Satz 1.10.4 über die darstellende Matrix einer Verknüpfung.

Definition 1.10.8. Gegeben zwei angeordnete Basen $\mathcal{A} = (v_1, \ldots, v_n)$ und $\mathcal{B} = (w_1, \ldots, w_n)$ eines Vektorraums V nennt man die darstellende Matrix der Identität

$${}_{\mathcal{B}}[\mathrm{id}_V]_{\mathcal{A}}$$

in diesen Basen die **Basiswechselmatrix**. Ihre Einträge a_{ij} werden per definitionem festgelegt durch die Gleichungen $w_j = \sum_{i=1}^{n} a_{ij} v_i$.

1.10.9 (**Änderung der darstellenden Matrix bei Basiswechsel**). Offensichtlich ist ${}_{\mathcal{A}}[\mathrm{id}]_{\mathcal{A}} = I$ die Einheitsmatrix. Nach 1.10.4 ist damit die Basiswechselmatrix ${}_{\mathcal{A}}[\mathrm{id}]_{\mathcal{B}}$ invers zur Basiswechselmatrix in der Gegenrichtung ${}_{\mathcal{B}}[\mathrm{id}]_{\mathcal{A}}$, in Formeln ${}_{\mathcal{A}}[\mathrm{id}]_{\mathcal{B}}^{-1} = {}_{\mathcal{B}}[\mathrm{id}]_{\mathcal{A}}$. Haben wir nun eine lineare Abbildung $f : V \to W$ und angeordnete Basen $\mathcal{A}, \mathcal{B}$ von V und angeordnete Basen $\mathcal{C}, \mathcal{D}$ von W, so folgt aus 1.10.4 die Identität ${}_{\mathcal{D}}[f]_{\mathcal{B}} = {}_{\mathcal{D}}[\mathrm{id}_W]_{\mathcal{C}} \circ {}_{\mathcal{C}}[f]_{\mathcal{A}} \circ {}_{\mathcal{A}}[\mathrm{id}_V]_{\mathcal{B}}$. Sind noch spezieller $\mathcal{A}, \mathcal{B}$ zwei angeordnete Basen ein- und desselben Vektorraums V und ist $f : V \to V$ ein Endomorphismus von V, so erhalten wir die Identität ${}_{\mathcal{B}}[f]_{\mathcal{B}} = {}_{\mathcal{B}}[\mathrm{id}]_{\mathcal{A}} \circ {}_{\mathcal{A}}[f]_{\mathcal{A}} \circ {}_{\mathcal{A}}[\mathrm{id}]_{\mathcal{B}}$ alias

$$N = T^{-1}MT$$

für $N = {}_{\mathcal{B}}[f]_{\mathcal{B}}$ und $M = {}_{\mathcal{A}}[f]_{\mathcal{A}}$ die darstellenden Matrizen bezüglich unserer beiden Basen und $T = {}_{\mathcal{A}}[\mathrm{id}]_{\mathcal{B}}$ die Basiswechselmatrix.

Übung 1.10.10. Gegeben ein K-Vektorraum V mit einer angeordneten Basis $\mathcal{A} = (v_1, \ldots, v_n)$ liefert die Zuordnung, die jeder weiteren angeordneten Basis $\mathcal{B}$ die Basiswechselmatrix von $\mathcal{A}$ nach $\mathcal{B}$ zuordnet, eine Bijektion

$$\begin{array}{ccc} \{\text{angeordnete Basen von } V\} & \xrightarrow{\sim} & \mathrm{GL}(n;K) \\ \mathcal{B} & \mapsto & {}_{\mathcal{B}}[\mathrm{id}]_{\mathcal{A}} \end{array}$$

Satz 1.10.11 (**Smith-Normalform**). *Gegeben eine lineare Abbildung endlichdimensionaler Vektorräume $f : V \to W$ existieren stets angeordnete Basen $\mathcal{A}$ von V und $\mathcal{B}$ von W derart, daß die darstellende Matrix ${}_{\mathcal{B}}[f]_{\mathcal{A}}$ nur auf der Diagonale von Null verschiedene Einträge hat, und zwar erst einige Einsen und danach nur noch Nullen.*

Beweis. Das folgt sofort aus 1.6.13: Wir wählen zunächst eine angeordnete Basis $(w_1, \ldots, w_r)$ des Bildes von f, dazu Urbilder $v_1, \ldots, v_r$ in V, ergänzen diese durch eine angeordnete Basis des Kerns von f zu einer angeordneten Basis $\mathcal{A} = (v_1, \ldots, v_n)$ von V, und ergänzen unsere angeordnete Basis des Bildes zu einer angeordneten Basis $\mathcal{B} = (w_1, \ldots, w_m)$ von W. In diesen Basen hat dann die Matrix von f offensichtlich die behauptete Gestalt. □

Ergänzende Übung 1.10.12. Sei $f : V \to V$ ein **nilpotenter** Endomorphismus eines endlichdimensionalen Vektorraums, als da heißt, es gebe $d \in \mathbb{N}$ mit $f^d = 0$. Man zeige, daß unser Vektorraum eine angeordnete Basis $\mathcal{B}$ besitzt derart, daß die Matrix ${}_{\mathcal{B}}[f]_{\mathcal{B}}$ von f in Bezug auf diese Basis eine obere Dreiecksmatrix ist mit Nullen auf der Diagonalen. Man zeige umgekehrt auch, daß für jede derartige $(n \times n)$-Matrix D gilt $D^{n-1} = 0$. Hinweis: Man betrachte die Teilräume $\ker(f) \subset \ldots \subset \ker(f^{d-1}) \subset \ker(f^d) = V$, beginne mit einer Basis von $\ker(f)$ und ergänze sie sukzessive zu einer Basis von V. Eine stärkere Aussage in dieser Richtung werden wir als 6.5.2 zeigen.

Definition 1.10.13. Die **Spur** einer endlichen quadratischen Matrix ist definiert als die Summe ihrer Diagonaleinträge. Auf englisch und französisch sagt man **trace**, und ich werde die Spur einer Matrix A auch notieren als

$$\operatorname{tr}(A)$$

1.10.14. Eine vielleicht natürlichere Definition der Spur wird in 9.4.5 erklärt. Im Rahmen der Analysis werden wir die Spur in **??** als das Differential der Determinante an der Einheitsmatrix wiedersehen.

Übung 1.10.15. Man zeige $\operatorname{tr}(AB) = \operatorname{tr}(BA)$ wann immer A eine $(m\times n)$-Matrix ist und B eine $(n \times m)$-Matrix. Man folgere daraus die Identität $\operatorname{tr}(BAB^{-1}) = \operatorname{tr}(A)$ wann immer A eine $(n \times n)$-Matrix ist und B eine invertierbare $(n \times n)$-Matrix. Insbesondere kann man jedem Endomorphismus f eines endlichdimensionalen Vektorraums V über einem Körper k seine **Spur**

$$\operatorname{tr}(f) = \operatorname{tr}(f|V) = \operatorname{tr}_k(f|V)$$

zuordnen als die Spur seiner Matrix in Bezug auf eine und jede Basis. Gegeben endlichdimensionale Vektorräume V, W und lineare Abbildungen $f : V \to W$ und $g : W \to V$ zeige man auch $\operatorname{tr}(fg) = \operatorname{tr}(gf)$.

Ergänzende Übung 1.10.16. Leser, die schon mit dem Inhalt des Abschnitts 2.1 über komplexe Zahlen vertraut sind, mögen zeigen: Ist $f : V \to V$ ein Endomorphismus eines endlichdimensionalen $\mathbb{C}$-Vektorraums, so gilt für seine Spur $\operatorname{tr}_{\mathbb{R}}(f|V) = 2 \operatorname{Re} \operatorname{tr}_{\mathbb{C}}(f|V)$.

Ergänzende Übung 1.10.17. Ist L ein endlichdimensionaler k-Vektorraum und $A : L \to L$ eine k-lineare Abbildung, so gilt

$$\operatorname{tr}((A\circ)|\operatorname{End}_k L) = (\dim_k L)\operatorname{tr}(A|L)$$

Ergänzung 1.10.18. Sei f ein Endomorphismus eines Vektorraums V. Ist f von endlichem Rang, so erklärt man die **Spur**

$$\operatorname{tr} f = \operatorname{tr}(f|V)$$

von f als die Spur der Verknüpfung $\operatorname{im} f \hookrightarrow V \twoheadrightarrow \operatorname{im} f$ im Sinne unserer Definition 1.10.15 für die Spur eines Endomorphismus eines endlichdimensionalen Vektorraums. Aus 1.10.15 folgt unmittelbar, daß diese Definition im Fall eines endlichdimensionalen Raums V dieselbe Spur liefert wie unsere ursprüngliche auf den endlichdimensionalen Fall beschränkte Definition 1.10.13.

Ergänzende Übung 1.10.19. Sind V, W Vektorräume und $f : V \to W$ sowie $g : W \to V$ lineare Abbildungen und ist eine unserer Abbildungen von endlichem Rang, so gilt $\operatorname{tr}(fg) = \operatorname{tr}(gf)$. Hinweis: Der endlichdimensionale Fall kann nach 1.10.15 vorausgesetzt werden.

Ergänzende Übung 1.10.20. Gegeben ein Endomorphismus f von endlichem Rang eines Vektorraums mit der Eigenschaft $f^2 = af$ für ein Element a des Grundkörpers gilt stets $\mathrm{tr}(f) = a\dim(\mathrm{im}\, f)$. Hinweis: 1.6.5.

1.11 Dualräume und transponierte Abbildungen

Definition 1.11.1. Gegeben ein Körper K und ein K-Vektorraum V nennt man eine lineare Abbildung $V \to K$ eine **Linearform auf** V oder auch einen **Kovektor**. Die Menge aller solchen Linearformen bildet nach 1.5.17 einen Untervektorraum $\mathrm{Hom}_K(V, K) \subset \mathrm{Ens}(V, K)$. Man nennt diesen Vektorraum aller Linearformen den **Dualraum von** V. Wir verwenden dafür die beiden Notationen

$$V^* = V^\top := \mathrm{Hom}_K(V, K)$$

Üblich ist die Notation V^*. Im Zusammenhang mir darstellenden Matrizen und dergleichen schien mir jedoch die Notation als $V^\top$ suggestivere Formeln zu liefern, weshalb ich in diesem Zusammenhang die sonst eher unübliche Notation $V^\top$ vorziehe.

1.11.2. Die Bezeichnung als **Form** für Abbildungen mit Werten im Grundkörper ist allgemein üblich: Wir kennen bis jetzt nur Linearformen, später werden noch Bilinearformen und quadratische Formen hinzukommen. Über die Herkunft dieser Bezeichnungsweise weiß ich wenig, vermutlich steckt derselbe Wortstamm wie bei dem Wort “Formel” dahinter.

Beispiel 1.11.3. Denken wir uns die Gesamtheit aller Zeitspannen als reellen Vektorraum, so können wir uns den Dualraum dieses Vektorraums denken als die Gesamtheit aller “Frequenzen” oder vielleicht besser aller möglichen “Drehgeschwindigkeiten von Drehungen um eine feste Achse”. Zeichnen wir genauer einen Drehsinn als positiv aus, so entpräche eine Drehgeschwindigkeit der Linearform, die jeder Zeitspanne die Zahl der in dieser Zeitspanne erfolgten Umdrehungen zuordnet. Die zur Basis “Minute” der Gesamtheit aller Zeitspannen “duale Basis”, die wir gleich in allgemeinen Dualräumen einführen werden, bestünde dann aus dem Vektor “eine Umdrehung pro Minute in positivem Drehsinn”, den man üblicherweise **Umin** notiert. An dieser Stelle möchte ich Sie am liebsten wieder einmal davon überzeugen, daß das Abstrakte das eigentlich Konkrete ist.

Beispiel 1.11.4. Denken wir uns wie in 1.3.15 den Raum der Anschauung mit einem ausgezeichneten festen Punkt als reellen Vektorraum, so liefert jeder von Null verschiedene Vektor eine Linearform auf unserem Vektorraum vermittels der anschaulich zu verstehenden Vorschrift “projiziere jeden weiteren Vektor orthogonal auf die Gerade durch den gegebenen Vektor und nimm die Zahl, mit der

man den den gegebenen Vektor multiplizieren muß, um die Projektion zu erhalten". Diese Entsprechung hat nur den Nachteil, daß der doppelte Vektor die halbe Linearform liefert und daß überhaupt die Addition von Vektoren keineswegs der Addition von Linearformen entspricht. Wählt man eine feste anschaulich zu verstehende Längeneinheit, so kann man den Raum der Linearformen auf dem Raum der Vektoren in unserem Bild identifizieren mit dem Raum der Vektoren selber, indem man jedem Vektor als Linearform dieselbe Linearform wie oben zuordnet, nur noch zusätzlich geteilt durch das Quadrat seiner Länge. In anderen Worten kann diese Linearform auch beschrieben werden als "beliebigem Vektor ordne zu Länge der Projektion mal Länge des gegebenen Vektors". Diese Identifikation entspräche dann einem Vektorraumisomorphismus, und es ist vielleicht die Möglichkeit dieser Identifikation, die es uns so schwer macht, eine Anschauung für den Dualraum zu entwickeln. Sie benutzt jedoch die "euklidische Struktur" des Raums der Anschauung, die das Reden über orthogonale Projektionen eigentlich erst ermöglicht und die wir in erst 4.1 mathematisch modellieren werden. Auf allgemeinen Vektorräumen stehen uns keine orthogonalen Projektionen zur Verfügung und der Dualraum kann dann nicht mehr in natürlicher Weise mit dem Ausgangsraum identifiziert werden.

1.11.5. Gegeben ein k-Vektorraum V haben wir stets eine kanonische bilineare Abbildung $V \times V^\top \to k$, die **Auswertungsabbildung**, auch die **kanonische Paarung** von Vektoren mit Kovektoren genannt.

1.11.6. Gegeben ein endlichdimensionaler Vektorraum stimmt seine Dimension etwa nach 1.5.17 mit der Dimension seines Dualraums überein, in Formeln

$$\dim V^\top = \dim V$$

Ergänzung 1.11.7. Im Fall eines unendlichdimensionalen Vektorraums ist wieder nach 1.5.17 auch sein Dualraum unendlichdimensional, aber seine Dimension ist "noch unendlicher" als die Dimension des Ausgangsraums in einem Sinne, der in **??** präzisiert wird.

Ergänzende Übung 1.11.8. Sei k ein Körper und V ein k-Vektorraum. Eine endliche Familie von Linearformen $f_1, \ldots, f_n \in V^\top$ ist linear unabhängig genau dann, wenn sie eine Surjektion $(f_1, \ldots, f_n) : V \twoheadrightarrow k^n$ liefert.

Definition 1.11.9. Gegeben eine K-linare Abbildung $f : V \to W$ erklären wir die **duale** oder auch **transponierte** Abbildung

$$f^\top : W^\top \to V^\top$$

als das "Vorschalten von f", in Formeln $f^\top(\lambda) = \lambda \circ f : V \to K$ für jede Linearform $\lambda : W \to K$. Man beachte, daß diese Abbildung "in die umgekehrte

Richtung" geht. Oft wird sie diese Abbildung auch $f^* : W^* \to V^*$ notiert. Nicht selten schreibt man auch ein kleines t als Index oben links und notiert die transponierte Abbildung ${}^t f$.

1.11.10. Sicher gilt stets $\mathrm{id}_V^\top = \mathrm{id}_{V^\top} : V^\top \to V^\top$. Man prüft auch leicht für eine Verknüpfung $f \circ g$ von linearen Abbildungen die Identität

$$(f \circ g)^\top = g^\top \circ f^\top$$

In der Tat bedeutet das Vorschalten von $f \circ g$ nichts anderes, als erst f und dann g vorzuschalten.

Übung 1.11.11. Gegeben Vektorräume V, W liefern die transponierten Abbildungen zu den kanonischen Injektionen nach 1.5.3 auf den Dualräumen einen Isomorphismus $(\mathrm{in}_V^\top, \mathrm{in}_W^\top) : (V \oplus W)^\top \xrightarrow{\sim} V^\top \oplus W^\top$. Analoges gilt für allgemeinere endliche Summen.

1.11.12. Eine von Null verschiedene Linearform mag man sich veranschaulichen, indem man sich den affinen Teilraum vorstellt, auf dem sie den Wert Eins annimmt. In dieser Anschauung ist insbesondere für einen Automorphismus $f : \mathbb{R}^2 \xrightarrow{\sim} \mathbb{R}^2$ der Effekt des Inversen $(f^\top)^{-1}$ der transponierten Abbildung auf Linearformen gut verständlich.

1.11.13. Gegeben eine Basis $B \subset V$ erhalten wir im Dualraum $V^\top$ eine linear unabhängige Familie von Linearformen

$$(b^\top)_{b \in B}$$

indem wir $b^\top : V \to K$ erklären durch $b^\top(c) = \delta_{bc} \quad \forall c \in B$. Die $b^\top$ heißen die **Koordinatenfunktionen** oder kurz **Koordinaten** zur Basis B. Vielfach werden sie auch b^* notiert. Ist etwa $V = \mathbb{R}^n$ und $B = (\vec{e}_1, \ldots, \vec{e}_n)$ die Standardbasis, so wird $\vec{e}_i^\top : \mathbb{R}^n \to \mathbb{R}$ die "Projektion auf die i-te Koordinate" $\vec{e}_i^\top : (x_1, \ldots, x_n) \mapsto x_i$, die man oft auch einfach $x_i : \mathbb{R}^n \to \mathbb{R}$ notiert und die "i-te Koordinatenfunktion" nennt. Man beachte, daß die Koordinatenfunktion $b^\top$ keineswegs nur vom Basisvektor b abhängt, auch wenn die Notation das suggerieren mag, sondern vielmehr von der ganzen Basis B.

1.11.14. Für jeden endlichdimensionalen Vektorraum V hat der Dualraum, wie etwa aus 1.5.17 folgt, dieselbe Dimension wie V selber. Ist also $\mathcal{B}$ eine angeordnete Basis von V, so ist $\mathcal{B}^\top = (b^\top)_{b \in \mathcal{B}}$ als linear unabhängige Familie der richtigen Kardinalität auch eine angeordnete Basis des Dualraums $V^\top$. Man nennt dann $\mathcal{B}^\top$ die **duale Basis** zur Basis $\mathcal{B}$.

Proposition 1.11.15 (Matrix der dualen Abbildung). *Gegeben eine lineare Abbildung $f : V \to W$ von endlichdimensionalen Vektorräumen mit angeordneten*

Basen $\mathcal{A}$ bzw. $\mathcal{B}$ ist die darstellende Matrix der dualen Abbildung $f^\top : W^\top \to V^\top$ bezüglich der dualen Basen $\mathcal{B}^\top$ bzw. $\mathcal{A}^\top$ gerade die transponierte Matrix, in Formeln

$$ {}_{\mathcal{A}^\top}[f^\top]_{\mathcal{B}^\top} = ({}_{\mathcal{B}}[f]_{\mathcal{A}})^\top $$

1.11.16. Diese Identität ist der Grund dafür, daß ich für den Dualraum vorzugsweise die Notation mit einem hochgestellten $\top$ verwenden will.

Beweis. Seien etwa $\mathcal{A} = (v_1, \ldots, v_n)$ und $\mathcal{B} = (w_1, \ldots, w_n)$. Die Matrixeinträge a_{ij} der darstellenden Matrix ${}_{\mathcal{B}}[f]_{\mathcal{A}}$ sind festgelegt durch die Identität von Vektoren $f(v_j) = \sum_i a_{ij} w_i$. Die Matrixeinträge b_{ji} der darstellenden Matrix ${}_{\mathcal{A}^\top}[f^\top]_{\mathcal{B}^\top}$ sind festgelegt durch die Identität von Linearformen $f^\top(w_i^\top) = \sum_j b_{ji} v_j^\top$. Es gilt zu zeigen $b_{ji} = a_{ij}$. Um das zu sehen, werten wir diese Identität von Linearformen auf den Vektoren v_k aus und erhalten

$$ b_{ki} = \sum_j b_{ji} v_j^\top(v_k) = (f^\top(w_i^\top))(v_k) = w_i^\top(f(v_k)) = w_i^\top\left(\sum_l a_{lk} w_l\right) = a_{ik} $$

was zu zeigen war. □

1.11.17. Sei V ein endlichdimensionaler Vektorraum mit einer angeordneten Basis $\mathcal{A}$. Gegeben ein Vektor $v \in V$ und eine Linearform $\lambda \in V^\top$ kann man den Wert der Linearform auf dem Vektor auch darstellen als das Matrixprodukt $\lambda(v) = ({}_{\mathcal{A}^\top}[\lambda])^\top \circ {}_{\mathcal{A}}[v]$ der Zeilenmatrix $({}_{\mathcal{A}^\top}[\lambda])^\top$ mit der Spaltenmatrix ${}_{\mathcal{A}}[v]$. Ist in der Tat $\mathcal{A} = (v_1, \ldots, v_n)$ und $v = a_1 v_1 + \ldots + a_n v_n$ und $\lambda = b_1 v_1^\top + \ldots + b_n v_n^\top$, so finden wir unmittelbar $\lambda(v) = b_1 a_1 + \ldots + b_n a_n$. Vereinbaren wir zusätzlich die Notation $({}_{\mathcal{A}^\top}[\lambda])^\top = [\lambda]_{\mathcal{A}}$, so nimmt diese Formel die besonders einfache Gestalt

$$ \lambda(v) = [\lambda]_{\mathcal{A}} \circ {}_{\mathcal{A}}[v] $$

an. Diese Notation ist auch deshalb vernünftig, weil ja bezüglich der Standardbasis (1) des Grundkörpers K per definitionem gilt

$$ {}_{(1)}[\lambda]_{\mathcal{A}} = [\lambda]_{\mathcal{A}} $$

Erinnern wir dann noch für $v \in V$ an die lineare Abbildung $(\cdot v) : K \to V$ mit $\alpha \mapsto \alpha v$ und unsere Identität ${}_{\mathcal{A}}[\cdot v]_{(1)} = {}_{\mathcal{A}}[v]$, so kann auch obige Formel interpretiert werden als der Spezialfall

$$ {}_{(1)}[\lambda \circ (\cdot v)]_{(1)} = {}_{(1)}[\lambda]_{\mathcal{A}} \circ {}_{\mathcal{A}}[\cdot v]_{(1)} $$

der allgemeinen Formel 1.10.4 für die Matrix der Verknüpfung zweier linearer Abbildungen.

Beispiel 1.11.18. Gegeben ein Vektorraumisomorphismus $f : V \xrightarrow{\sim} W$ ist die duale Abbildung ein Vektorraumisomorphismus $f^\top : W^\top \xrightarrow{\sim} V^\top$ und ihre Inverse ist ein Vektorraumisomorphismus $(f^\top)^{-1} : V^\top \xrightarrow{\sim} W^\top$. Dieser Isomorphismus leistet, was man sich anschaulich vielleicht am ehesten unter dem "Transport einer Linearform" vorstellt: Gegeben $v \in V$ und $\lambda \in V^\top$ nimmt $(f^\top)^{-1}(\lambda)$ auf $f(v)$ denselben Wert an wie λ auf v. Betrachten wir etwa die Scherung $f : \mathbb{R}^2 \xrightarrow{\sim} \mathbb{R}^2$, $(x, y) \mapsto (x + y, y)$ mit der Matrix $[f] = \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$und $f(\vec{e}_1) = \vec{e}_1, f(\vec{e}_2) = \vec{e}_1 + \vec{e}_2$. Offensichtlich bleibt die y-Koordinate eines Punktes unter solch einer Scherung unverändert, $(f^\top)^{-1}(\vec{e}_2^\top) = \vec{e}_2^\top$, und die x-Koordinate des Urbildpunkts entspricht der Differenz zwischen x-Koordinate und y-Koordinate des Bildpunkts, $(f^\top)^{-1}(\vec{e}_1^\top) = \vec{e}_1^\top - \vec{e}_2^\top$. Das entspricht auch unseren Formeln, nach denen $f^\top$ bezüglich der Basis $(\vec{e}_1^\top, \vec{e}_2^\top)$ dargestellt wird durch die transponierte Matrix $\left(\begin{smallmatrix}1 & 0\\ -1 & 1\end{smallmatrix}\right)$, was genau die Formel $(f^\top)^{-1} : \vec{e}_1^\top \mapsto \vec{e}_1^\top - \vec{e}_2^\top$ und $(f^\top)^{-1} : \vec{e}_2^\top \mapsto \vec{e}_2^\top$ beinhaltet.

Definition 1.11.19. Sei K ein Körper und V ein K-Vektorraum. Der Dualraum des Dualraums von V heißt sein **Bidualraum** und wird notiert $(V^\top)^\top = V^{\top\top}$ oder in der Literatur meist V^{**}. Wir erklären die **kanonische Einbettung in den Bidualraum** alias **Evaluationsabbildung**

$$\mathrm{ev} = \mathrm{ev}_V : V \hookrightarrow V^{\top\top}$$

als die Vorschrift, die jedem Vektor $v \in V$ das "Evaluieren auf v" zuordnet. In Formeln ist $\mathrm{ev}(v) \in V^{\top\top}$ also definiert als die lineare Abbildung $\mathrm{ev}(v) : V^\top \to K, \lambda \mapsto \lambda(v)$.

1.11.20. Die Injektivität der kanonischen Abbildung $V \to V^{\top\top}$ ergibt sich aus der Erkenntnis, daß es für jeden von Null verschiedenen Vektor $v \neq 0$ eine Linearform $\lambda \in V^\top$ gibt mit $\lambda(v) \neq 0$. Man kann das etwa zeigen, indem man den Satz 1.5.24 über die Fortsetzbarkeit linearer Abbildungen bemüht oder auch, indem man v zu einer Basis B von V ergänzt und dann $\lambda = v^\top$ wählt. Im Fall unendlichdimensionaler Räume brauchen wir jedoch in jedem Fall den Basiserweiterungssatz in seiner vollen Allgemeinheit 1.4.38, in der wir ihn nicht bewiesen, sondern als Axiom hingenommen haben. Man kann ohne die ihm zugrundeliegenden raffinierteren Methoden der Mengenlehre noch nicht einmal zeigen, daß es auf einem beliebigen von Null verschiedenen Vektorraum überhaupt irgendeine von Null verschiedene Linearform gibt.

1.11.21. Im Fall eines endlichdimensionalen Vektorraums V zeigt ein Dimensionsvergleich unmittelbar, daß die Evaluationsabbildung einen Isomorphismus $V \xrightarrow{\sim} V^{\top\top}$ liefern muß. Manchmal wird diese Erkenntnis als Gleichung $V = V^{\top\top}$ geschrieben, aber das ist dann mit einigen Hintergedanken zu lesen, denn gleich sind diese beiden Mengen ja keineswegs.

1.11.22. Oft verwende ich für das Auswerten einer Linearform $\lambda \in V^\top$ auf einem Vektor $v \in V$ auch die symmetrischeren Notationen $\langle \lambda, v\rangle$ oder sogar $\langle v, \lambda\rangle$.

1.11.23. Gegeben eine lineare Abbildung $f : V \to W$ kommutiert das Diagramm

$$\begin{array}{ccc} V & \xrightarrow{\mathrm{ev}_V} & V^{\top\top} \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f^{\top\top}} \\ W & \xrightarrow{\mathrm{ev}_W} & W^{\top\top} \end{array}$$

als da heißt, es gilt die Identität $\mathrm{ev}_W \circ f = f^{\top\top} \circ \mathrm{ev}_V$ von Abbildungen $V \to W^{\top\top}$. Um das zu sehen, muß man nur für alle $v \in V$ die Identität $f^{\top\top}(\mathrm{ev}_V(v)) = \mathrm{ev}_W(f(v))$ in $W^{\top\top}$ prüfen. Dazu gilt es zu zeigen, daß beide Seiten auf allen $\lambda \in W^\top$ denselben Wert annehmen, daß also gilt

$$(f^{\top\top}(\mathrm{ev}_V(v)))(\lambda) = (\mathrm{ev}_W(f(v)))(\lambda)$$

alias $((\mathrm{ev}_V\, v) \circ f^\top)(\lambda) = \lambda(f(v))$ alias $(\mathrm{ev}_V\, v)(\lambda \circ f) = \lambda(f(v))$, und das ist klar.

Übung 1.11.24. Für endlichdimensionale Vektorräume V ist die kanonische Einbettung aus Dimensionsgründen stets ein Isomorphismus $V \xrightarrow{\sim} V^{\top\top}$. Gegeben ein endlichdimensionaler Vektorraum V zeige man, daß unter der kanonischen Identifikation $\mathrm{ev}_V : V \xrightarrow{\sim} V^{\top\top}$ jede Basis B ihrer Bidualen entspricht, in Formeln

$$\mathrm{ev}_V(b) = (b^\top)^\top \quad \forall b \in B$$

Ergänzende Übung 1.11.25. Man zeige: Gegeben ein Vektorraum V ist die Verknüpfung

$$V^\top \xrightarrow{\mathrm{ev}_{V^\top}} V^{\top\top\top} \xrightarrow{\mathrm{ev}_V^\top} V^\top$$

der Auswertungsabbildung zum Dualraum von V mit der Transponierten der Auswertungsabbildung von V die Identität auf dem Dualraum von V.

Ergänzende Übung 1.11.26. Gegeben ein affiner Raum E über einem Körper k ist der Raum $\mathrm{Aff}(E,k) \subset \mathrm{Ens}(E,k)$ aller affinen Abbildungen $E \to k$ ein Untervektorraum im Raum aller Abbildungen von E nach k. Den in seinem Dualraum von den Auswertungen an Punkten aufgespannten Untervektorraum $\mathrm{Lin}(E) \subset \mathrm{Aff}(E,k)^\top$ nennen wir die **Linearisierung** des affinen Raums E. Man zeige: Im endlichdimensionalen Fall ist diese Linearisierung bereits der ganze Dualraum, in Formeln $\mathrm{Lin}(E) = \mathrm{Aff}(E,k)^\top$. In jedem Fall erhalten wir eine Bijektion

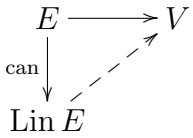
$$(E \times k^\times) \sqcup \vec{E} \;\xrightarrow{\sim}\; \mathrm{Lin}(E)$$

indem wir jedem Paar (e, λ) das λ-fache der Auswertung bei e zuordnen und jedem Richtungsvektor $\vec{v}$ die Vorschrift, die einem $\varphi \in \mathrm{Aff}(E,k)$ den Wert der

konstanten Funktion $p \mapsto \varphi(p + \vec{v}) - \varphi(p)$ zuordnet. Man gebe nun Formeln an für die Verknüpfung auf $(E \times k^\times) \sqcup \vec{E}$, die unter besagter Bijektion der Addition von Vektoren entsprechen. Man zeige weiter, daß die kanonische Abbildung $\mathrm{can} : E \to \mathrm{Lin}\, E$, die jedem Punkt $e \in E$ das Auswerten bei e zuordnet, die universelle Eigenschaft hat, daß für jeden k-Vektorraum das Vorschalten von can eine Bijektion

$$\mathrm{Hom}_k(\mathrm{Lin}\, E, V) \xrightarrow{\sim} \mathrm{Aff}_k(E, V)$$

induziert. In anderen Worten faktorisiert also jede affine Abbildung von einem affinen Raum in einen Vektorraum auf genau eine Weise über eine linare Abbildung seiner Linearisierung in besagten Vektorraum, im Diagramm



2 Gruppen, Ringe, Polynome

2.1 Der Körper der komplexen Zahlen

2.1.1. Viele mathematische Zusammenhänge werden besonders transparent, wenn man sie im Rahmen der sogenannten "komplexen Zahlen" behandelt. Ich denke hier etwa an die Integration rationaler Funktionen **??**, die Normalform orthogonaler Matrizen 4.3.23 oder die Lösung der Schwingungsgleichung **??**. Die abschreckenden Bezeichnungen "komplexe Zahlen" oder auch "imaginäre Zahlen" für diesen ebenso einfachen wie konkreten Körper haben historische Gründe: Als man in Italien bemerkte, daß man polynomiale Gleichungen der Ordnungen drei und vier lösen kann, wenn man so tut, als ob man aus -1 eine Quadratwurzel ziehen könnte, gab es noch keine Mengenlehre und erst recht nicht den abstrakten Begriff eines Körpers I.3.3.1. Das Rechnen mit Zahlen, die keine konkreten Interpretationen als Länge oder Guthaben oder zumindest als Schulden haben, schien eine "imaginäre" Angelegenheit, ein bloßer Trick, um zu reellen Lösungen reeller Gleichungen zu kommen.

2.1.2. In diesem Abschnitt werden die komplexen Zahlen nur als algebraische Struktur diskutiert. Für die Diskussion der analytischen Aspekte, insbesondere die komplexe Exponentialfunktion und ihre Beziehung zu den trigonometrischen Funktionen, sowie für den Beweis des Fundamentalsatzes der Algebra, verweise ich auf die Analysis, insbesondere auf **??** und **??**.

Satz 2.1.3 (Charakterisierung der komplexen Zahlen). *1. Es gibt Tripel $(\mathbb{C}, \mathrm{i}, c)$ bestehend aus einem Körper $\mathbb{C}$, einem Element $\mathrm{i} \in \mathbb{C}$ und einem Körperhomomorphismus $c : \mathbb{R} \to \mathbb{C}$ derart, daß gilt $\mathrm{i}^2 = -1$ und daß i und 1 eine $\mathbb{R}$-Basis von $\mathbb{C}$ bilden, für die durch c auf $\mathbb{C}$ gegebene Struktur als $\mathbb{R}$-Vektorraum.*

2. Derartige Tripel sind im Wesentlichen eindeutig bestimmt. Ist genauer $(\mathbb{C}', \mathrm{i}', c')$ ein weiteres derartiges Tripel, so gibt es genau einen Körperisomorphismus $\varphi : \mathbb{C} \xrightarrow{\sim} \mathbb{C}'$ mit $\varphi : \mathrm{i} \mapsto \mathrm{i}'$ und $\varphi \circ c = c'$.

Definition 2.1.4. Wir wählen für den weiteren Verlauf der Vorlesung ein festes Tripel $(\mathbb{C}, \mathrm{i}, c)$ der im Satz beschriebenen Art, kürzen für reelle Zahlen $a \in \mathbb{R}$ stets $c(a) = a$ ab, und gehen sogar so weit, die reellen Zahlen vermittels c als Teilmenge von $\mathbb{C}$ aufzufassen. Wegen der im zweiten Teil des Satzes formulierten "Eindeutigkeit bis auf eindeutigen Isomorphismus" erlauben wir uns von nun an auch den bestimmten Artikel und nennen $\mathbb{C}$ **den Körper der komplexen Zahlen**.

Ergänzung 2.1.5. Man beachte, daß $\mathbb{C}$ als Körper ohne weitere Daten in keinster Weise eindeutig ist bis auf eindeutigen Isomorphismus, im Gegensatz zum Körper

SkriptenBilder/Bild0018.png

Anschauung für das Quadrieren komplexer Zahlen

der reellen Zahlen **??**. Genauer gibt es überabzählbar viele Körperisomorphismen $\mathbb{C} \xrightarrow{\sim} \mathbb{C}$ und auch überabzählbar viele nicht-bijektive Körperhomomorphismen $\mathbb{C} \to \mathbb{C}$, wie etwa in **??** ausgeführt wird. Beschränkt man sich jedoch auf im Sinne von **??** "stetige" Körperhomomorphismen $\mathbb{C} \to \mathbb{C}$ in Bezug auf die "natürliche Topologie" im Sinne von **??**, so gibt es davon nur noch zwei, die Identität und die sogenannte "komplexe Konjugation", die wir bald kennenlernen werden.

2.1.6. Ich hoffe, Sie werden bald merken, daß viele Fragestellungen sich bei Verwendung dieser sogenannt komplexen Zahlen sehr viel leichter lösen lassen, und daß die komplexen Zahlen auch der Anschauung ebenso zugänglich sind wie die reellen Zahlen. Früher schrieb man "complex", deshalb die Bezeichnung $\mathbb{C}$. Unser i ist eine "Wurzel aus -1", und weil es so eine Wurzel in den reellen Zahlen nicht geben kann, notiert man sie i wie "imaginär".

Ergänzung 2.1.7. Für feinere Untersuchungen finde ich es praktisch, auch Paare (K, c) zu betrachten, die aus einem Körper K nebst einem Körperhomomorphismus $c : \mathbb{R} \to K$ bestehen derart, daß es einen Isomorphismus $a : K \xrightarrow{\sim} \mathbb{C}$ gibt, der mit den vorgegebenen Einbettungen von $\mathbb{R}$ verträglich ist. Auch bei solch einem Paar notiere ich den Körper K gerne $\mathbb{C}$, fasse die Einbettung von $\mathbb{R}$ als Einbettung einer Teilmenge auf, und notiere sie nicht. Ich rede dann von einem Körper von **vergesslichen komplexen Zahlen**, da es sich dabei salopp gesprochen um eine "Kopie von $\mathbb{C}$ handelt, die vergessen hat, welche ihrer beiden Wurzeln von -1 sie als i auszeichnen wollte".

Beweis. Wir beginnen mit der Eindeutigkeit. Jede komplexe Zahl $z \in \mathbb{C}$ läßt sich ja eindeutig schreiben in der Form $z = a + b\,\mathrm{i}$ mit $a, b \in \mathbb{R}$. Die Addition und Multiplikation in $\mathbb{C}$ haben in dieser Notation die Gestalt

$$\begin{aligned}(a + b\,\mathrm{i}) + (c + d\,\mathrm{i}) &= (a + c) + (b + d)\,\mathrm{i}\\ (a + b\,\mathrm{i})(c + d\,\mathrm{i}) &= (ac - bd) + (ad + bc)\,\mathrm{i}\end{aligned}$$

und damit ist auch bereits die im zweiten Teil formulierte Eindeutigkeitsaussage gezeigt. Natürlich kann man auch die Existenz direkt anhand dieser Rechenregeln prüfen. So gewinnt man an Unabhängigkeit von der linearen Algebra, verliert aber an Anschauung und muß die Körperaxiome ohne Einsicht nachrechnen. Das sollten Sie bereits als Übung I.3.3.14 durchgeführt haben. Alternativ kann man die im ersten Teil behauptete Existenz mit mehr Kenntnissen in linearer Algebra auch mit weniger Rechnung wie folgt einsehen: Man betrachte die Menge $\mathbb{C}$ aller reellen 2×2-Matrizen der Gestalt

$$\mathbb{C} = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \middle| \, a, b \in \mathbb{R} \right\} \subset \mathrm{M}(2 \times 2; \mathbb{R})$$

Das sind genau die Matrizen zu Drehstreckungen der Ebene. Die Addition und Multiplikation von Matrizen induziert offensichtlich eine Addition und Multiplikation auf $\mathbb{C}$, man prüft mühelos die Körperaxiome I.3.3.1 und erhält so einen Körper $\mathbb{C}$. Die Drehung um einen rechten Winkel oder vielmehr ihre Matrix

$$\mathrm{i} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

hat natürlich die Eigenschaft sofort $\mathrm{i}^2 = -1$, und die Abbildung $c : \mathbb{R} \to \mathbb{C}$ gegeben durch $a \mapsto \mathrm{diag}(a, a)$ ist ein Körperhomomorphismus derart, daß das Tripel $(\mathbb{C}, \mathrm{i}, c)$ die geforderten Eigenschaften besitzt. □

2.1.8. Es ist allgemein üblich, komplexe Zahlen mit z zu bezeichnen und als $z = x+y\,\mathrm{i}$ zu schreiben mit $x, y \in \mathbb{R}$. Man kann sich die komplexe Zahl $z = x+y\,\mathrm{i}$ vorstellen als den Punkt (x, y) der Koordinatenebene $\mathbb{R}^2$. Unter dieser Identifikation von $\mathbb{C}$ mit $\mathbb{R}^2$ bedeutet für $w \in \mathbb{C}$ die Additionsabbildung $(w+) : \mathbb{C} \to \mathbb{C}$, $z \mapsto w + z$ geometrisch die Verschiebung um den Vektor w, und die Multiplikationsabbildung $(w\cdot) : \mathbb{C} \to \mathbb{C}$, $z \mapsto wz$ bedeutet diejenige Drehstreckung, die $(1, 0)$ in w überführt.

Definition 2.1.9. Für eine komplexe Zahl $z = x + y\,\mathrm{i}$ nennt man x ihren **Realteil** $x = \mathrm{Re}\, z$ und y ihren **Imaginärteil** $y = \mathrm{Im}\, z$. Wir haben damit zwei Funktionen

$$\mathrm{Re}, \mathrm{Im} : \mathbb{C} \to \mathbb{R}$$

definiert und es gilt $z = \mathrm{Re}\, z + \mathrm{i}\,\mathrm{Im}\, z$ für alle $z \in \mathbb{C}$. Man definiert weiter die **Norm** $|z|$ einer komplexen Zahl $z = x + y\,\mathrm{i} \in \mathbb{C}$ durch $|z| = \sqrt{x^2 + y^2} \in \mathbb{R}_{\geq 0}$.

2.1.10. Offensichtlich gilt für unsere Norm komplexer Zahlen aus 2.1.9

$$|z| = 0 \Leftrightarrow z = 0$$

Da in einem Dreieck eine einzelne Seite nicht länger sein kann als die beiden anderen zusammengenommen und formal etwa nach 4.2.20.2 gilt weiter die **Dreiecksungleichung**

$$|z + w| \leq |z| + |w|$$

Da offensichtlich auch gilt $|\lambda z| = |\lambda||z|$ für alle $\lambda \in \mathbb{R}$ ist unsere Norm $z \mapsto |z|$ im Sinne von **??** eine Norm auf dem $\mathbb{R}$-Vektorraum $\mathbb{C}$. Die durch diese Norm definierte Metrik nehmen wir als unsere Standardmetrik auf $\mathbb{C}$.

2.1.11. Stellen wir uns $|z|$ vor als den Streckfaktor der Drehstreckung $(z\cdot)$, so wird anschaulich klar, daß sogar für alle $z, w \in \mathbb{C}$ gelten muß

$$|zw| = |z||w|$$

Dies Bild soll zusätzliche Anschauung für die Abbildung $z \mapsto z^2$ der komplexen Zahlenebene auf sich selbst vermitteln. Es stellt diese Abbildung dar als die Komposition einer Abbildung der Einheitskreisscheibe auf eine räumliche sich selbst durchdringende Fläche, gegeben in etwa durch eine Formel der Gestalt $z \mapsto (z^2, \varepsilon(\operatorname{Im} z))$ in $\mathbb{C} \times \mathbb{R} \cong \mathbb{R}^3$ für geeignetes monotones und in einer Umgebung von Null streng monotones ε, gefolgt von einer senkrechten Projektion auf die ersten beiden Koordinaten. Das hat den Vorteil, daß im ersten Schritt nur Punkte der reellen Achse identifiziert werden, was man sich leicht wegdenken kann, und daß der zweite Schritt eine sehr anschauliche Bedeutung hat, eben die senkrechte Projektion.

Besonders bequem rechnet man diese Formel nach, indem man zunächst für $z = x + y\,\mathrm{i} \in \mathbb{C}$ die **konjugierte komplexe Zahl** $\bar{z} = x - y\,\mathrm{i} \in \mathbb{C}$ einführt und die Formeln

$$\begin{aligned} \overline{z+w} &= \bar{z} + \bar{w} \\ \overline{z \cdot w} &= \bar{z} \cdot \bar{w} \\ |z|^2 &= z\bar{z} \end{aligned}$$

prüft. Dann rechnet man einfach

$$|zw|^2 = zw\overline{zw} = z\bar{z}w\bar{w} = |z|^2|w|^2$$

In der Terminologie aus I.3.3.13 ist $z \mapsto \bar{z}$ ein Körperisomorphismus $\mathbb{C} \to \mathbb{C}$ und es gilt offensichtlich $\bar{\bar{z}} = z$.

2.1.12. Wir können den Realteil und den Imaginärteil von $z \in \mathbb{C}$ mithilfe der konjugierten komplexen Zahl ausdrücken als

$$\mathrm{Re}\, z = \frac{z + \bar{z}}{2} \qquad \mathrm{Im}\, z = \frac{z - \bar{z}}{2\,\mathrm{i}}$$

Weiter gilt offensichtlich $z = \overline{z} \Leftrightarrow z \in \mathbb{R}$, und für komplexe Zahlen z der Norm $|z| = 1$ ist die konjugierte komplexe Zahl genau das Inverse, in Formeln $|z| = 1 \Leftrightarrow \bar{z} = z^{-1}$. Anschaulich kann man das Bilden des Inversen interpretieren als die "Spiegelung" oder präziser **Inversion** am Einheitskreis $z \mapsto z/|z|^2$ gefolgt von der Spiegelung an der reellen Achse $z \mapsto \bar{z}$.

Übung 2.1.13. Man beschreibe die Abbildung $z \mapsto (az+b)/(cz+d)$ für $a, b, c, d \in \mathbb{C}$ anschaulich als Produkt einer Inversion an einem geeigneten Kreis gefolgt von einer Spiegelung an einer geeigneten Geraden.

Übung 2.1.14. Gegeben eine komplexe Zahl $z = x + \mathrm{i}\, y$ zeige man für Real- und Imaginärteil ihrer Inversen die Formeln $\mathrm{Re}(z^{-1}) = x/(x^2 + y^2)$ und $\mathrm{Im}(z^{-1}) = -y/(x^2 + y^2)$.

Übung 2.1.15. Man bestimme Real- und Imaginärteil einer Quadratwurzel von i. Man bestimme Real- und Imaginärteil einer Quadratwurzel von $1 + \mathrm{i}$.

2.1.16. Für eine Diskussion der analytischen Aspekte der komplexen Zahlen, insbesondere die komplexe Exponentialfunktion und ihre Beziehung zu den trigonometrischen Funktionen, sowie für den Beweis des Fundamentalsatzes der Algebra, verweise ich wie bereits erwähnt auf die Analysis, insbesondere auf **??** und **??**.

2.2 Untergruppen der ganzen Zahlen

Definition 2.2.1. Eine Teilmenge einer Gruppe heißt eine **Untergruppe** genau dann, wenn sie abgeschlossen ist unter der Verknüpfung und der Inversenbildung

Anschauung für das Invertieren komplexer Zahlen

und wenn sie zusätzlich das neutrale Element enthält. Ist G eine multiplikativ geschriebene Gruppe, so ist demnach eine Teilmenge $U \subset G$ eine Untergruppe genau dann, wenn in Formeln gilt: $a, b \in U \Rightarrow ab \in U$, $a \in U \Rightarrow a^{-1} \in U$ sowie $1 \in U$.

Ergänzung 2.2.2. Nach der reinen Lehre sollte eine Teilmenge einer Gruppe eine "Untergruppe" heißen genau dann, wenn sie so mit der Struktur einer Gruppe versehen werden kann, daß die Einbettung ein Gruppenhomomorphismus wird. Da diese Definition jedoch für Anwendungen erst aufgeschlüsselt werden muß, haben wir gleich die aufgeschlüsselte Fassung als unsere Definition genommen und überlassen den Nachweis der Äquivalenz zur Definition nach der reinen Lehre dem Leser zur Übung.

Beispiele 2.2.3. In jeder Gruppe ist die einelementige Teilmenge, die nur aus dem neutralen Element besteht, eine Untergruppe. Wir nennen sie die **triviale Untergruppe**. Ebenso ist natürlich die ganze Gruppe stets eine Untergruppe von sich selber.

Ergänzende Übung 2.2.4. Eine endliche Teilmenge einer Gruppe, die mit je zwei Elementen auch die Verknüpfung der beiden enthält, ist notwendig bereits eine Untergruppe.

Übung 2.2.5. Sind $H, K \subset G$ zwei Untergruppen einer multiplikativ gedachten Gruppe mit $H \cap K = 1$, so definiert die Multiplikation eine Injektion $H \times K \hookrightarrow G$.

Übung 2.2.6. Wieviele Untergruppen hat die additive Gruppe eines zweidimensionalen Vektorraums über dem Körper mit zwei Elementen? Wieviele Untergruppen hat die additive Gruppe eines n-dimensionalen Vektorraums über dem Körper mit zwei Elementen?

2.2.7. Der Schnitt über eine beliebige Familie von Untergruppen einer gegebenen Gruppe ist selbst wieder eine Untergruppe. Für eine Teilmenge T einer Gruppe G definieren wir die **von T erzeugte Untergruppe**

$$\langle T \rangle \subset G$$

als die kleinste Untergruppe von G, die T enthält. Natürlich gibt es so eine kleinste Untergruppe, nämlich den Schnitt über alle Untergruppen von G, die T enthalten. Für $T \neq \emptyset$ können wir $\langle T \rangle$ konkret beschreiben als die Menge aller endlichen Produkte von Elementen aus T und deren Inversen. Für $T = \emptyset$ besteht $\langle T \rangle$ nur aus dem neutralen Element. Ist T durch einen Ausdruck in Mengenklammern gegeben, so lassen wir diese meist weg und schreiben also zum Beispiel kürzer $\langle a_1, \ldots, a_n \rangle$ statt $\langle \{a_1, \ldots, a_n\} \rangle$. Ob der Ausdruck $\langle T \rangle$ in einem speziellen Fall die von einer Menge T erzeugte Untergruppe oder vielmehr die von der einelementigen Menge mit einzigem Element T erzeugte Untergruppe meint, muß der

Leser meist selbst aus dem Kontext erschließen. Schreiben wir jedoch $\langle !T\rangle$, so ist stets zu verstehen, daß T eine Menge von Erzeugern und nicht einen einzelnen Erzeuger meint.

2.2.8. Ist V ein k-Vektorraum und $T \subset V$ eine Teilmenge, so muß der Leser von nun an aus dem Kontext erschließen, ob mit $\langle T\rangle$ die von T erzeugte Untergruppe oder der von T erzeugte Untervektorraum gemeint ist. Zur Unterscheidung schreiben wir manchmal $\langle T\rangle_{\mathbb{Z}}$ für die von T erzeugte Untergruppe und $\langle T\rangle_k$ für den von T erzeugten Untervektorraum.

Lemma 2.2.9. *Das Bild einer Untergruppe unter einem Gruppenhomomorphismus ist stets eine Untergruppe. Das Urbild einer Untergruppe unter einem Gruppenhomomorphismus ist stets eine Untergruppe.*

Beweis. Dem Leser überlassen. □

Definition 2.2.10. Sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Das Urbild der trivialen Untergruppe von H heißt der **Kern** von φ und wird bezeichnet mit

$$\ker \varphi = \{g \in G \mid \varphi(g) = e\}$$

Definition 2.2.11. Das **Bild** $\varphi(G)$ von ganz G unter φ wird nach der englischen und französischen Bezeichnung **image** bezeichnet mit

$$\operatorname{im} \varphi = \{\varphi(g) \mid g \in G\}$$

2.2.12. Nach 2.2.9 sind Kern und Bild eines Gruppenhomomorphismus stets Untergruppen im Definitionsbereich bzw. Wertebereich unseres Gruppenhomomorphismus.

Ergänzende Übung 2.2.13. Sei G eine Gruppe und $\varphi : G \to G$ ein Gruppenhomomorphismus. Man zeige: Gilt für ein $n \in \mathbb{N}$ die Geichheit $\ker \varphi^n = \ker \varphi^{n+1}$, so folgt $\ker \varphi^n = \ker \varphi^{n+1} = \ker \varphi^{n+2} = \ldots$ Hinweis: Man mag I.2.2.15 erinnern.

Lemma 2.2.14. *Ein Gruppenhomomorphismus ist injektiv genau dann, wenn sein Kern trivial ist.*

2.2.15. In 1.6.3 haben wir bereits einen Spezialfall dieses Resultats bewiesen, allerdings in additiver Notation, da es dort um lineare Abbildungen zwischen Vektorräumen ging.

Beweis. Sei $\varphi : G \to H$ unser Gruppenhomomorphismus. Wir argumentieren durch Widerspruch: Besteht $\ker \varphi$ aus mehr als einem Element, so kann φ natürlich nicht injektiv sein. Gibt es umgekehrt $x \neq y$ mit $\varphi(x) = \varphi(y)$, so liegen $x^{-1}y \neq e$ beide in $\ker \varphi$. □

Satz 2.2.16 (Untergruppen von $\mathbb{Z}$). *Jede Untergruppe $H \subset \mathbb{Z}$ ist von der Form $H = m\mathbb{Z}$ für genau ein $m \in \mathbb{N}$.*

Beweis. Im Fall $H = \{0\}$ ist $m = 0$ die einzige natürliche Zahl mit $H = m\mathbb{Z}$. Gilt $H \neq \{0\}$, so enthält H echt positive Elemente. Sei dann $m \in H$ das kleinste echt positive Element von H. Wir behaupten $H = m\mathbb{Z}$. Die Inklusion $H \supset m\mathbb{Z}$ ist hier offensichtlich. Aber gäbe es $n \in H \setminus m\mathbb{Z}$, so könnten wir n mit Rest teilen durch m und also schreiben $n = ms + r$ für geeignete $s, r \in \mathbb{Z}$ mit $0 < r < m$ und hätten $r = n - ms \in H$ im Widerspruch zur Minimalität von m. □

2.3 Primfaktorzerlegung

Definition 2.3.1. Eine **Primzahl** ist eine natürliche Zahl $p > 1$ derart, daß aus $p = ab$ mit $a, b \in \mathbb{N}$ schon folgt $a = 1$ oder $b = 1$.

2.3.2. Eine Möglichkeit, alle Primzahlen zu finden, ist das sogenannte **Sieb des Eratosthenes**: Man beginnt mit der kleinsten Primzahl, der Zwei. Streicht man alle Vielfachen der Zwei, d.h. alle geraden Zahlen, so ist die erste Zahl unter den Übrigen die nächste Primzahl, die Drei. Streicht man nun auch noch alle Vielfachen der Drei, so ist die erste Zahl unter den Übrigen die nächste Primzahl, die Fünf, und so weiter. “Der Erste” heißt auf lateinisch “Primus” und auf griechisch ähnlich und es könnte sein, daß die Bezeichnung “Primzahl” daher rührt.

Satz 2.3.3 (Existenz einer Primfaktorzerlegung). *Jede natürliche Zahl $n \geq 2$ kann als ein Produkt von Primzahlen $n = p_1 p_2 \ldots p_r$ dargestellt werden.*

2.3.4. Der Satz gilt in unserer Terminologie auch für die Zahl $n = 1$, die eben durch das “leere Produkt” mit $r = 0$ dargestellt wird.

Beweis. Das ist klar mit vollständiger Induktion: Ist eine Zahl nicht bereits selbst prim, so kann sie als Produkt echt kleinerer Faktoren geschrieben werden, von denen nach Induktionsannahme bereits bekannt ist, daß sie Primfaktorzerlegungen besitzen. □

Satz 2.3.5. *Es gibt unendlich viele Primzahlen.*

Beweis. Durch Widerspruch. Gäbe es nur endlich viele Primzahlen, so könnten wir deren Produkt betrachten und dazu Eins hinzuzählen. Die so neu entstehende Zahl müßte dann wie jede von Null verschiedene natürliche Zahl nach 2.3.3 eine Primfaktorzerlegung besitzen, aber keine unserer endlich vielen Primzahlen käme als Primfaktor in Frage. □

Ergänzung 2.3.6. Noch offen (2009) ist die Frage, ob es auch unendlich viele **Primzahlzwillinge** gibt, d.h. Paare von Primzahlen mit der Differenz Zwei, wie zum Beispiel $5, 7$ oder $11, 13$ oder $17, 19$. Ebenso offen ist die Frage, ob jede gerade Zahl $n > 2$ die Summe von zwei Primzahlen ist. Diese Vermutung, daß das richtig sein sollte, ist bekannt als **Goldbach-Vermutung**.

Satz 2.3.7 (Eindeutigkeit der Primfaktorzerlegung). *Die Darstellung einer natürlichen Zahl $n \geq 1$ als ein Produkt von Primzahlen $n = p_1 p_2 \ldots p_r$ ist eindeutig bis auf die Reihenfolge der Faktoren. Nehmen wir zusätzlich $p_1 \leq p_2 \leq \ldots \leq p_r$ an, so ist unsere Darstellung mithin eindeutig.*

2.3.8. Dieser Satz ist einer von vielen Gründen, aus denen man bei der Definition des Begriffs einer Primzahl die Eins ausschließt, obwohl das die Definition verlängert: Hätten wir der Eins erlaubt, zu unseren Primzahlen dazuzugehören, so wäre der vorhergehende Satz in dieser Formulierung falsch.

Beweis. Der Beweis dieses Satzes braucht einige Vorbereitungen. Ich bitte Sie, gut aufzupassen, daß wir ihn nicht verwenden, bis er dann nach Lemma 2.3.13 endlich bewiesen werden kann. □

Definition 2.3.9. Seien $a, b \in \mathbb{Z}$. Wir sagen a **teilt** b und schreiben $a|b$ genau dann, wenn es $d \in \mathbb{Z}$ gibt mit $ad = b$. Sind zwei ganze Zahlen a, b nicht beide Null, so gibt es eine größte ganze Zahl c, die sie beide teilt. Diese Zahl heißt der **größte gemeinsame Teiler** von a und b. Zwei ganze Zahlen a und b heißen **teilerfremd** genau dann, wenn ihr größter gemeinsamer Teiler die Eins ist. Insbesondere sind also $a = 0$ und $b = 0$ nicht teilerfremd.

Satz 2.3.10 (über den größten gemeinsamen Teiler). *Sind zwei ganze Zahlen $a, b \in \mathbb{Z}$ nicht beide Null und ist c ihr größter gemeinsamer Teiler, so gilt:*

1. *Der größte gemeinsamen Teiler kann als eine ganzzahlige Linearkombination unserer beiden Zahlen dargestellt werden, es gibt also in Formeln $r, s \in \mathbb{Z}$ mit $c = ra + sb$.*

2. *Teilt $d \in \mathbb{Z}$ sowohl a als auch b, so teilt d auch den größten gemeinsamen Teiler von a und b.*

2.3.11. Der zweite Teil dieses Satzes ist einigermaßen offensichtlich, wenn man die Eindeutigkeit der Primfaktorzerlegung als bekannt voraussetzt. Da wir besagte Eindeutigkeit der Primfaktorzerlegung jedoch erst aus besagtem zweiten Teil ableiten werden, ist es wichtig, auch für den zweiten Teil dieses Satzes einen eigenständigen Beweis zu geben.

Beweis. Man betrachte die Teilmenge $a\mathbb{Z} + b\mathbb{Z} = \{ar + bs \mid r, s \in \mathbb{Z}\} \subset \mathbb{Z}$. Sie ist offensichtlich eine von Null verschiedene Untergruppe von $\mathbb{Z}$. Also ist sie nach 2.2.16 von der Form $a\mathbb{Z} + b\mathbb{Z} = \hat{c}\mathbb{Z}$ für genau ein $\hat{c} > 0$ und es gilt

i. $\hat{c}$ teilt a und b; In der Tat haben wir ja $a, b \in \hat{c}\mathbb{Z}$;

ii. $\hat{c} = ra + sb$ für geeignete $r, s \in \mathbb{Z}$; In der Tat haben wir ja $\hat{c} \in a\mathbb{Z} + b\mathbb{Z}$;

iii. (d teilt a und b) $\Rightarrow$ (d teilt $\hat{c}$);

Daraus folgt aber sofort, daß $\hat{c}$ der größte gemeinsame Teiler von a und b ist, und damit folgt dann der Satz. □

2.3.12. Gegeben $a_1, \ldots, a_n \in \mathbb{Z}$ können wir mit der Notation 2.2.7 kürzer schreiben

$$a_1\mathbb{Z} + \ldots + a_n\mathbb{Z} = \langle a_1, \ldots, a_n \rangle$$

Üblich ist hier auch die Notation $(a_1, \ldots, a_n)$, die jedoch oft auch n-Tupel von ganzen Zahlen bezeichnet, also Elemente von $\mathbb{Z}^n$, und in der Analysis im Fall $n = 2$ meist ein offenes Intervall. Es gilt dann aus dem Kontext zu erschließen, was jeweils gemeint ist. Sind a und b nicht beide Null und ist c ihr größter gemeinsamer Teiler, so haben wir nach dem Vorhergehenden $\langle a, b \rangle = \langle c \rangle$. Wir benutzen von nun an diese Notation. Über die Tintenersparnis hinaus hat sie den Vorteil, auch im Fall $a = b = 0$ sinnvoll zu bleiben.

Lemma 2.3.13. *Teilt eine Primzahl ein Produkt von zwei ganzen Zahlen, so teilt sie einen der Faktoren.*

2.3.14. Wenn wir die Eindeutigkeit der Primfaktorzerlegung als bekannt voraussetzen, so ist dies Lemma offensichtlich. Diese Argumentation hilft aber hier nicht weiter, da sie voraussetzt, was wir gerade erst beweisen wollen. Sicher ist Ihnen die Eindeutigkeit der Primfaktorzerlegung aus der Schule und ihrer Rechenerfahrung wohlvertraut. Um die Schwierigkeit zu sehen, sollten Sie vielleicht selbst einmal versuchen, einen Beweis dafür anzugeben. Im übrigen werden wir in III.2.3.8 sehen, daß etwa im Ring $\mathbb{Z}[\sqrt{-5}]$ das Analogon zur Eindeutigkeit der Primfaktorzerlegung nicht mehr richtig ist.

Beweis. Sei p unsere Primzahl und seien $a, b \in \mathbb{Z}$ gegeben mit $p|ab$. Teilt p nicht a, so folgt für den größten gemeinsamen Teiler $\langle p, a \rangle = \langle 1 \rangle$, denn die Primzahl p hat nur die Teiler ± 1 und $\pm p$. Der größte gemeinsame Teiler von p und a kann aber nicht p sein und muß folglich 1 sein. Nach 2.3.10 gibt es also $r, s \in \mathbb{Z}$ mit $1 = rp + sa$. Es folgt $b = rpb + sab$ und damit $p|b$, denn p teilt natürlich rpb und teilt nach Annahme auch sab. □

Beweis der Eindeutigkeit der Primfaktorzerlegung 2.3.7. Zunächst sei bemerkt, daß aus Lemma 2.3.13 per Induktion dieselbe Aussage auch für Produkte beliebiger Länge folgt: Teilt eine Primzahl ein Produkt, so teilt sie einen der Faktoren. Seien $n = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s$ zwei Primfaktorzerlegungen derselben Zahl $n \geq 1$. Da p_1 unser n teilt, muß es damit eines der q_i teilen. Da auch dies q_i prim ist, folgt $p_1 = q_i$. Wir kürzen den gemeinsamen Primfaktor und sind fertig per Induktion. □

2.3.15. Ich erkläre am Beispiel $a = 160, b = 625$ den sogenannten **euklidischen Algorithmus**, mit dem man den größten gemeinsamen Teiler c zweier positiver natürlicher Zahlen a, b bestimmen kann nebst einer Darstellung $c = ra + rb$. In unseren Gleichungen wird jeweils geteilt mit Rest.

$$\begin{aligned} 160 &= 1\cdot\ 145 \ +\ 15 \\ 145 &= 9\cdot\ 15 \ +\ 10 \\ 15 &= 1\cdot\ 10 \ +\ 5 \\ 10 &= 2\cdot\ 5 \ +\ 0 \end{aligned}$$

Daraus folgt für den größten gemeinsamen Teiler $\langle 625, 160\rangle = \langle 160, 145\rangle = \langle 145, 15\rangle = \langle 15, 10\rangle = \langle 10, 5\rangle = \langle 5, 0\rangle = \langle 5\rangle$. Die vorletzte Zeile liefert eine Darstellung $5 = x \cdot 10 + y \cdot 15$ unseres größten gemeinsamen Teilers $5 = \mathrm{ggT}(10, 15)$ als ganzzahlige Linearkombination von 10 und 15. Die vorvorletzte Zeile eine Darstellung $10 = x' \cdot 15 + y' \cdot 145$ und nach Einsetzen in die vorherige Gleichung eine Darstellung $5 = x(x' \cdot 15 + y' \cdot 145) + y \cdot 15$ unseres größten gemeinsamen Teilers $5 = \mathrm{ggT}(15, 145)$ als ganzzahlige Linearkombination von 15 und 145. Indem wir so induktiv hochsteigen, erhalten wir schließlich für den größten gemeinsamen Teiler die Darstellung $5 = -11 \cdot 625 + 43 \cdot 160$.

Übung 2.3.16. Man berechne den größten gemeinsamen Teiler von 3456 und 436 und eine Darstellung desselben als ganzzahlige Linearkombination unserer beiden Zahlen.

Übung 2.3.17. Gegeben zwei von Null verschiedene natürliche Zahlen a, b nennt man die kleinste von Null verschiedene natürliche Zahl, die sowohl ein Vielfaches von a als auch ein Vielfaches von b ist, das **kleinste gemeinsame Vielfache** von a und b und notiert sie $\mathrm{kgV}(a, b)$. Man zeige in dieser Notation die Formel $\mathrm{kgV}(a, b)\,\mathrm{ggT}(a, b) = ab$.

Ergänzende Übung 2.3.18. Beim sogenannten "Spirographen", einem Zeichenspiel für Kinder, kann man an einem innen mit 105 Zähnen versehenen Ring ein Zahnrad mit 24 Zähnen entlanglaufen lassen. Steckt man dabei einen Stift durch ein Loch außerhalb des Zentrums des Zahnrads, so entstehen dabei die köstlichsten Figuren. Wie oft muß man das Zahnrad auf dem inneren Zahnkranz umlaufen, bevor solch eine Figur fertig gemalt ist?

Der Spirograph aus Übung 2.3.18

Ergänzende Übung 2.3.19. Berechnen Sie, wieviele verschiedene Strophen das schöne Lied hat, dessen erste Strophe lautet:

Tomatensalat Tomatensalatooo-
-matensalat Tomatensaaaaaaaa-
-lat Tomatensalat Tomatensalat
Tomatensalat Tomatensaaaaaaa-

2.4 Ringe

Definition 2.4.1. Ein **Ring**, französisch **anneau**, ist eine Menge mit zwei Verknüpfungen $(R, +, \cdot)$ derart, daß gilt

1. $(R, +)$ ist eine kommutative Gruppe;
2. $(R, \cdot)$ ist ein Monoid; ausgeschrieben heißt das, daß auch die zweite Verknüpfung ist assoziativ und daß es ein Element $1 = 1_R \in R$ gibt, das **Eins-Element** oder kurz die **Eins** unseres Rings, mit der Eigenschaft $1 \cdot a = a \cdot 1 = a \quad \forall a \in R$.
3. Es gelten die Distributivgesetze, d.h. für alle $a, b, c \in R$ gilt

$$\begin{aligned} a \cdot (b + c) &= (a \cdot b) + (a \cdot c) \\ (a + b) \cdot c &= (a \cdot c) + (b \cdot c) \end{aligned}$$

Die beiden Verknüpfungen heißen die **Addition** und die **Multiplikation** in unserem Ring. Das Element $1 \in R$ aus unserer Definition ist wohlbestimmt als das neutrale Element des Monoids $(R, \cdot)$, vergleiche I.3.1.13. Ein Ring, dessen Multiplikation kommutativ ist, heißt ein **kommutativer Ring** und bei uns in unüblicher Verkürzung ein **Kring**.

2.4.2. Wir schreiben meist kürzer $a \cdot b = ab$ und vereinbaren die Regel "Punkt vor Strich", so daß zum Beispiel das erste Distributivgesetz auch in der Form $a(b + c) = ab + ac$ geschrieben werden kann.

Ergänzung 2.4.3. Der Begriff "Ring" soll zum Ausdruck bringen, daß diese Struktur nicht in demselben Maße "geschlossen" ist wie ein Körper, da wir nämlich nicht die Existenz von multiplikativen Inversen fordern. Er wird auch im juristischen Sinne für gewisse Arten weniger geschlossenener Körperschaften verwendet. So gibt es etwa den "Ring deutscher Makler" oder den "Ring deutscher Bergingenieure". Eine Struktur wie in der vorhergehenden Definition, bei der nur die Existenz eines Einselements nicht gefordert wird, bezeichnen wir als **Rng**. In der Literatur wird jedoch auch diese Struktur oft als "Ring" bezeichnet, leider sogar bei der von mir hochgeschätzten Quelle Bourbaki. Die Ringe, die eine Eins besitzen, heißen in dieser Terminologie "unitäre Ringe".

Beispiele 2.4.4. Die einelementige Menge mit der offensichtlichen Addition und Multiplikation ist ein Ring, der **Nullring**. Jeder Körper ist ein Ring. Die ganzen Zahlen $\mathbb{Z}$ bilden einen Ring. Ist R ein Ring und X eine Menge, so ist die Menge $\mathrm{Ens}(X, R)$ aller Abbildungen von X nach R ein Ring unter punktweiser Multiplikation und Addition. Ist R ein Ring und $n \in \mathbb{N}$, so bilden die $(n \times n)$-Matrizen mit Einträgen in R einen Ring $\mathrm{M}(n \times n; R)$ unter der üblichen Addition und Multiplikation von Matrizen; im Fall $n = 0$ erhalten wir den Nullring, im Fall $n = 1$ ergibt sich R selbst. Ist A eine abelsche Gruppe, so bilden die Gruppenhomomorphismen von A in sich selbst, die sogenannten **Endomorphismen** von A, einen Ring mit der Verknüpfung von Abbildungen als Multiplikation und der punktweisen Summe als Addition. Man notiert diesen Ring

$$\mathrm{End}\, A$$

und nennt ihn den **Endomorphismenring der abelschen Gruppe** A. Ähnlich bilden auch die Endomorphismen eines Vektorraums V über einem Körper k einen Ring $\mathrm{End}_k V$, den sogenannten **Endomorphismenring von** V. Oft notiert man auch den Endomorphismenring eines Vektorraums abkürzend $\mathrm{End}\, V$ in der Hoffnung, daß aus dem Kontext klar wird, daß die Endomorphismen von V als Vektorraum gemeint sind und nicht die Endomorphismen der V zugrundeliegenden abelschen Gruppe. Will man besonders betonen, daß die Endomorphismen als Gruppe gemeint sind, so schreibt man manchmal auch $\mathrm{End}_{\mathbb{Z}} A$ aus Gründen, die erst in IV.1.3.2 erklärt werden. Ich verwende für diesen Ring zur Vermeidung von Indizes lieber die Notation $\mathrm{End}_{\mathbb{Z}} A = \mathrm{Ab}\, A$, die sich aus den allgemeinen kategorientheoretischen Konventionen 10.1.7 und 10.1 ergibt.

Ergänzende Übung 2.4.5. Auf der abelschen Gruppe $\mathbb{Z}$ gibt es genau zwei Verknüpfungen, die als Multiplikation genommen die Addition zu einer Ringstruktur ergänzen.

2.4.6. Allgemeiner als in 1.6.5 erklärt heißt ein Element a eines beliebigen Rnges **idempotent** genau dann, wenn gilt $a^2 = a$. Allgemeiner als in 1.10.12 erklärt heißt ein Element a eines beliebigen Rnges **nilpotent** genau dann, wenn es $d \in \mathbb{N}$ gibt mit $a^d = 0$.

Beispiel 2.4.7. Gegeben eine ganze Zahl $m \in \mathbb{Z}$ konstruieren wir den **Restklassenring** $\mathbb{Z}/m\mathbb{Z}$ wie folgt: Seine Elemente sind diejenigen Teilmengen T von $\mathbb{Z}$, die in der Form $T = a + m\mathbb{Z}$ mit $a \in \mathbb{Z}$ dargestellt werden können. Die Teilmenge $a + m\mathbb{Z}$ heißt auch die **Restklasse von** a **modulo** m, da zumindest im Fall $a \geq 0$ ihre nichtnegativen Elemente genau alle natürlichen Zahlen sind, die beim Teilen durch m denselben Rest lassen wie a. Wir notieren diese Restklasse auch $\bar{a}$. Natürlich ist $\bar{a} = \bar{b}$ gleichbedeutend zu $a - b \in m\mathbb{Z}$. Gehören a und b zur selben Restklasse, in Formeln $a + m\mathbb{Z} = b + m\mathbb{Z}$, so nennen wir sie **kongruent modulo**

m und schreiben

$$a \equiv b \pmod{m}$$

Offensichtlich gibt es für $m \in \mathbb{N}_{\geq 1}$ genau m Restklassen modulo m, in Formeln $|\mathbb{Z}/m\mathbb{Z}| = m$, und wir haben genauer

$$\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$$

Für alle $m \in \mathbb{Z}$ bilden die Restklassen ein Mengensystem $\mathbb{Z}/m\mathbb{Z} \subset \mathcal{P}(\mathbb{Z})$, das stabil ist unter der von der Addition auf $\mathbb{Z}$ im Sinne von I.3.1.2 6 induzierten Verknüpfung. Mit dieser Verknüpfung gilt $\bar{a} + \bar{b} = \overline{a+b} \quad \forall a, b \in \mathbb{Z}$ und $\mathbb{Z}/m\mathbb{Z}$ wird eine abelsche Gruppe. Diese Gruppe wird sogar zu einem Ring vermittels der Multiplikation

$$T \odot S = T \cdot S + m\mathbb{Z} = \{ab + mr \mid a \in T, b \in S, r \in \mathbb{Z}\}$$

In der Tat prüft man für die so erklärte Multiplikation mühelos die Formeln

$$\bar{a} \odot \bar{b} = \overline{ab}$$

und damit folgen die Distributivgesetze für $\mathbb{Z}/m\mathbb{Z}$ unmittelbar aus den Distributivgesetzen im Ring $\mathbb{Z}$. Wir geben wir die komische Notation $\odot$ nun auch gleich wieder auf und schreiben stattdessen $\bar{a} \cdot \bar{b}$ oder noch kürzer $\bar{a}\bar{b}$.

Beispiel 2.4.8. Modulo $m = 2$ gibt es genau zwei Restklassen: Die Elemente der Restklasse von 0 bezeichnet man üblicherweise als **gerade Zahlen**, die Elemente der Restklasse von 1 als **ungerade Zahlen**. Der Ring $\mathbb{Z}/2\mathbb{Z}$ mit diesen beiden Elementen $\bar{0}$ und $\bar{1}$ ist offensichtlich sogar ein Körper.

Beispiel 2.4.9. Den Ring $\mathbb{Z}/12\mathbb{Z}$ könnte man als "Ring von Uhrzeiten" ansehen. Er hat die zwölf Elemente $\{\bar{0}, \bar{1}, \ldots, \overline{11}\}$ und wir haben $\overline{11} + \bar{5} = \overline{16} = \bar{4}$ alias "5 Stunden nach 11 Uhr ist es 4 Uhr." Weiter haben wir in $\mathbb{Z}/12\mathbb{Z}$ etwa auch $\bar{3} \cdot \bar{8} = \overline{24} = \bar{0}$. In einem Ring kann es also durchaus passieren, daß ein Produkt von zwei von Null verschiedenen Faktoren Null ist.

Proposition 2.4.10 (Teilbarkeitskriterien über Quersummen). *Eine natürliche Zahl ist genau dann durch drei bzw. durch neun teilbar, wenn ihre Quersumme durch drei bzw. durch neun teilbar ist.*

Beweis. Wir erklären das Argument nur an einem Beispiel. Per definitionem gilt

$$1258 = 1 \cdot 10^3 + 2 \cdot 10^2 + 5 \cdot 10 + 8$$

Offensichtlich folgt

$$1258 \equiv 1 \cdot 10^3 + 2 \cdot 10^2 + 5 \cdot 10 + 8 \pmod{3}$$

Da 10 kongruent ist zu 1 modulo 3 erhalten wir daraus

$$1258 \equiv 1 + 2 + 5 + 8 \pmod 3$$

Insbesondere ist die rechte Seite durch drei teilbar genau dann, wenn die linke Seite durch drei teilbar ist. Das Argument für neun statt drei geht genauso. □

Ergänzende Übung 2.4.11. Wieviele Untergruppen hat die abelsche Gruppe $\mathbb{Z}/4\mathbb{Z}$? Wieviele Untergruppen hat die abelsche Gruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$?

Ergänzende Übung 2.4.12. Eine natürliche Zahl ist durch 11 teilbar genau dann, wenn ihre "alternierende Quersumme" durch 11 teilbar ist.

Ergänzende Übung 2.4.13. Eine natürliche Zahl, die kongruent zu sieben ist modulo acht, kann nicht eine Summe von drei Quadraten sein.

Ergänzende Übung 2.4.14. Eine Zahl mit einer Dezimaldarstellung der Gestalt $abcabc$ wie zum Beispiel 349349 ist stets durch 7 teilbar.

2.4.15. In $\mathbb{Z}/12\mathbb{Z}$ gilt zum Beispiel $\bar{3} \cdot \bar{5} = \bar{3} \cdot \bar{1}$. In allgemeinen Ringen dürfen wir also nicht kürzen. Dies Phänomen werden wir nun begrifflich fassen.

Definition 2.4.16.

1. Gegeben ein Kring R und Elemente $a, b \in R$ sagen wir, a **teilt** b oder auch a ist ein **Teiler** von b und schreiben $a|b$ genau dann, wenn es $d \in R$ gibt mit $ad = b$.

2. Natürlich teilt jedes Element eines Krings die Null. Ein Element a eines Rings R heißt ein **Nullteiler** von R genau dann, wenn es die Null "in nichttrivialer Weise teilt", wenn es genauer und in Formeln $d \in R\backslash 0$ gibt mit $ad = 0$ oder $da = 0$.

3. Ein Ring heißt **nullteilerfrei** genau dann, wenn er außer der Null keine Nullteiler besitzt, wenn also das Produkt von je zwei von Null verschiedenen Elementen auch wieder von Null verschieden ist.

4. Ein Ring heißt ein **Integritätsbereich** genau dann, wenn er nullteilerfrei und ausserdem nicht der Nullring ist.

2.4.17. Manche Autoren fordern von nullteilerfreien Ringen zusätzlich, daß sie nicht der Nullring sein dürfen, benutzen also dieses Wort als Synonym für "Integritätsbereich".

Übung 2.4.18. Man bestimme alle Nullteiler im Restklassenring $\mathbb{Z}/12\mathbb{Z}$.

2.4.19 (**Kürzen in Ringen**). Sei R ein Ring. Ist $a \in R$ kein Nullteiler, so folgt aus $ax = ay$ schon $x = y$. In der Tat haben wir nämlich $ax = ay \Rightarrow a(x - y) = 0 \Rightarrow x - y = 0 \Rightarrow x = y$.

Definition 2.4.20. Eine Abbildung $\varphi : R \to S$ von einem Ring in einen weiteren Ring heißt ein **Ringhomomorphismus** genau dann, wenn gilt $\varphi(1) = 1$ und $\varphi(a+b) = \varphi(a) + \varphi(b)$ sowie $\varphi(ab) = \varphi(a)\varphi(b)$ für alle $a, b \in R$. In anderen Worten ist ein Ringhomomorphismus also eine Abbildung, die sowohl für die Addition als auch für die Multiplikation ein Monoidhomomorphismus ist.

Ergänzende Übung 2.4.21. Gegeben eine abelsche Gruppe V und ein Körper k induziert die kanonische Identifikation $\mathrm{Ens}(k \times V, V) \xrightarrow{\sim} \mathrm{Ens}(k, \mathrm{Ens}(V, V))$ aus I.2.2.26 eine Bijektion

$$\left\{ \begin{array}{c} \text{Strukturen als } k\text{-Vektorraum} \\ \text{auf der abelschen Gruppe } V \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{c} \text{Ringhomomorphismen} \\ k \to \mathrm{Ab}\, V \end{array} \right\}$$

Wir verwenden hier unsere alternative Notation $\mathrm{Ab}\, V$ für den Endomorphismenring der abelschen Gruppe V, um jede Verwechslung mit dem Endomorphismenring als Vektorraum auszuschließen.

2.4.22. Von Homomorphismen zwischen Rngen können wir natürlich nicht fordern, daß sie das Einselement auf das Einselement abbilden. Wir sprechen dann von **Rnghomomorphismen**. In der Terminologie, in der unsere Rnge als Ringe bezeichnet werden, werden unsere Ringhomomorphismen "unitäre Ringhomomorphismen" genannt.

Übung 2.4.23. Für jeden Ring R gibt es genau einen Ringhomomorphismus $\mathbb{Z} \to R$. Im Fall $R = \mathbb{Z}/m\mathbb{Z}$ wird dieser Ringhomomorphismus gegeben durch die Vorschrift $n \mapsto \bar{n}$. Im allgemeinen notieren wir ihn manchmal $n \mapsto n_R$ und meist $n \mapsto n$. Hinweis: Man erinnere I.3.3.12.

2.4.24. Ich will kurz diskutieren, warum es ungefährlich ist, das Bild einer ganzen Zahl $n \in \mathbb{Z}$ in einem Ring R unter dem einzigen Ringhomomorphismus $\mathbb{Z} \to R$ kurzerhand mit $n_R = n$ zu bezeichnen. Gegeben ein Ring R und $r \in R$ und $n \in \mathbb{Z}$ gilt nämlich stets $nr = n_R r = r n_R$, wobei nr in Bezug auf die Struktur von R als additive abelsche Gruppe verstehen, also $nr = r + r \ldots + r$ mit n Summanden falls $n \geq 1$ und so weiter, wie in der Tabelle I.3.2.11 und in I.3.2.9 ausgeführt wird. Unsere Gleichung $nr = n_R r = r n_R$ bedeutet dann hinwiederum, daß es auf den Unterschied zwischen n_R und n meist gar nicht ankommt. Deshalb führt es auch selten zu Mißvertändnissen, wenn wir statt n_R nur kurz n schreiben.

Definition 2.4.25. Ein Element a eines Rings R heißt **invertierbar** oder genauer **invertierbar in** R oder auch eine **Einheit von** R genau dann, wenn es bezüglich der Multiplikation invertierbar ist im Sinne von I.3.2.2, wenn es also $b \in R$ gibt mit $ab = ba = 1$. Die Menge der invertierbaren Elemente eines Rings bildet unter der Multiplikation eine Gruppe, die man die **Gruppe der Einheiten von** R nennt und gemäß unserer allgemeinen Konventionen I.3.2.11 mit $R^\times$ bezeichnet. Zwei

Elemente eines Rings oder allgemeiner die Elemente einer beliebigen Teilmenge eines Rings heißen **teilerfremd** genau dann, wenn sie außer Einheiten keine gemeinsamen Teiler haben.

Beispiel 2.4.26. Der Ring der ganzen Zahlen $\mathbb{Z}$ hat genau zwei Einheiten, nämlich 1 und (-1). In Formeln haben wir also $\mathbb{Z}^\times = \{1, -1\}$. Dahingegen sind die Einheiten im Ring der rationalen Zahlen $\mathbb{Q}$ genau alle von Null verschiedenen Elemente, in Formeln $\mathbb{Q}^\times = \mathbb{Q}\backslash 0$.

Bemerkung 2.4.27. A priori meint eine Einheit in der Physik das, was ein Mathematiker eine Basis eines eindimensionalen Vektorraums nennen würde. So wäre etwa die Sekunde s eine Basis des reellen Vektorraums $\vec{\mathbb{T}}$ aller Zeitspannen aus 1.7.9. In Formeln ausgedrückt bedeutet das gerade, daß das Daranmultiplizieren von s eine Bijektion $\mathbb{R} \xrightarrow{\sim} \vec{\mathbb{T}}$ liefert. Mit den Einheiten eines kommutativen Ringes R verhält es sich nun genauso: Genau dann ist $u \in R$ eine Einheit, wenn das Daranmultiplizieren von u eine Bijektion $R \xrightarrow{\sim} R$ liefert. Daher rührt dann wohl auch die Terminologie.

2.4.28. Ein Körper ist in dieser Terminologie ein kommutativer Ring, der nicht der Nullring ist und in dem jedes von Null verschiedene Element eine Einheit ist.

Übung 2.4.29. Jeder Ringhomomorphismus macht Einheiten zu Einheiten. Jeder Ringhomomorphismus von einem Körper in einen vom Nullring verschiedenen Ring ist injektiv.

Übung 2.4.30. Ein Nullteiler kann nur im Nullring eine Einheit sein.

Proposition 2.4.31 (Endliche Primkörper). *Sei $m \in \mathbb{N}$.*

1. *Genau dann ist der Restklassenring $\mathbb{Z}/m\mathbb{Z}$ ein Integritätsbereich, wenn m eine Primzahl ist oder wenn gilt $m = 0$.*

2. *Genau dann ist $\mathbb{Z}/m\mathbb{Z}$ ein Körper, wenn m eine Primzahl ist.*

2.4.32. Die Körper $\mathbb{Z}/p\mathbb{Z}$ für Primzahlen p sowie der Körper $\mathbb{Q}$ sind die "kleinstmöglichen Körper" in einem Sinne, der in III.3.1.6 präzisiert wird. Man nennt diese Körper deshalb auch **Primkörper**. Die endlichen Primkörper werden meist $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ notiert, mit einem $\mathbb{F}$ für "field" oder "finite". Die Notation $\mathbb{F}_q$ verwendet man allerdings auch allgemeiner mit einer Primzahlpotenz q im Index als Bezeichnung für "den endlichen Körper mit q Elementen", den wir erst in III.3.4.1 kennenlernen werden, und der weder als Ring noch als abelsche Gruppe isomorph ist zu $\mathbb{Z}/q\mathbb{Z}$.

Beweis. 1. Für $m = 0$ ist $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}$ offensichtlich ein Integritätsbereich. Für m eine Primzahl ist $\mathbb{Z}/m\mathbb{Z}$ ein Integritätsbereich, da eine Primzahl nach 2.3.13 nur dann ein Produkt teilen kann, wenn sie bereits einen der Faktoren teilt. Für

$m = 1$ ist $\mathbb{Z}/m\mathbb{Z}$ der Nullring und damit kein Integritätsbereich. Für $m > 1$ keine Primzahl faktorisieren wir $m = ab$ mit $1 < a, b < m$ und erhalten $0 = \bar{a}\bar{b}$ aber $\bar{a} \neq 0, \bar{b} \neq 0$. Mithin hat dann $\mathbb{Z}/m\mathbb{Z}$ von Null verschiedene Nullteiler, und diese können offensichtlich keine Einheiten sein.

2. Es muß nur noch gezeigt werden, daß für jede Primzahl p der Ring $\mathbb{Z}/p\mathbb{Z}$ ein Körper ist, daß also jedes von Null verschiedene Element $a \neq 0$ ein multiplikatives Inverses besitzt. Da $\mathbb{Z}/p\mathbb{Z}$ nullteilerfrei ist, muß jedoch die Multiplikation mit jedem Element $a \neq 0$ injektiv und damit bijektiv sein, also gibt es zu jedem $a \neq 0$ ein $b \in \mathbb{Z}/p\mathbb{Z}$ mit $ab = 1$. □

Übung 2.4.33. Man finde das multiplikative Inverse der Nebenklasse von 22 im Körper $\mathbb{F}_{31}$. Hinweis: Euklidischer Algorithmus.

Übung 2.4.34. Man konstruiere einen Körper mit 49 Elementen und einen Körper mit 25 Elementen. Hinweis: I.3.3.14 und I.3.3.15.

Ergänzung 2.4.35. Ich will versuchen, das **Verfahren von Diffie-Hellman** zum öffentlichen Vereinbaren geheimer Schlüssel anhand des folgenden Schemas zu erklären.

Geheimbereich Alice	Öffentlicher Bereich	Geheimbereich Bob
	Bekanntgemacht wird eine Gruppe G und ein Element $g \in G$.	
Alice wählt $a \in \mathbb{N}$, berechnet g^a und macht es öffentlich.		Bob wählt $b \in \mathbb{N}$, berechnet g^b und macht es öffentlich.
	g^a, g^b	
Nach dem öffentlichen Austausch berechnet Alice $(g^b)^a = g^{ba} = g^{ab}$.		Nach dem öffentlichen Austauch berechnet Bob $(g^a)^b = g^{ab} = g^{ba}$.

Das Gruppenelement $g^{ba} = g^{ab}$ ist dann der gemeinsame hoffentlich geheime Schlüssel. Der Trick hierbei besteht darin, geeignete Paare (G, g) und geeignete Zahlen a so zu finden, daß die Berechnung von g^a unproblematisch ist, daß jedoch kein schneller Algorithmus bekannt ist, der aus der Kenntnis von G, g und g^a ein mögliches a bestimmt, der also, wie man auch sagt, einen **diskreten Logarithmus von** g^a **zur Basis** g findet. Dann kann Alice g^a veröffentlichen und dennoch a geheim halten und ebenso kann Bob g^b veröffentlichen und dennoch b geheim halten. Zum Beispiel kann man für G die Einheitengruppe $G = (\mathbb{Z}/p\mathbb{Z})^\times$ des Primkörpers zu einer großen Primzahl p nehmen. Nun ist es natürlich denkbar, daß man aus der Kenntnis von g^a und g^b direkt g^{ab} berechnen kann, ohne zuvor a zu be-

stimmen, aber auch für die Lösung dieses sogenannten **Diffie-Hellman-Problems** ist in diesem Fall kein schneller Algorithmus bekannt. Mit den derzeitig verfügbaren Rechenmaschinen können also Alice und Bob mit einer Rechenzeit von unter einer Minute einen geheimen Schlüssel vereinbaren, dessen Entschlüsselung auf derselben Maschine beim gegenwärtigen Stand der veröffentlichten Forschung Millionen von Jahren bräuchte. Allerdings ist auch wieder nicht bewiesen, daß es in diesem Fall nicht doch einen effizienten Algorithmus zur Lösung des Diffie-Hellman-Problems gibt.

Ergänzung 2.4.36. Statt mit der Einheitengruppe endlicher Körper arbeitet man in der Praxis auch oft mit sogenannten "elliptischen Kurven", als da heißt, Lösungsmengen kubischer Gleichungen, deren Gruppengesetz sie in einer Vorlesung über algebraische Geometrie kennenlernen können.

Definition 2.4.37. Gegeben ein Ring R gibt es nach 2.4.23 genau einen Ringhomomorphismus $\mathbb{Z} \to R$. Dessen Kern ist nach 2.2.9 eine Untergruppe von $\mathbb{Z}$ und hat nach 2.2.16 folglich die Gestalt $m\mathbb{Z}$ für genau ein $m \in \mathbb{N}$. Diese natürliche Zahl m nennt man die **Charakteristik des Rings** R und notiert sie $m = \operatorname{char} R$. Wir haben also etwa $\operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{R} = \operatorname{char} \mathbb{C} = 0$ und $\operatorname{char}(\mathbb{Z}/p\mathbb{Z}) = p$.

2.4.38. Es ist leicht zu sehen, daß die Charakteristik eines Körpers, wenn sie nicht Null ist, stets eine Primzahl sein muß: Hätten wir sonst einen Körper der Charakteristik $m = ab > 0$ mit natürlichen Zahlen $a < m$ und $b < m$, so wären die Bilder von a und b in unserem Körper k von Null verschiedene Elemente mit Produkt Null. Widerspruch!

Ergänzende Übung 2.4.39. Sei R ein kommutativer Ring, dessen Charakteristik eine Primzahl p ist, für den es also einen Ringhomomorphismus $\mathbb{Z}/p\mathbb{Z} \to R$ gibt. Man zeige, daß dann der sogenannte **Frobenius-Homomorphismus** $F : R \to R$, $a \mapsto a^p$ ein Ringhomomorphismus von R in sich selber ist. Hinweis: Man verwende, daß die binomische Formel I.3.3.4 offensichtlich in jedem kommutativen Ring gilt, ja sogar für je zwei Elemente a, b eines beliebigen Rings mit $ab = ba$.

Übung 2.4.40. Sei p eine Primzahl. Eine abelsche Gruppe G kann genau dann mit der Struktur eines $\mathbb{F}_p$-Vektorraums versehen werden, wenn in additiver Notation gilt $pg = 0$ für alle $g \in G$, und die fragliche Vektorraumstruktur ist dann durch die Gruppenstruktur eindeutig bestimmt.

Ergänzende Übung 2.4.41. Wieviele Untervektorräume hat ein zweidimensionaler Vektorraum über einem Körper mit fünf Elementen? Wieviele angeordnete Basen?

Ergänzende Übung 2.4.42. Gegeben ein Vektorraum über einem endlichen Primkörper sind seine Untervektorräume genau die Untergruppen der zugrundeliegenden abelschen Gruppe.

Ergänzende Übung 2.4.43. Man zeige: In jedem endlichen Körper ist das Produkt aller von Null verschiedenen Elemente (-1). Hinweis: Man zeige zunächst, daß nur die Elemente ± 1 ihre eigenen Inversen sind. Als Spezialfall erhält man $(p-1)! \equiv -1 \pmod p$ für jede Primzahl p. Diese Aussage wird manchmal auch als **Satz von Wilson** zitiert.

Ergänzung 2.4.44. Sei $m \geq 1$ eine natürliche Zahl. Eine Restklasse modulo m heißt eine **prime Restklasse** genau dann, wenn sie aus zu m teilerfremden Zahlen besteht. Wir zeigen in **??**, daß es in jeder primen Restklasse unendlich viele Primzahlen gibt. Im Fall $m = 10$ bedeutet das zum Beispiel, daß es jeweils unendlich viele Primzahlen gibt, deren Dezimaldarstellung mit einer der Ziffern $1, 3, 7$ und 9 endet.

Übung 2.4.45. Gegeben $m \geq 1$ sind die Einheiten des Restklassenrings $\mathbb{Z}/m\mathbb{Z}$ genau die Restklassen derjenigen Zahlen a mit $0 \leq a < m$, die zu m teilerfremd sind, in anderen Worten die primen Restklassen. In Formeln haben wir also $(\mathbb{Z}/m\mathbb{Z})^\times = \{\bar{a} \mid 0 \leq a < m,\ \langle m, a\rangle = \langle 1\rangle\}$. Hinweis: 2.3.10.

2.5 Polynome

2.5.1. Ist k ein Ring, so bildet die Menge $k[X]$ aller "formalen Ausdrücke" der Gestalt $a_n X^n + \ldots + a_1 X + a_0$ mit $a_i \in k$ unter der offensichtlichen Addition und Multiplikation einen Ring, den **Polynomring** über k in einer Veränderlichen X, und wir haben eine offensichtliche Einbettung $\mathrm{can} : k \hookrightarrow k[X]$. Die Herkunft der Bezeichnung diskutieren wir in **??**. Die a_ν heißen in diesem Zusammenhang die **Koeffizienten** unseres Polynoms, genauer heißt a_ν der **Koeffizient von** X^ν. Das X heißt die **Variable** unseres Polynoms und kann auch schon mal mit einem anderen Buchstaben bezeichnet werden: Besonders gebräuchlich sind hierbei Großbuchstaben vom Ende des Alphabets. Unsere Beschreibung ist hoffentlich verständlich, sie ist aber nicht so exakt, wie eine Definition es sein sollte. Deshalb geben wir auch noch eine exakte Variante.

Definition 2.5.2. Sei k ein Ring. Wir bezeichnen mit $k[X]$ die Menge aller Abbildungen $\varphi : \mathbb{N} \to k$, die nur an endlich vielen Stellen von Null verschiedene Werte annehmen, und definieren auf $k[X]$ eine Addition und eine Multiplikation durch die Regeln

$$\begin{aligned}(\varphi + \psi)(n) &= \varphi(n) + \psi(n)\\ (\varphi \cdot \psi)(n) &= \textstyle\sum_{i+j=n} \varphi(i)\psi(j)\end{aligned}$$

Mit diesen Verknüpfungen wird $k[X]$ ein Ring, und ordnen wir jedem $a \in k$ die Abbildung $\mathbb{N} \to k$ zu, die bei 0 den Wert a annimmt und sonst den Wert Null, so erhalten wir eine Einbettung $\mathrm{can} : k \hookrightarrow k[X]$, die wir schlicht $a \mapsto a$ notieren. Bezeichnen wir mit X die Abbildung $\mathbb{N} \to k$, die bei 1 den Wert 1 annimmt

und sonst nur den Wert Null, so können wir jede Abbildung $\varphi \in k[X]$ eindeutig schreiben in der Form $\varphi = \sum_\nu \varphi(\nu) X^\nu$ und sind auf einem etwas formaleren Weg wieder am selben Punkt angelangt.

2.5.3. Die wichtigste Eigenschaft eines Polynomrings ist, daß man "für die Variable etwas einsetzen darf". Das wollen wir nun formal korrekt aufschreiben. Wir sagen, zwei Elemente a und b eines Rings **kommutieren** genau dann, wenn gilt $ab = ba$.

Proposition 2.5.4 (Einsetzen in Polynome). *Seien k und R Ringe, $i : k \to R$ ein Ringhomomorphismus und $b \in R$ ein Element, das mit jedem Element $a \in i(k)$ kommutiert. So gibt es genau eine Erweiterung $\tilde{\imath} = \tilde{\imath}_b$ von i zu einem Ringhomomorphismus $\tilde{\imath} : k[X] \to R$ mit $\tilde{\imath}(X) = b$ alias ganz formal: Genau einen Ringhomomorphismus $\tilde{\imath} : k[X] \to R$ mit $\tilde{\imath}(X) = b$ und $\tilde{\imath} \circ \mathrm{can} = i$.*

Beweis. Diese eindeutig bestimmte Abbildung $\tilde{\imath}$ ist eben gegeben durch die Vorschrift $\tilde{\imath}(a_n X^n + \ldots + a_1 X + a_0) = i(a_n)b^n + \ldots + i(a_1)b + i(a_0)$. □

2.5.5. Es ist üblich, das Bild unter $\tilde{\imath}_b$ eines Polynoms $P \in k[X]$ abzukürzen als $P(b) := \tilde{\imath}_b(P)$. So schreiben wir im Fall eines kommutativen Rings k zum Beispiel $P(A)$ für die Matrix, die ensteht beim Einsetzen einer quadratischen Matrix A in das Polynom P. In diesem Fall hätten wir $R = \mathrm{M}(n \times n; k)$ und i wäre der Ringhomomorphismus, die jedem $a \in k$ das a-fache der Einheitsmatrix zuordnet.

2.5.6. Ist speziell $\varphi : k \to S$ ein Ringhomomorphismus, so erhalten wir einen Homomorphismus $k[X] \to S[X]$ der zugehörigen Polynomringe durch das "Anwenden von φ auf die Koeffizienten" oder formal im Sinne unserer Proposition das "Einsetzen von X für X".

Übung 2.5.7. Welche Matrix entsteht beim Einsetzen der quadratischen Matrix $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ in das Polynom $X^2 + 1$?

Definition 2.5.8. Sei k ein Kring und $P \in k[X]$ ein Polynom. Ein Element $a \in k$ heißt eine **Nullstelle** oder auch eine **Wurzel** von P genau dann, wenn gilt $P(a) = 0$.

Ergänzende Übung 2.5.9. Man zeige, daß jede Nullstelle $\alpha \in \mathbb{C}$ eines normierten Polynoms mit komplexen Koeffizienten $X^n + a_{n-1}X^{n-1} + \ldots + a_0$ die Abschätzung $|\alpha| \leq 1 + |a_{n-1}| + \ldots + |a_0|$ erfüllt. Umgekehrt zeige man auch, daß aus der Abschätzung $|\alpha| \leq C$ für alle komplexen Wurzeln die Abschätzung $|a_k| \leq \binom{n}{k} C^{n-k}$ für die Koeffizienten folgt.

Übung 2.5.10. Ist $P \in \mathbb{R}[X]$ ein Polynom mit reellen Koeffizienten und $\mu \in \mathbb{C}$ eine komplexe Zahl, so gilt $P(\mu) = 0 \Rightarrow P(\bar{\mu}) = 0$. Ist also eine komplexe Zahl Nullstelle eines Polynoms mit reellen Koeffizienten, so ist auch die konjugiert komplexe Zahl eine Nullstelle desselben Polynoms.

Die komplexen Nullstellen eines Polynoms mit reellen Koeffizienten, die nicht reell sind, tauchen immer in Paaren aus einer Wurzel und ihrer komplex Konjugierten auf, vergleiche auch Übung 2.5.10.

Ergänzende Übung 2.5.11. Sei $i : k \to K$ ein Ringomomorphismus kommutativer Ringe und bezeichne $i : k[X] \to K[X]$ auch den induzierten Ringhomomorphismus zwischen den zugehörigen Polynomringen. Man zeige: Ist und $\lambda \in k$ eine Nullstelle eines Polynoms $P \in k[X]$, so ist $i(\lambda) \in K$ eine Nullstelle des Polynoms $i(P)$.

Definition 2.5.12. Sei k ein Ring. Jedem Polynom $P \in k[X]$ ordnen wir seinen **Grad** (engl. degree, franz. degré) $\operatorname{grad} P \in \mathbb{N} \cup \{-\infty\}$ zu durch die Vorschrift

$$\begin{array}{ll} \operatorname{grad} P = n & \text{falls } P = a_n X^n + \ldots + a_0 \text{ mit } a_n \neq 0; \\ \operatorname{grad} P = -\infty & \text{für } P \text{ das Nullpolynom.} \end{array}$$

Für ein von Null verschiedenes Polynom $P = a_n X^n + \ldots + a_1 X + a_0$ mit $n = \operatorname{grad} P$ nennt man $a_n \in k\backslash 0$ seinen **Leitkoeffizienten**. Den Leitkoeffizienten des Nullpolynoms definieren wir als die Null von k. Ein Polynom heißt **normiert** genau dann, wenn sein Leitkoeffizient 1 ist. Das Nullpolynom ist demnach nur über dem Nullring normiert. Ein Polynom vom Grad Eins heißt **linear**, ein Polynom vom Grad Zwei **quadratisch**, ein Polynom vom Grad Drei **kubisch**.

Lemma 2.5.13 (Grad eines Produkts). *Ist k ein nullteilerfreier Ring, so ist auch der Polynomring $k[X]$ nullteilerfrei und es gilt* $\operatorname{grad}(PQ) = \operatorname{grad} P + \operatorname{grad} Q$.

Beweis. Ist k nullteilerfrei, so ist offensichtlich der Leitkoeffizient von PQ das Produkt der Leitkoeffizienten von P und von Q. □

Ergänzende Übung 2.5.14. Ist k ein Integritätsbereich, so induziert die kanonische Einbettung $k \hookrightarrow k[X]$ auf den Einheitengruppen eine Bijektion $k^\times \xrightarrow{\sim} (k[X])^\times$. Im Ring $(\mathbb{Z}/4\mathbb{Z})[X]$ aber ist etwa auch $\bar{1} + \bar{2}X$ eine Einheit.

Lemma 2.5.15 (Teilen mit Rest in Polynomringen). *Sei k ein vom Nullring verschiedener Ring. Gegeben Polynome $P, Q \in k[X]$ mit Q normiert gibt es Polynome A, R mit $P = AQ + R$ und* $\operatorname{grad} R < \operatorname{grad} Q$. *Ist k nullteilerfrei, so sind diese Polynome A und R sogar eindeutig bestimmt.*

Beispiel 2.5.16. Die Polynomdivision mit Rest des Polynoms $(X^4 + 2X^2)$ durch $(X^2 + 2X + 1)$ liefert

$$\begin{array}{rcl} X^4 + 2X^2 & = & X^2(X^2 + 2X + 1) - 2X^3 + X^2 \\ & = & X^2(X^2 + 2X + 1) - 2X(X^2 + 2X + 1) + 5X^2 + 2X \\ & = & (X^2 - 2X + 5)(X^2 + 2X + 1) - 8X - 5 \end{array}$$

Beweis. Wir suchen A mit $\operatorname{grad}(P - AQ)$ kleinstmöglich. Gälte dann noch $\operatorname{grad}(P - AQ) \geq \operatorname{grad}(Q)$, sagen wir $P - AQ = aX^r + \ldots + c$ mit $a \neq 0$ und $r \geq d = \operatorname{grad}(Q)$, so hätte $P - (A + aX^{r-d})Q$ echt kleineren Grad als R, im Widerspruch

zur Wahl von A. Das zeigt die Existenz. Für den Nachweis der Eindeutigkeit gehen wir aus von einer weiteren Gleichung $P = A'Q + R'$ mit $\operatorname{grad} R' < d$. Es folgt zunächst $(A - A')Q = R' - R$ und mit 2.5.13 weiter $A - A' = 0$ und dann auch $R' - R = 0$. □

Korollar 2.5.17 (Abspalten von Linearfaktoren bei Nullstellen). *Sei k ein Kring und $P \in k[X]$ ein Polynom. Genau dann ist $\lambda \in k$ eine Nullstelle des Polynoms P, wenn $(X - \lambda)$ das Polynom P teilt.*

2.5.18. Der im Sinne von 2.5.12 lineare Faktor $(X - \lambda)$ unseres Polynoms heißt auch ein **Linearfaktor**, daher der Name des Korollars.

Beweis. Nach Lemma 2.5.15 über die Division mit Rest finden wir ein Polynom $A \in k[X]$ und eine Konstante $b \in k$ mit $P = A(X - \lambda) + b$. Einsetzen von $X = \lambda$ liefert dann $b = 0$. □

Satz 2.5.19 (Zahl der Nullstellen eines Polynoms). *Ist k ein Körper oder allgemeiner ein kommutativer Integritätsbereich, so hat ein von Null verschiedenes Polynom $P \in k[X]$ höchstens $\operatorname{grad} P$ Nullstellen in k.*

Beweis. Ist $\lambda \in k$ eine Nullstelle, so finden wir nach 2.5.17 eine Darstellung $P = A(X - \lambda)$ mit $\operatorname{grad} A = \operatorname{grad} P - 1$. Eine von λ verschiedene Nullstelle von P ist für k nullteilerfrei notwendig eine Nullstelle von A und der Satz folgt mit Induktion. □

Beispiel 2.5.20. In einem Körper k gibt es zu jedem Körperelement $b \in k$ höchstens zwei Elemente $a \in k$ mit $a^2 = b$. Ist nämlich a eine Lösung dieser Gleichung, so gilt $(X^2 - b) = (X - a)(X + a)$, und wenn wir da für X etwas von $\pm a$ Verschiedenes einsetzen, kommt sicher nicht Null heraus.

Ergänzung 2.5.21. Die Kommutativität ist hierbei wesentlich. In 2.9.4 werden wir den sogenannten "Schiefkörper der Quaternionen" einführen, einen Ring, der außer der Kommutativität der Multiplikation alle unsere Körperaxiome erfüllt. In diesem Ring hat die Gleichung $X^2 = -1$ dann nach **??** sogar unendlich viele Lösungen.

Übung 2.5.22. Man zeige, daß es in einem endlichen Körper $\mathbb{F}$ einer von 2 verschiedenen Charakteristik genau $(|\mathbb{F}| + 1)/2$ Quadrate gibt, wohingegen in einem endlichen Körper der Charakteristik 2 jedes Element das Quadrat eines weiteren Elements ist.

2.5.23. Ist k ein Körper oder allgemeiner ein kommutativer Integritätsbereich, $P \in k[X]$ ein Polynom und $\lambda \in k$ eine Nullstelle von P, so nennen wir das Supremum über alle $n \in \mathbb{N}$ mit $(X - \lambda)^n | P$ die **Vielfachheit der Nullstelle** λ oder auch ihre **Ordnung**. Ganz genauso wie eben zeigt man weiter, daß die Zahl der mit ihren Vielfachheiten gezählten Nullstellen eines von Null verschiedenen Polynoms beschränkt ist durch seinen Grad.

Definition 2.5.24. Ein Körper k heißt **algebraisch abgeschlossen** genau dann, wenn jedes nichtkonstante Polynom $P \in k[X] \setminus k$ mit Koeffizienten in unserem Körper k auch eine Nullstelle in unserem Körper k hat.

Beispiel 2.5.25. Der Körper $\mathbb{C}$ der komplexen Zahlen ist algebraisch abgeschlossen. Das ist die Aussage des sogenannten "Fundamentalsatzes der Algebra", für den wir mehrere Beweise geben werden: Einen besonders elementaren Beweis nach Argand geben wir in der Analysis in **??**, einen sehr eleganten mit den Methoden der Funktionentheorie in **??**, einen mehr algebraischen Beweis, bei dem die Analysis nur über den Zwischenwertsatz eingeht, in III.4.4.12. Mir gefällt der Beweis mit den Mitteln der Topologie **??**, der in analytischer Verkleidung auch in **??** gegeben wird, am besten, da er meine Anschauung am meisten anspricht.

Satz 2.5.26. *Ist k ein algebraisch abgeschlossener Körper, so hat jedes von Null verschiedene Polynom $P \in k[X]\backslash 0$ eine* **Zerlegung in Linearfaktoren** *der Gestalt*

$$P = c(X - \lambda_1) \dots (X - \lambda_n)$$

mit $n \geq 0$, $c \in k^\times$, und $\lambda_1, \dots, \lambda_n \in k$, und diese Zerlegung ist eindeutig bis auf die Reihenfolge der Faktoren.

2.5.27. Gegeben eine Nullstelle μ von P ist in diesem Fall die Zahl der Indizes i mit $\lambda_i = \mu$ die Vielfachheit der Nullstelle μ.

Beweis. Ist P ein konstantes Polynom, so ist nichts zu zeigen. Ist P nicht konstant, so gibt es nach Annahme eine Nullstelle $\lambda \in k$ von P und wir finden genau ein Polynom $\tilde{P}$ mit $P = (X - \lambda)\tilde{P}$. Der Satz folgt durch vollständige Induktion über den Grad von P. □

Korollar 2.5.28 (Faktorisierung reeller Polynome). *Jedes von Null verschiedene Polynom P mit reellen Koeffizienten besitzt eine Zerlegung in Faktoren der Gestalt*

$$P = c(X - \lambda_1) \dots (X - \lambda_r)(X^2 + \mu_1 X + \nu_1) \dots (X^2 + \mu_s X + \nu_s)$$

mit $c, \lambda_1, \dots, \lambda_r, \mu_1, \dots, \mu_s, \nu_1, \dots, \nu_s \in \mathbb{R}$ derart, daß die quadratischen Faktoren keine reellen Nullstellen haben. Diese Zerlegung ist eindeutig bis auf die Reihenfolge der Faktoren.

Beweis. Da unser Polynom stabil ist unter der komplexen Konjugation, müssen sich seine mit ihren Vielfachheiten genommenen komplexen Nullstellen so durchnummerieren lassen, daß $\lambda_1, \dots, \lambda_r$ reell sind und daß eine gerade Zahl nicht reeller Nullstellen übrigbleibt mit $\lambda_{r+2i} = \bar{\lambda}_{r+2i+1}$. Die Produkte $(X - \lambda_{r+2i})(X - \lambda_{r+2i+1})$ haben dann reelle Koeffizienten, da sie ja stabil sind unter der komplexen Konjugation, haben jedoch keine reellen Nullstellen. □

Heuristische Begründung für den Fundamentalsatz der Algebra. Ein Polynom n-ten Grades wird eine sehr große Kreislinie in der komplexen Zahlenebene mit Zentrum im Ursprung abbilden auf einen Weg in der komplexen Zahlenebene, der "den Ursprung n-mal umläuft". Angedeutet ist etwa das Bild einer sehr großen Kreislinie unter einem Polynom vom Grad Zwei. Schrumpfen wir nun unsere sehr große Kreislinie zu immer kleineren Kreislinien bis auf einen Punkt, so schrumpfen auch diese Wege zu einem konstanten Weg zusammen. Diese n-fach um einen etwa am Ursprung aufgestellten Pfahl laufende Seilschlinge kann jedoch offensichtlich nicht auf einen Punkt zusammengezogen werden, ohne daß wir sie über den Pfahl heben, oder anders gesagt: Mindestens eines der Bilder dieser kleineren Kreislinien muß durch den Ursprung laufen, als da heißt, unser Polynom muß auf mindestens einer dieser kleineren Kreislinien eine Nullstelle habe. In **??** oder besser **??** werden wir diese Heuristik zu einem formalen Beweis ausbauen.

Ergänzende Übung 2.5.29. Ein reelles Polynom hat bei $\lambda \in \mathbb{R}$ eine mehrfache Nullstelle genau dann, wenn auch seine Ableitung bei λ verschwindet.

Ergänzende Übung 2.5.30. Gegeben ein reelles Polynom, dessen komplexe Nullstellen bereits sämtlich reell sind, ist jede Nullstelle seiner Ableitung, die keine Nullstelle der Funktion selbst ist, eine einfache Nullstelle der Ableitung. Hinweis: Zwischen je zwei Nullstellen unserer Funktion muß mindestens eine Nullstelle ihrer Ableitung liegen.

Ergänzende Übung 2.5.31. Man zeige: Die rationalen Nullstellen eines normierten Polynoms mit ganzzahligen Koeffizienten $P \in \mathbb{Z}[X]$ sind bereits alle ganz. In Formeln folgt aus $P(\lambda) = 0$ für $\lambda \in \mathbb{Q}$ also bereits $\lambda \in \mathbb{Z}$.

2.5.32. Ähnlich wie den Polynomring in einer Variablen 2.5.2 konstruiert man auch Polynomringe in mehr Variablen. Ist die Zahl der Variablen endlich, so kann man induktiv definieren

$$R[X_1, \ldots, X_n] = (R[X_1, \ldots, X_{n-1}])[X_n]$$

Man kann aber auch für eine beliebige Menge I den Polynomring $R[X_i]_{i\in I}$ bilden als die Menge aller "endlichen formalen Linearkombinationen mit Koeffizienten aus R von endlichen Monomen in den X_i". Ich verzichte an dieser Stelle auf eine formale Definition.

Ergänzende Übung 2.5.33. Gegeben ein Ring k bilden auch die **formalen Potenzreihen mit Koeffizienten in** k der Gestalt $\sum_{n\geq 0} a_n X^n$ mit $a_n \in k$ einen Ring, der meist $k[\![X]\!]$ notiert wird. Man gebe eine exakte Definition dieses Rings und zeige, daß seine Einheiten genau diejenigen Potenzreihen sind, deren konstanter Term eine Einheit in k ist, in Formeln

$$k[\![X]\!]^\times = k^\times + Xk[\![X]\!]$$

Ergänzende Übung 2.5.34. Gegeben ein Ring k bilden auch die **Laurentreihen mit Koeffizienten in** k der Gestalt $\sum_{n\geq -N} a_n X^n$ mit $a_n \in k$ und $N \in \mathbb{N}$ einen Ring, der meist $k(\!(X)\!)$ notiert wird. Man gebe eine exakte Definition dieses Rings und zeige, daß seine Einheiten genau diejenigen Potenzreihen sind, bei denen der Koeffizient der kleinsten mit von Null verschiedenem Koeffizienten auftauchenden Potenz von X eine Einheit in k ist, in Formeln

$$k(\!(X)\!)^\times = \bigcup_{n\in\mathbb{Z}} X^n k[\![X]\!]^\times$$

Insbesondere ist im Fall eines Körpers k auch $k(\!(X)\!)$ ein Körper.

Lemma 2.5.35 (Interpolation durch Polynome). *Seien k ein Körper, $x_0, \ldots, x_n \in k$ paarweise verschiedene "Stützstellen" und $y_0, \ldots, y_n \in k$ beliebig vorgegeben. So gibt es genau ein Polynom $P \in k[X]$ vom Grad $\leq n$ mit $P(x_0) = y_0, \ldots, P(x_n) = y_n$.*

Das Polynom $P(X) = X^3 - 3X + 1$ mit reellen Koeffizienten, das die an den Stützstellen $-1, 1, 2$ vorgegebenen Werte $3, -1, 3$ interpoliert.

Beweis. Zunächst ist sicher $(X - x_1) \dots (X - x_n) = A_0(X)$ ein Polynom vom Grad n, das bei $x_1, \dots, x_n$ verschwindet und an allen anderen Stellen von Null verschieden ist, insbesondere auch bei x_0. Dann ist $L_0(X) = A_0(X)/A_0(x_0)$ ein Polynom vom Grad n, das bei x_0 den Wert Eins annimmt und bei $x_1, \dots, x_n$ verschwindet. In derselben Weise konstruieren wir auch Polynome $L_1(X), \dots, L_n(X)$ und erhalten ein mögliches Interpolationspolynom als

$$P(X) = y_0 L_0(X) + \dots + y_n L_n(X) = \sum_{i=0}^{n} y_i \frac{\prod_{j \neq i}(X - x_j)}{\prod_{j \neq i}(x_i - x_j)}$$

Das zeigt die Existenz. Ist Q eine weitere Lösung derselben Interpolationsaufgabe vom Grad $\leq n$, so ist $P - Q$ ein Polynom vom Grad $\leq n$ mit $n+1$ Nullstellen, eben bei den Stützstellen $x_0, \dots, x_n$. Wegen 2.5.19 muß dann $P - Q$ das Nullpolynom sein, und das zeigt die Eindeutigkeit. □

2.5.36. Um die bisher eingeführten algebraischen Konzepte anschaulicher zu machen, will ich sie in Bezug setzen zu geometrischen Konzepten. Ist k ein Kring, so können wir jedem Polynom $f \in k[X_1, \dots, X_n]$ die Funktion $\tilde{f} : k^n \to k$, $(x_1, \dots, x_n) \mapsto f(x_1, \dots, x_n)$ zuordnen. Wir erhalten so einen Ringhomomorphismus

$$k[X_1, \dots, X_n] \to \mathrm{Ens}(k^n, k)$$

Dieser Homomorphismus ist im Allgemeinen weder injektiv noch surjektiv. Schon für $n = 1$, $k = \mathbb{R}$ läßt sich ja keineswegs jede Abbildung $\mathbb{R} \to \mathbb{R}$ durch ein Polynom beschreiben, und im Fall eines endlichen Körpers k kann für $n \geq 1$ unsere k-lineare Auswertungsabbildung vom unendlichdimensionalen k-Vektorraum $k[X_1, \dots, X_n]$ in den endlichdimensionalen k-Vektorraum $\mathrm{Ens}(k^n, k)$ unmöglich injektiv sein. Wir haben jedoch:

Satz 2.5.37 (Polynome als Funktionen). *1. Ist k ein unendlicher Körper oder allgemeiner ein unendlicher nullteilerfreier Kring, so ist für alle $n \in \mathbb{N}$ die Auswertungsabbildung eine Injektion $k[X_1, \dots, X_n] \hookrightarrow \mathrm{Ens}(k^n, k)$.*

2. Ist k ein endlicher Körper, so ist für alle $n \in \mathbb{N}$ die Auswertungsabbildung eine Surjektion $k[X_1, \dots, X_n] \twoheadrightarrow \mathrm{Ens}(k^n, k)$. Den Kern dieser Surjektion beschreibt Übung 7.3.10.

Beweis. 1. Durch Induktion über n. Der Fall $n = 0$ ist eh klar. Für $n = 1$ folgt die Behauptung aus der Erkenntnis, das jedes von Null verschiedene Polynom in $k[X]$ nur endlich viele Nullstellen in k haben kann. Der Kern der Abbildung

$$k[X] \to \mathrm{Ens}(k, k)$$

besteht also nur aus dem Nullpolynom. Für den Induktionsschritt setzen wir $X_n = Y$ und schreiben unser Polynom in der Gestalt

$$P = a_d Y^d + \ldots + a_1 Y + a_0$$

mit $a_i \in k[X_1, \ldots, X_{n-1}]$. Halten wir $(x_1, \ldots, x_{n-1}) = x \in k^{n-1}$ fest, so ist $a_d(x)Y^d + \ldots + a_1(x)Y + a_0(x) \in k[Y]$ das Nullpolynom nach dem Fall $n = 1$. Also verschwinden $a_d(x), \ldots, a_1(x), a_0(x)$ für alle $x \in k^{n-1}$, mit Induktion sind somit alle a_i schon das Nullpolynom und wir haben $P = 0$.

2. Das bleibt dem Leser überlassen. Man mag sich beim Beweis an 2.5.35 orientieren. Wir folgern in III.2.2.7 eine allgemeinere Aussage aus dem abstrakten chinesischen Restsatz. □

Ergänzende Übung 2.5.38. Man zeige, daß jeder algebraisch abgeschlossene Körper unendlich ist. Hinweis: Im Fall $1 \neq -1$ reicht es, Quadratwurzeln zu suchen. Man zeige, daß ein nichtkonstantes Polynom in zwei oder mehr Veränderlichen über einem algebraisch abgeschlossenen Körper stets unendlich viele Nullstellen hat.

Ergänzende Übung 2.5.39. Sei k ein unendlicher Körper. Verschwindet ein Polynom im Polynomring in d Variablen über k auf einer affinen Hyperebene in k^d, so wird es von der, bis auf einen Skalar eindeutig bestimmten, linearen Gleichung besagter Hyperebene geteilt. Hinweis: Ohne Beschränkung der Allgemeinheit mag man unsere Hyperebene als eine der Koordinatenhyperebenen annehmen. Man zeige auch allgemeiner: Verschwindet ein Polynom in d Veränderlichen über einem unendlichen Körper auf der Vereinigung der paarweise verschiedenen affinen Hyperebenen $H_1, \ldots, H_n \subset k^d$, so wird es vom Produkt der linearen Gleichungen unserer Hyperebenen geteilt.

Ergänzende Übung 2.5.40 (**Pythagoreische Zahlen**). Man zeige: Stellen wir eine Lampe oben auf den Einheitskreis und bilden jeden von $(0, 1)$ verschiedenen Punkt des Einheitskreises ab auf denjenigen Punkt der Parallelen zur x-Achse durch $(0, -1)$, auf den sein Schatten fällt, so entsprechen die Punkte mit rationalen Koordinaten auf dem Einheitskreis genau den Punkten mit rationalen Koordinaten auf unserer Parallelen. Hinweis: Hat ein Polynom in $\mathbb{Q}[X]$ vom Grad drei zwei rationale Nullstellen, so ist auch seine dritte Nullstelle rational.

Ergänzung 2.5.41. Unter einem **pythagoreischen Zahlentripel** versteht man ein Tripel (a, b, c) von positiven natürlichen Zahlen mit $a^2 + b^2 = c^2$, die also als Seitenlängen eines rechtwinkligen Dreiecks auftreten können. Es scheint mir jedoch offensichtlich, daß die Bestimmung aller pythagoreischen Zahlentripel im wesentlichen äquivalent ist zur Bestimmung aller Punkte mit rationalen Koordinaten auf dem Einheitskreis, also aller $(x, y) \in \mathbb{Q}^2$ mit $x^2 + y^2 = 1$.

Wir stellen eine Lampe oben auf den Einheitskreis und bilden jeden von $(0,1)$ verschiedenen Punkt des Einheitskreises ab auf denjenigen Punkt der Parallelen zur x-Achse durch $(0,-1)$, auf den sein Schatten fällt. So entsprechen nach Übung 2.5.40 die Punkte mit rationalen Koordinaten auf dem Einheitskreis genau den Punkten mit rationalen Koordinaten auf unserer Parallelen. Ein Tripel $a,b,c \in \mathbb{Z}$ mit $a^2+b^2=c^2$ heißt ein **pythagoreisches Zahlentripel**. Die pythagoreischen Zahlentripel mit größtem gemeinsamen Teiler $\langle a,b,c\rangle = \langle 1\rangle$ und $c>0$ entsprechen nun offensichtlich eineindeutig den Punkten mit rationalen Koordinaten auf dem Einheitskreis vermittels der Vorschrift $(a,b,c) \mapsto (a/c, b/c)$. In dieser Weise liefert unser Bild also einen geometrischen Zugang zur Klassifikation der pythagoreischen Zahlentripel.

2.6 Äquivalenzrelationen

Definition 2.6.1. Eine Relation $R \subset X \times X$ auf einer Menge X im Sinne von **??** heißt eine **Äquivalenzrelation** genau dann, wenn für alle $x, y, z \in X$ gilt

1. **Transitivität:** (xRy und yRz) $\Rightarrow xRz$;
2. **Symmetrie:** $xRy \Leftrightarrow yRx$;
3. **Reflexivität:** xRx.

2.6.2. Ist eine Relation symmetrisch und transitiv und ist jedes Element in Relation zu mindestens einem weiteren Element, so ist unsere Relation bereits reflexiv. Ein Beispiel für eine Relation, die symmetrisch und transitiv ist, aber nicht reflexiv, wäre etwa die "leere Relation" $R = \emptyset$ auf einer nichtleeren Menge $X \neq \emptyset$.

2.6.3. Gegeben eine Äquivalenzrelation $\sim$ auf einer Menge X betrachtet man für $x \in X$ die Menge $A(x) := \{z \in X \mid z \sim x\}$ und nennt sie die **Äquivalenzklasse von** x. Eine Teilmenge $A \subset X$ heißt eine **Äquivalenzklasse** für unsere Äquivalenzrelation genau dann, wenn es ein $x \in X$ gibt derart, daß $A = A(x)$ die Äquivalenzklasse von x ist. Ein Element einer Äquivalenzklasse nennt man auch einen **Repräsentanten** der Klasse. Eine Teilmenge $Z \subset X$, die aus jeder Äquivalenzklasse genau ein Element enthält, heißt ein **Repräsentantensystem**. Aufgrund der Reflexivität gilt $x \in A(x)$, und man sieht leicht, daß für $x, y \in X$ die folgenden drei Aussagen gleichbedeutend sind:

1. $x \sim y$;
2. $A(x) = A(y)$;
3. $A(x) \cap A(y) \neq \emptyset$.

2.6.4. Gegeben eine Äquivalenzrelation $\sim$ auf einer Menge X bezeichnen wir die Menge aller Äquivalenzklassen, eine Teilmenge der Potenzmenge $\mathcal{P}(X)$, mit

$$(X/\sim) := \{A(x) \mid x \in X\}$$

und haben eine kanonische Abbildung $\mathrm{can} : X \to (X/\sim),\ x \mapsto A(x)$. Ist weiter $f : X \to Z$ eine Abbildung mit $x \sim y \Rightarrow f(x) = f(y)$, so gibt es genau eine Abbildung $\bar{f} : (X/\sim) \to Z$ mit $f = \bar{f} \circ \mathrm{can}$. Wir zitieren diese Eigenschaft manchmal als die **universelle Eigenschaft des Raums der Äquivalenzklassen**. Sagt man, eine Abbildung $g : (X/\sim) \to Z$ sei **wohldefiniert** durch eine Abbildung $f : X \to Z$, so ist gemeint, daß f die Eigenschaft $x \sim y \Rightarrow f(x) = f(y)$ hat und daß man $g = \bar{f}$ setzt.

2.6.5. Die kanonische Abbildung $\mathrm{can} : X \to (X/\sim)$ ist stets eine Surjektion. Ist umgekehrt $f : X \twoheadrightarrow Z$ eine Surjektion und betrachten wir auf X die Relation $x \sim y \Leftrightarrow f(x) = f(y)$, so ist besagte Relation eine Äquivalenzrelation und die kanonische Abbildung $\bar{f}$ liefert eine Bijektion $\bar{f} : (X/\sim) \xrightarrow{\sim} Z$.

Beispiel 2.6.6. Gegeben eine ganze Zahl $m \in \mathbb{Z}$ ist unser "kongruent modulo m" aus 2.4.7 eine Äquivalenzrelation $\sim$ auf $\mathbb{Z}$ und die zugehörigen Äquivalenzklassen sind genau unsere Restklassen von dort, so daß wir also $(\mathbb{Z}/\sim) = \mathbb{Z}/m\mathbb{Z}$ erhalten.

Ergänzung 2.6.7. Sind $R \subset X \times X$ und $S \subset Y \times Y$ Äquivalenzrelationen, so auch das Bild von $(R \times S) \subset (X \times X) \times (Y \times Y)$ unter der durch Vertauschen der mittleren Einträge gegebenen Identifikation $(X \times X) \times (Y \times Y) \xrightarrow{\sim} (X \times Y) \times (X \times Y)$. Wir notieren diese Äquivalenzrelation auf dem Produkt kurz $R \times S$.

Ergänzende Übung 2.6.8. Ist G eine Gruppe und $H \subset G \times G$ eine Untergruppe, die die Diagonale umfaßt, so ist H eine Äquivalenzrelation.

Ergänzung 2.6.9. Gegeben auf einer Menge X eine Relation $R \subset X \times X$ gibt es eine kleinste Äquivalenzrelation $T \subset X \times X$, die R umfaßt. Man kann diese Äquivalenzrelation entweder beschreiben als den Schnitt aller Äquivalenzrelationen, die R umfassen, oder auch als die Menge T aller Paare (x, y) derart, daß es ein $n \geq 0$ gibt und Elemente $x = x_0, x_1, \ldots, x_n = y$ von X mit $x_\nu R x_{\nu-1}$ oder $x_{\nu-1} R x_\nu$ für alle ν mit $1 \leq \nu \leq n$. Wir nennen T auch die **von der Relation R erzeugte Äquivalenzrelation auf X**. Denken wir uns etwa X als die "Menge aller Tiere" und R als die Relation "könnten im Prinzip miteinander fruchtbaren Nachwuchs zeugen", so wären die Äquivalenzklassen unter der von dieser Relation erzeugten Äquivalenzrelation eine mathematische Fassung dessen, was Biologen unter einer "Tierart" verstehen würden.

2.7 Rechnen mit Einheiten*

2.7.1. In der Physik rechnet man meist mit sogenannten **Einheiten** oder genauer **physikalischen Einheiten**, um das Ergebnis der Rechnung auch im materiellen Teil unserer Welt interpretieren zu können. Mathematisch mag man diese Einheiten als Erzeuger eindimensionaler reeller Vektorräume modellieren, den **Dimensionen** oder genauer **physikalischen Dimensionen**. Während die physikalischen Einheiten begrifflich eng mit unseren mathematischen Einheiten aus 2.4.25 verwandt sind, haben die physikalischen Dimensionen wie Zeit und Ort mit dem mathematischen Begriff der Dimension eines Vektorraums nun leider rein gar nichts zu tun, wie bereits in 1.4.26 angesprochen. Zeiteinheiten wie Sekunde, Minute, Stunde, Woche und dergleichen modellieren wir mathematisch nach 1.7.9 etwa als Elemente eines eindimensionalen Vektorraums $\vec{\mathbb{T}}$ aller Zeitspannen. Längeneinheiten wie Meter, Zoll, Inch, Fuß, Elle und dergleichen modellieren wir

mathematisch als Elemente eines eindimensionalen reellen Vektorraums $\mathbb{L}$ aller "Längen", dessen Beziehung zum Anschauungsraum $\mathbb{E}$ wir in 8.6.6 noch ausführlich diskutieren werden. Weitere Beispiele von Einheiten sind Ihnen sicher bereits begegnet, und sie haben sicher auch im Physikunterricht schon ausgiebig mit Einheiten gerechnet. Um derartige Rechnungen im Rahmen der Mengenlehre zu formalisieren, gilt es, die Räume zu konstruieren, in denen denn nun diese Produkte und Quotienten von Einheiten liegen sollen. Das wird im folgenden ausgeführt.

Definition 2.7.2. Gegeben ein Körper k und ein k-Vektorraum V und ein eindimensionaler k-Vektorraum L definieren wir einen neuen k-Vektorraum, das **Tensorprodukt**

$$V \otimes L = V \otimes_k L$$

der Räume V und L, wie folgt: Wir beginnen mit der Menge $V \times L$ und definieren darauf eine Äquivalenzrelation $\sim$ durch die Vorschrift $(\lambda v, l) \sim (v, \lambda l)\ \forall \lambda \in k$, $v \in V$ und $l \in L$. Dann betrachten wir die Menge der Äquivalenzklassen $V \otimes L := (V \times L)/\sim$. Die Äquivalenzklasse des Paars (v, l) notieren wir $v \otimes l$. Im folgenden zeigen wir, daß es auf unserer Menge $V \otimes L$ genau eine Struktur als k-Vektorraum gibt mit den Eigenschaften $(v \otimes l) + (w \otimes l) = (v + w) \otimes l$ und $\lambda(v \otimes l) = (\lambda v) \otimes l$ $\forall \lambda \in k$, $v, w \in V$ und $l \in L$. Diesen Vektorraum notieren wir dann $V \otimes L$ und nennen ihn das Tensorprodukt von V und L.

2.7.3. In 9.3.2 werden wir lernen, wie man allgemeiner für zwei beliebige Vektorräume ihr Tensorprodukt definiert. Hier beschränken wir uns auf den einfacheren Fall des Tensorprodukts mit eindimensionalen Räumen.

2.7.4. Um auf der Menge $V \otimes L$ die Existenz einer Vektorraumstruktur mit den behaupteten Eigenschaften zu zeigen, betrachten wir die Abbildung $V \times L \to \mathrm{Hom}(L^\top, V)$ in den Raum der Homomorphismen des Dualraums von L nach V, gegeben durch die Abbildungsvorschrift $(v, l) \mapsto (f \mapsto f(l)v)$ für alle Linearformen f auf L. Es ist leicht zu sehen, daß diese Abbildung auf Äquivalenzklassen eine Bijektion $V \otimes L \xrightarrow{\sim} \mathrm{Hom}(L^\top, V)$ induziert, und daß die vermittels dieser Bijektion auf die linke Seite übertragene Vektorraumstruktur auch durch die in unserer Definition 2.7.2 angegebenen Eigenschaften charakterisiert werden kann.

2.7.5. Man könnte auch anders vorgehen und das Tensorprodukt $V \otimes L$ kurzerhand definieren als den Homomorphismenraum $\mathrm{Hom}(L^\top, V)$. Mir scheint jedoch dieser Zugang weniger durchsichtig, weshalb ich den formal umständlicheren Zugang aus der obigen Definition 2.7.2 gewählt habe.

Beispiel 2.7.6. Es ist üblich, bei Produkten von Einheiten das Tensorzeichen wegzulassen. Betrachten wir etwa zunächst einmal noch nicht ganz so mathematisch den Vektorraum $\mathbb{L}$ aller Längen und darin die beiden Basen m, genannt "Meter", und km, genannt "Kilometer", so daß also gilt $\mathrm{km} = 1000\,\mathrm{m}$. Gegeben $l \in \mathbb{L}$ kürzt

man üblicherweise $l^2 := l^{\otimes 2} := l \otimes l$ ab. In $\mathbb{L} \otimes \mathbb{L}$ erhalten wir dann $\mathrm{km}^2 = 10^6\,\mathrm{m}^2$. In unserem Formalismus ist also in der Tat und wie es sich gehört ein Quadratkilometer eine Million Quadratmeter. Etwas mathematischer folgt auch für zwei beliebige Vektoren v, w eines eindimensionalen Vektorraums L mit $v = \lambda w$ im Tensorquadrat $L \otimes L$ die Identität $v \otimes v = \lambda^2(w \otimes w)$.

Ergänzung 2.7.7. Sei weiter V ein Vektorraum und L ein eindimensionaler Vektorraum. Unsere kanonische Bijektion $V \otimes L \xrightarrow{\sim} \mathrm{Hom}(L^\top, V)$ aus 2.7.4 liefert zusammen mit der kanonischen Identifikation eines endlichdimensionalen Raums mit seinem Bidualraum 1.11.21 auch eine kanonische Bijektion

$$V \otimes L^\top \xrightarrow{\sim} \mathrm{Hom}(L, V)$$

Mithilfe dieser Bijektion können wir etwa unseren Raum der vektoriellen Geschwindigkeiten $\mathrm{Hom}(\vec{\mathbb{T}}, \vec{\mathbb{E}})$ aus 1.7.10 mit dem Tensorprodukt $\vec{\mathbb{E}} \otimes \vec{\mathbb{T}}^\top$ identifizieren. Ich finde diese Darstellung insbesondere bei komplizierteren Ausdrücken übersichtlicher.

Übung 2.7.8. Gegeben eine lineare Abbildung $f : V \to W$ und eine lineare Abbildung von eindimensionalen Räumen $g : L \to M$ gibt es genau eine lineare Abbildung $f \otimes g : V \otimes L \to W \otimes M$ mit $f \otimes g : v \otimes l \mapsto f(v) \otimes g(l)$.

Übung 2.7.9. Sei V ein Vektorraum und L ein eindimensionaler Vektorraum. Ist $(v_i)_{i \in I}$ eine Basis von V und $l \in L$ ein von Null verschiedener Vektor, so ist $(v_i \otimes l)_{i \in I}$ eine Basis von $V \otimes L$.

Übung 2.7.10. Gegeben ein Vektorraum V und eindimensionale Vektorräume L, M gibt es genau einen Vektorraumisomorphismus

$$(V \otimes L) \otimes M \xrightarrow{\sim} V \otimes (L \otimes M)$$

mit $(v \otimes l) \otimes m \mapsto v \otimes (l \otimes m)$ für alle $v \in V$, $l \in L$ und $m \in M$. Gegeben eindimensionale Vektorräume L, M gibt es genau einen Vektorraumisomorphismus $L \otimes M \xrightarrow{\sim} M \otimes L$ mit $l \otimes m \mapsto m \otimes l$ für alle $l \in L$ und $m \in M$.

Übung 2.7.11. Ist V ein k-Vektorraum, so gibt es genau einen Vektorraumisomorphismus $V \otimes_k k \xrightarrow{\sim} V$ mit $v \otimes \lambda \mapsto \lambda v$ für alle $v \in V$ und $\lambda \in k$.

Übung 2.7.12. Ist k ein Körper, L ein eindimensionaler k-Vektorraum und $L^\top$ sein Dualraum, so gibt es genau einen Vektorraumisomorphismus $L \otimes L^\top \xrightarrow{\sim} k$ mit $l \otimes f \mapsto f(l)$ für alle $l \in L$ und $f \in L^\top$.

2.7.13. Bei längeren Tensorprodukten lassen wir die Klammern meist weg und interpretieren solche Ausdrücke als “der Reihe nach immer mehr Faktoren hinten drantensoriert”. Das r-fache Tensorprodukt eines eindimensionalen k-Vektorraums L mit sich selbst notieren wir $L^{\otimes r}$ und das r-fache Tensorprodukt eines Vektors

$l \in L$ mit sich selbst darin $l^{\otimes r} \in L^{\otimes r}$. Dann gilt $l^{\otimes r} \otimes l^{\otimes s} \mapsto l^{\otimes(r+s)}$ für alle natürlichen Zahlen $r, s \geq 1$ unter allen durch eine Verknüpfung der Isomorphismen 2.7.10 gegebenen Identifikationen

$$L^{\otimes r} \otimes L^{\otimes s} \xrightarrow{\sim} L^{\otimes(r+s)}$$

Vereinbaren wir weiter $L^{\otimes 0} = k$ und $l^{\otimes 0} = 1$ für alle $l \in L$, so gilt sogar $l^{\otimes r} \otimes l^{\otimes s} \mapsto l^{\otimes(r+s)}$ für alle natürlichen Zahlen $r, s \geq 0$ unter allen durch durch eine Verknüpfung der Isomorphismen 2.7.10, 2.7.11 gegebenen Identifikationen $L^{\otimes r} \otimes L^{\otimes s} \xrightarrow{\sim} L^{\otimes(r+s)}$. Vereinbaren wir schließlich für ganze Zahlen $r < 0$ die Notation $L^{\otimes r} = (L^\top)^{\otimes(-r)}$ und bezeichnen für $l \in L\backslash 0$ mit $l^{\otimes(-1)} \in L^\top$ den eindeutig bestimmten Vektor des Dualraums, der auf l den Wert 1 annimmt, und setzen $l^{\otimes r} = (l^{\otimes(-1)})^{\otimes(-r)}$, so gilt $l^{\otimes r} \otimes l^{\otimes s} \mapsto l^{\otimes(r+s)}$ bei $l \neq 0$ für alle ganzen Zahlen $r, s \in \mathbb{Z}$ unter allen durch eine Verknüpfung der Isomorphismen 2.7.10, 2.7.11 und 2.7.12 gegebenen Identifikationen $L^{\otimes r} \otimes L^{\otimes s} \xrightarrow{\sim} L^{\otimes(r+s)}$.

Ergänzung 2.7.14. Es ist auch hier üblich, bei Potenzen von Einheiten das Tensorzeichen wegzulassen. Ist zum Beispiel und noch nicht ganz so mathematisch $\mathbb{L}$ der eindimensionale Vektorraum der Längen und $\mathrm{m} \in \mathbb{L}$ seine Basis "Meter", so bezeichnet $\mathrm{m}^3 := \mathrm{m}^{\otimes 3}$ den Basisvektor des Raums $\mathbb{L}^{\otimes 3}$, dessen Elemente man gemeinhin **Volumina** nennt. Für m^3 ist auch die Bezeichnung **Kubikmeter** gebräuchlich. In 8.6.10 lernen wir das "Spatprodukt" kennen, das die Beziehung zwischen der dritten Tensorpotenz des Vektorraums der Längen und unserer Anschauung für Volumina dann auch formal rechtfertigt.

2.8 Quotientenkörper

Definition 2.8.1. Gegeben ein kommutativer Integritätsbereich R konstruieren wir seinen **Quotientenkörper**

$$\mathrm{Quot}(R)$$

wie folgt: Wir betrachten die Menge $R \times (R\backslash 0)$ und definieren darauf eine Relation $\sim$ durch die Vorschrift

$$(a, s) \sim (b, t) \text{ genau dann, wenn gilt } at = bs.$$

Diese Relation ist eine Äquivalenzrelation, wie man leicht prüft. Wir bezeichnen die Menge der Äquivalenzklassen mit $\mathrm{Quot}(R)$ und die Äquivalenzklasse von (a, s) mit $\frac{a}{s}$ oder a/s. Dann definieren wir auf $\mathrm{Quot}(R)$ Verknüpfungen $+$ und $\cdot$ durch die Regeln

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} \quad \text{und} \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

und überlassen dem Leser den Nachweis, daß diese Verknüpfungen wohldefiniert sind und $\mathrm{Quot}(R)$ zu einem Körper machen und daß die Abbildung $\mathrm{can} : R \to$

$\mathrm{Quot}(R), r \mapsto r/1$ ein injektiver Ringhomomorphismus ist. Er heißt die **kanonische Einbettung** unseres Integritätsbereichs in seinen Quotientenkörper.

Ergänzung 2.8.2. Auf Englisch bezeichnet man den Quotientenkörper als **fraction field** und auf Französisch als **corps de fractions**. Dort verwendet man folgerichtig statt unserer Notation $\mathrm{Quot}(R)$ die Notation $\mathrm{Frac}(R)$. Die noch allgemeinere Konstruktion der "Lokalisierung" lernen wir erst in **??** kennen.

Beispiel 2.8.3. Der Körper der rationalen Zahlen $\mathbb{Q}$ wird formal definiert als der Quotientenkörper des Rings der ganzen Zahlen, in Formeln

$$\mathbb{Q} := \mathrm{Quot}\,\mathbb{Z}$$

Sicher wäre es unter formalen Aspekten betrachtet eigentlich richtig gewesen, diese Definition schon viel früher zu geben. Es schien mir jedoch didaktisch ungeschickt, gleich am Anfang derart viel Zeit und Formeln auf die exakte Konstruktion einer Struktur zu verwenden, die Ihnen bereits zu Beginn ihres Studiums hinreichend vertraut sein sollte. Wie bereits bei rationalen Zahlen nennt man auch im allgemeinen bei einem Bruch g/h das g den **Zähler** und das h den **Nenner** des Bruchs.

Satz 2.8.4 (Universelle Eigenschaft des Quotientenkörpers). *Sei R ein kommutativer Integritätsbereich. Ist $\varphi : R \to A$ ein Ringhomomorphismus, unter dem jedes von Null verschiedene Element von R auf eine Einheit von A abgebildet wird, so faktorisiert φ eindeutig über* $\mathrm{Quot}\, R$*, es gibt also in Formeln genau einen Ringhomomorphismus $\tilde{\varphi} : \mathrm{Quot}\, R \to A$ mit $\varphi = \tilde{\varphi} \circ \mathrm{can}$.*

Beweis. Für jedes mögliche $\tilde{\varphi}$ muß gelten $\tilde{\varphi}(r/s) = \varphi(r)\varphi(s)^{-1}$, und das zeigt bereits die Eindeutigkeit von $\tilde{\varphi}$. Um auch seine Existenz zu zeigen, betrachten wir die Abbildung $\hat{\varphi} : R \times (R\backslash 0) \to A$ gegeben durch $\hat{\varphi}(r,s) = \varphi(r)\varphi(s)^{-1}$ und prüfen, daß sie konstant ist auf Äquivalenzklassen. Dann muß sie nach 2.6.4 eine wohlbestimmte Abbildung $\mathrm{Quot}\, R \to A$ induzieren, von der der Leser leicht selbst prüfen wird, daß sie ein Ringhomomorphismus ist. □

2.8.5. Ist k ein Körper, so bezeichnet man den Quotientenkörper des Polynomrings mit $k(X) := \mathrm{Quot}\, k[X]$ und nennt seine Elemente **rationale Funktionen**. Ähnlich schreibt man bei mehreren Veränderlichen

$$k(X_1, \ldots, X_n) := \mathrm{Quot}\, k[X_1, \ldots, X_n]$$

Ist k unendlich, so kann man sich die Elemente von $k(X)$ als "fast überall definierte k-wertige Funktionen auf k" vorstellen. Etwas formaler betrachten wir für eine beliebige Menge M auf dem Ring $\mathrm{Ens}(M,k)$ aller Abbildungen von M nach k die Äquivalenzrelation $\sim$ gegeben durch $f \sim g$ genau dann, wenn gilt

$f(x) = g(x)$ an allen außer endlich vielen Stellen $x \in M$. Es ist hoffentlich klar, wie zwei Äquivalenzklassen zu addieren bzw. zu multiplizieren sind, und daß die Menge der Äquivalenzklassen $(\mathrm{Ens}(M,k)/\sim)$ so zu einem Ring wird. Wir nennen ihn den **Ring der fast überall definierten k-wertigen Funktionen auf M** und notieren ihn $\mathrm{Ensf}(M,k)$. Dann liefert die universelle Eigenschaft des Quotientenkörpers 2.8.4 eine Einbettung

$$k(X) \hookrightarrow \mathrm{Ensf}(k,k)$$

Man definiert für jede rationale Funktion $f \in k(X)$ ihren **Definitionsbereich** $D(f) \subset k$ als die Menge aller Punkte $a \in k$ derart, daß f sich schreiben läßt als Quotient von zwei Polynomen $f = g/h$ mit $h(a) \neq 0$. Haben wir zwei solche Darstellungen $f = g/h = \hat{g}/\hat{h}$ mit $h(a) \neq 0 \neq \hat{h}(a)$, so gilt offensichtlich $g(a)/h(a) = \hat{g}(a)/\hat{h}(a)$ und wir definieren $f(a)$ als diesen gemeinsamen Wert. In diesem Sinne liefert also jedes $f \in k(X)$ eine Abbildung

$$f : D(f) \to k$$

Es ist leicht einzusehen, daß stets gilt $D(fg), D(f+g) \supset D(f) \cap D(g)$ sowie $(fg)(a) = f(a)g(a)$ und $(f+g)(a) = f(a)+g(a)$ für alle $a \in D(f) \cap D(g)$. Die endlich vielen Punkte außerhalb des Definitionsbereichs von f heißen die **Polstellen** von f. Vereinbart man, daß f diesen Stellen als Wert ein neues Symbol ∞ zuweisen soll, so erhält man für jeden unendlichen Körper sogar eine wohlbestimmte Injektion $k(X) \hookrightarrow \mathrm{Ens}(k, k \sqcup \{\infty\})$. Durch "Kürzen von Nullstellen" überlegt man sich auch leicht, daß jede rationale Funktion so als Quotient $f = g/h$ geschrieben werden kann, daß Zähler und Nenner keine gemeinsamen Nullstellen in k haben, und daß dann die Polstellen gerade die Nullstellen des Nenners sind.

Ergänzung 2.8.6. Es ist sogar richtig, daß jede rationale Funktion eine eindeutige maximal gekürzte Darstellung mit normiertem Nenner hat: Um das einzusehen, benötigt man jedoch ein Analogon der eindeutigen Primfaktorzerlegung für Polynomringe, das wir erst in III.2.3.23 zeigen.

Ergänzende Übung 2.8.7. Gegeben ein unendlicher Körper k und eine von Null verschiedene rationale Funktion $f \in k(X)^\times$ sind die Polstellen von f genau die Nullstellen von $(1/f)$, als da heißt, die Stellen aus dem Definitionsbereich von $(1/f)$, an denen diese Funktion den Wert Null annimmt. Fassen wir genauer f als Abbildung $f : k \to k \sqcup \{\infty\}$ auf, so entspricht $(1/f)$ der Abbildung $a \mapsto f(a)^{-1}$, wenn wir $0^{-1} = \infty$ und $\infty^{-1} = 0$ vereinbaren.

2.8.8. Wir erinnern aus 2.5.33 und 2.5.34 die Ringe der Potenzreihen und der Laurentreihen. Gegeben ein Körper k liefert die Verknüpfung von Einbettungen $k[X] \hookrightarrow k[\![X]\!] \hookrightarrow k((X))$ offensichtlich einen Ringhomomorphismus und nach der universellen Eigenschaft 2.8.4 mithin eine Einbettung $k(X) \hookrightarrow k((X))$. Das

Bild von $(1-X)^{-1}$ unter dieser Einbettung wäre etwa die "formale geometrische Reihe" $1+X+X^2+X^3+\ldots$

Ergänzende Übung 2.8.9. Man zeige, daß im Körper $\mathbb{Q}((X))$ jede formale Potenzreihe mit konstantem Koeffizienten Eins eine Quadratwurzel besitzt. Die Quadratwurzel von $(1+X)$ kann sogar durch die binomische Reihe **??** explizit angegeben werden, aber das sieht man leichter mit den Methoden der Analysis.

Ergänzung 2.8.10. Sei k ein Körper. Ist $p \in k$ fest gewählt und $k(T) \xrightarrow{\sim} k(X)$ der durch $T \mapsto (X+p)$ gegebene Isomorphismus, so bezeichnet man das Bild von $f \in k(T)$ unter der Komposition $k(T) \xrightarrow{\sim} k(X) \hookrightarrow k((X))$ auch als die **Laurententwicklung von f um den Entwicklungspunkt** p. Meist schreibt man in einer Laurententwicklung statt X auch $(T-p)$. So wäre die Laurententwicklung von $f = T^2/(T-1)$ um den Entwicklungspunkt $T=1$ etwa die endliche Laurentreihe $(T-1)^{-1}+2+(T-1)$.

Satz 2.8.11 (Partialbruchzerlegung). *Ist k ein algebraisch abgeschlossener Körper, so wird eine k-Basis des Funktionenkörpers $k(X)$ gebildet von erstens den Potenzen der Variablen $(X^n)_{n\geq 1}$ mitsamt zweitens den Potenzen der Inversen der Linearfaktoren $((X-a)^{-n})_{n\geq 1,\, a\in k}$ zuzüglich drittens dem Einselement 1 aus $k(X)$.*

2.8.12. Eine Darstellung einer rationalen Funktion als Linearkombination der Elemente dieser Basis nennt man eine **Partialbruchzerlegung** unserer rationalen Funktion. Anschaulich scheint mir zumindest die lineare Unabhängigkeit der behaupteten Basis recht einsichtig: Polstellen an verschiedenen Punkten können sich ebensowenig gegenseitig aufheben wie Polstellen verschiedener Ordnung an einem vorgegebenen Punkt. Die $(X^n)_{n\geq 1}$ mag man dabei auffassen als Funktionen, die "eine Polstelle der Ordnung n im Unendlichen haben", wie im Fall $k=\mathbb{C}$ etwa in **??** ausgeführt wird.

Ergänzung 2.8.13. In Büchern zur Analysis findet man oft eine Variante dieses Satzes für den Körper $k=\mathbb{R}$: In diesem Fall werden die im Satz beschriebenen Elemente ergänzt zu einer Basis durch die $1/((X-\lambda)(X-\bar{\lambda}))^n$ und die $X/((X-\lambda)(X-\bar{\lambda}))^n$ für $\lambda \in \mathbb{C}$ mit positivem Imaginärteil und $n \geq 1$ beliebig, wie der Leser zur Übung selbst zeigen mag. Eine Verallgemeinerung auf den Fall eines beliebigen Körpers k wird in III.3.4.17 diskutiert.

Beweis. Wir zeigen zunächst, daß unsere Familie von Funktionen den Funktionenkörper als k-Vektorraum erzeugt. Sei also $f \in k(X)$ dargestellt als Quotient von zwei Polynomen $f=P/Q$ mit $Q \neq 0$. Wir argumentieren mit Induktion über den Grad von Q. Ist Q konstant, so haben wir schon gewonnen. Sonst besitzt Q eine Nullstelle $\mu \in k$ und wir können schreiben $Q(x) = (X-\mu)^m \tilde{Q}(x)$ mit

$m \geq 1$ und $\tilde{Q}(\mu) \neq 0$. Dann nehmen wir $c = P(\mu)/\tilde{Q}(\mu)$ und betrachten die Funktion

$$\frac{P}{Q} - \frac{c}{(X-\mu)^m} = \frac{P - c\tilde{Q}}{(X-\mu)^m \tilde{Q}}$$

Aufgrund unserer Wahl von c hat der Zähler auf der rechten Seite eine Nullstelle bei $X = \mu$, wir können im Bruch also $(X - \mu)$ kürzen, und eine offensichtliche Induktion über dem Grad des Polynoms Q beendet den Beweis. Den Beweis der linearen Unabhängigkeit überlassen wir dem Leser zur Übung. □

2.8.14. Will man konkret eine Partialbruchzerlegung bestimmen, so rate ich dazu, mit einer Polynomdivision zu beginnen und $P = AQ + R$ zu schreiben mit Polynomen A und R derart, daß der Grad von R echt kleiner ist als der Grad von Q. Wir erhalten $P/Q = A + R/Q$, und in der Partialbruchzerlegung von R/Q tritt dann kein polynomialer Summand mehr auf. Die Polstellen-Summanden gehören dann alle zu Nullstellen von Q und ihr Grad ist beschränkt durch die Vielfachheit der entsprechenden Nullstelle von Q. Nun setzen wir die Koeffizienten unserer Linearkombination als Unbestimmte an, für die wir dann ein lineares Gleichungssystem erhalten, das wir mit den üblichen Verfahren lösen.

Beispiel 2.8.15. Wir bestimmen von $(X^4 + 2X^2)/(X^2 + 2X + 1)$ die Partialbruchzerlegung. Die Polynomdivision haben wir bereits in 2.5.16 durchgeführt und $X^4 + 2X^2 = (X^2 - 2X + 5)(X^2 + 2X + 1) - 8X - 5$ erhalten, so daß sich unser Bruch vereinfacht zu

$$\frac{X^4 + 2X^2}{X^2 + 2X + 1} = X^2 - 2X + 5 - \frac{8X + 5}{X^2 + 2X + 1}$$

Jetzt zerlegen wir den Nenner in Linearfaktoren $X^2 + 2X + 1 = (X + 1)^2$ und dürfen nach unserem Satz über die Partialbruchzerlegung

$$\frac{8X + 5}{(X+1)^2} = \frac{a}{X+1} + \frac{b}{(X+1)^2}$$

ansetzen, woraus sich ergibt $8X + 5 = aX + a + b$ und damit $a = 8$ und $b = -3$. Die Partialbruchzerlegung unserer ursprünglichen Funktion hat also die Gestalt

$$\frac{X^4 + 2X^2}{X^2 + 2X + 1} = X^2 - 2X + 5 - \frac{8}{X+1} + \frac{3}{(X+1)^2}$$

Übung 2.8.16. Man bestimme die Partialbruchzerlegung von $1/(1+X^4)$ in $\mathbb{C}(X)$.

2.8.17. Wir bilden die sogenannte **erzeugende Funktion** der Fibonacci-Folge alias die formale Potenzreihe $f(x) = \sum_{n\geq 0} f_n x^n$ mit den Fibonacci-Zahlen aus I.1.2.1 als Koeffizienten. Die Rekursionsformel für Fibonacci-Zahlen liefert unmittelbar $xf(x) + x^2 f(x) = f(x) - ax - b$ und die Anfangswerte $f_0 = 0$ und

$f_1 = 1$ liefern erst $b = 0$ und dann $a = 1$. Wir folgern $(1 - x - x^2)f(x) = x$. Umgekehrt hat jede formale Potenzreihe, die diese Identität erfüllt, die Fibonacci-Zahlen als Koeffizienten. Es gilt also, die Funktion $x/(1 - x - x^2)$ in eine Potenzreihe zu entwickeln. Dazu erinnern wir Satz 2.8.11 über die Partialbruchzerlegung, schreiben $x^2 + x - 1 = (x - \beta_+)(x - \beta_-)$ mit $\beta_\pm = -\frac{1}{2} \pm \frac{1}{2}\sqrt{5}$ und dürfen $x/(1 - x - x^2) = a/(x - \beta_+) + b/(x - \beta_-)$ ansetzen. Zur Vereinfachung der weiteren Rechnungen erinnern wir $\beta_+\beta_- = -1$ und variieren unseren Ansatz zu $x/(1 - x - x^2) = c/(1 + x\beta_-) + d/(1 + x\beta_+)$. Das führt zu $c + d = 0$ alias $c = -d$ und $\beta_+c + \beta_-d = 1$ alias $c = 1/(\beta_+ - \beta_-) = 1/\sqrt{5}$. Die Entwicklung unserer Brüche in eine geometrische Reihe nach 2.8.8 liefert damit im Ring der formalen Potenzreihen die Identität

$$\frac{x}{1 - x - x^2} = \sum_{i \geq 0} \frac{(-x\beta_-)^i}{\sqrt{5}} - \frac{(-x\beta_+)^i}{\sqrt{5}}$$

und für den Koeffizienten von x^i alias die i-te Fibonacci-Zahl f_i ergibt sich wie in I.1.2.1 die Darstellung

$$f_i = \frac{1}{\sqrt{5}} \left(\frac{1 + \sqrt{5}}{2} \right)^i - \frac{1}{\sqrt{5}} \left(\frac{1 - \sqrt{5}}{2} \right)^i$$

2.9 Quaternionen*

2.9.1. Dieser Abschnitt ist für den Rest der Vorlesung unerheblich. Allerdings gehören die Quaternionen meines Erachtens zur mathematischen Allgemeinbildung.

Definition 2.9.2. Ein **Schiefkörper** ist ein Ring R, der nicht der Nullring ist, und in dem alle von Null verschiedenen Elemente Einheiten sind. Auf englisch sagt man **skew field**, auf französisch **corps gauche**.

Satz 2.9.3 (Quaternionen). *Es gibt ein Fünftupel $(\mathbb{H}, \mathrm{i}, \mathrm{j}, \mathrm{k}, c)$ bestehend aus einem Schiefkörper $\mathbb{H}$, Elementen $\mathrm{i}, \mathrm{j}, \mathrm{k} \in \mathbb{H}$ und einem Ringhomomorphismus $c : \mathbb{R} \to \mathbb{H}$ mit $c(\lambda)q = qc(\lambda)$ $\forall \lambda \in \mathbb{R}$, $q \in \mathbb{H}$ derart, daß gilt*

$$\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = \mathrm{i}\,\mathrm{j}\,\mathrm{k} = -1$$

und daß $1, \mathrm{i}, \mathrm{j}, \mathrm{k}$ eine Basis von $\mathbb{H}$ bilden für die durch c auf $\mathbb{H}$ gegebene Struktur als $\mathbb{R}$-Vektorraum. Des weiteren ist ein derartiges Fünftupel im Wesentlichen eindeutig bestimmt in einer Weise, deren Ausformulierung dem Leser überlassen bleiben möge.

Definition 2.9.4. Wir wählen für den weiteren Verlauf der Vorlesung ein festes Fünftupel $(\mathbb{H}, \mathrm{i}, \mathrm{j}, \mathrm{k}, c)$ der im Satz beschriebenen Art mit der zusätzlichen Eigenschaft, daß c eine Inklusion als Teilmenge ist und daß sogar die davon induzierte Abbildung $\mathbb{C} \to \mathbb{H}$ mit $\mathrm{i}_{\mathbb{C}} \mapsto \mathrm{i}$ eine Inklusion als Teilmenge ist. Hier habe ich, um die Aussage zu verdeutlichen, die ausgezeichnete Wurzel aus -1 in $\mathbb{C}$ einmal etwas pedantisch $\mathrm{i}_{\mathbb{C}}$ notiert. Wegen der im zweiten Teil des Satzes formulierten "Eindeutigkeit bis auf eindeutigen Isomorphismus" erlauben wir uns den bestimmten Artikel und nennen $\mathbb{H}$ den Schiefkörper der **Quaternionen**, da er nämlich als Vektorraum über den reellen Zahlen die Dimension Vier hat, oder auch den Schiefkörper der **Hamilton'schen Zahlen** nach seinem Erfinder Hamilton. In III.3.8.2 diskutieren wir, warum und in welcher Weise $\mathbb{R}, \mathbb{C}$ und $\mathbb{H}$ bis auf Isomorphismus die einzigen Schiefkörper endlicher Dimension "über dem Körper $\mathbb{R}$" sind.

2.9.5. Hamilton war von seiner Entdeckung so begeistert, daß er eine Gedenktafel an der Dubliner Broom Bridge anbringen ließ, auf der zu lesen ist: "Here as he walked by on the 16th of October 1843 Sir William Rowan Hamilton in a flash of genius discovered the fundamental formula for quaternion multiplication $\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = \mathrm{i}\,\mathrm{j}\,\mathrm{k} = -1$ & cut it on a stone of this bridge".

Beweis. Bezeichne $\mathbb{H}$ die Menge aller komplexen 2×2-Matrizen der Gestalt

$$\mathbb{H} = \left\{ \begin{pmatrix} z & -y \\ \bar{y} & \bar{z} \end{pmatrix} \middle| z, y \in \mathbb{C} \right\} \subset \mathrm{M}(2 \times 2; \mathbb{C})$$

Die Addition und Multiplikation von Matrizen induziert offensichtlich eine Addition und Multiplikation auf $\mathbb{H}$ und wir erhalten eine Einbettung $\mathbb{C} \hookrightarrow \mathbb{H}$ vermittels $z \mapsto \mathrm{diag}(z, \bar{z})$. Das Bilden der konjugierten transponierten Matrix definiert einen Antiautomorphismus $q \mapsto \bar{q}$ von $\mathbb{H}$, in Formeln $\overline{qw} = \bar{w}\bar{q}$, und $q\bar{q}$ ist für $q \neq 0$ stets positiv und reell. Folglich ist $\mathbb{H}$ ein Schiefkörper. Wir fassen $\mathbb{C}$ meist als Teilmenge von $\mathbb{H}$ auf vermittels der eben erklärten Einbettung, aber vorerst unterscheiden wir noch zwischen den komplexen Zahlen $1_{\mathbb{C}}$, $\mathrm{i}_{\mathbb{C}}$ und den Matrizen $1 = \mathrm{diag}(1_{\mathbb{C}}, 1_{\mathbb{C}})$, $\mathrm{i} = \mathrm{diag}(\mathrm{i}_{\mathbb{C}}, -\mathrm{i}_{\mathbb{C}})$. Unser $\mathbb{H}$ hat dann über $\mathbb{R}$ die Basis $1, \mathrm{i}, \mathrm{j}, \mathrm{k}$ mit $\mathrm{i} := \mathrm{diag}(\mathrm{i}_{\mathbb{C}}, -\mathrm{i}_{\mathbb{C}})$ und

$$\mathrm{j} := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ und } \mathrm{k} := \begin{pmatrix} 0 & \mathrm{i}_{\mathbb{C}} \\ \mathrm{i}_{\mathbb{C}} & 0 \end{pmatrix}$$

und es gilt

$$\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = \mathrm{i}\,\mathrm{j}\,\mathrm{k} = -1$$

Damit ist die Existenz gezeigt und nur die Eindeutigkeit muß noch nachgewiesen werden. Zunächst beachten wir, daß wir durch Multiplikation der letzten Gleichung von rechts und links mit i bzw. k folgern können

$$\mathrm{i}\,\mathrm{j}\,\mathrm{k} = \mathrm{j}\,\mathrm{k}\,\mathrm{i} = \mathrm{k}\,\mathrm{i}\,\mathrm{j} = -1$$

Das hinwiederum liefert die Identitäten $\mathrm{i}\,\mathrm{j} = \mathrm{k}$ mit ihren zyklischen Vertauschungen. Durch Invertieren ergeben sich weiter die Identitäten $\mathrm{j}\,\mathrm{i} = -\mathrm{k}$ mit ihren zyklischen Vertauschungen, und das zeigt dann die Eindeutigkeit. □

2.9.6. Jede zyklische Vertauschung von $\mathrm{i}, \mathrm{j}, \mathrm{k}$ liefert einen Automorphismus der Quaternionen. Die Konjugation $q \mapsto \bar{q}$ aus der im Beweis gegebenen Konstruktion hat in der Basis $1, \mathrm{i}, \mathrm{j}, \mathrm{k}$ die Gestalt

$$\overline{a + b\,\mathrm{i} + c\,\mathrm{j} + d\,\mathrm{k}} = a - b\,\mathrm{i} - c\,\mathrm{j} - d\,\mathrm{k}$$

und hat wie bereits erwähnt die Eigenschaft $\overline{qw} = \bar{w}\bar{q}$. Gegeben ein Quaternion $q = a + b\,\mathrm{i} + c\,\mathrm{j} + d\,\mathrm{k}$ nennt man $a = (q + \bar{q})/2$ seinen **Realteil** und schreibt $a = \mathrm{Re}(q)$. Für $q = a + b\,\mathrm{i} + c\,\mathrm{j} + d\,\mathrm{k}$ ist $q\bar{q} = \bar{q}q = a^2 + b^2 + c^2 + d^2$ und man setzt $|q| = \sqrt{q\bar{q}}$ und nennt diese reelle Zahl den **Betrag** unseres Quaternions. Offensichtlich kann für $q \neq 0$ sein Inverses durch die Formel $q^{-1} = \bar{q}/|q|^2$ angegeben werden. Offensichtlich gilt dann $|qw| = |q||w|$ für alle $q, w \in \mathbb{H}$ und die Gruppe aller Quaternionen der Länge Eins besteht genau aus allen unitären (2×2)-Matrizen mit Determinante Eins. Darin enthalten ist die Untergruppe der acht Quaternionen $\{\pm 1, \pm \mathrm{i}, \pm \mathrm{j}, \pm \mathrm{k}\}$, die sogenannte **Quaternionengruppe**, von deren Multiplikationstabelle Hamilton bei seiner Konstruktion ausgegangen war.

Ergänzende Übung 2.9.7. Man zeige: Sind zwei natürliche Zahlen jeweils eine Summe von vier Quadraten, so auch ihr Produkt. Diese Erkenntnis ist ein wichtiger Schritt bei einem Beweis des sogenannten **Vier-Quadrate-Satzes** von Lagrange, nach dem jede natürliche Zahl eine Summe von vier Quadratzahlen ist, etwa $3 = 1^2 + 1^2 + 1^2 + 0^2$ oder $23 = 3^2 + 3^2 + 2^2 + 1^2$.

2.10 Das Signum einer Permutation

2.10.1. Wir beginnen hier mit dem Studium der sogenannten "symmetrischen Gruppen". Mehr dazu können Sie später in III.1.3 lernen.

Definition 2.10.2. Die Gruppe aller Permutationen alias bijektiven Selbstabbildungen der Menge $\{1, 2, \ldots, n\}$ notieren wir

$$\mathcal{S}_n = \mathrm{Ens}^\times\{1, 2, \ldots, n\}$$

Sie heißt auch die **n-te symmetrische Gruppe**. Nach I.2.2.27 hat diese Gruppe $n!$ Elemente, in Formeln $|\mathcal{S}_n| = n!$. Viele Autoren verwenden statt $\mathcal{S}_n$ auch die alternative Notation Σ_n. Eine Permutation, die zwei Elemente unserer Menge vertauscht und alle anderen Elemente festhält, nennt man eine **Transposition**.

Definition 2.10.3. Ein **Fehlstand** einer Permutation $\sigma \in \mathcal{S}_n$ ist ein Paar (i,j) mit $1 \leq i < j \leq n$ aber $\sigma(i) > \sigma(j)$. Die Zahl der Fehlstände heißt die **Länge** $l(\sigma)$ unserer Permutation, in Formeln

$$l(\sigma) = |\{(i,j) \mid i < j \text{ aber } \sigma(i) > \sigma(j)\}|$$

Das **Signum** einer Permutation ist definiert als die Parität der Zahl ihrer Fehlstände, in Formeln

$$\operatorname{sgn}(\sigma) = (-1)^{l(\sigma)}$$

Eine Permutation mit Signum $+1$ alias gerader Länge heißt eine **gerade Permutation**, eine Permutation mit Signum -1 alias ungerader Länge eine **ungerade Permutation**.

Beispiel 2.10.4. Die Identität von $\mathcal{S}_n$ ist jeweils die einzige Permutation der Länge Null. Die Transposition, die die Zahlen i und j vertauscht, hat die Länge $2|i-j|-1$, wie auch nebenstehendes Bild sofort zeigt, und ist also insbesondere stets ungerade.

Lemma 2.10.5. *Für jede natürliche Zahl n ist unser Signum ein Gruppenhomomorphismus $\operatorname{sgn} : \mathcal{S}_n \to \{1,-1\}$ von der symmetrischen Gruppe $\mathcal{S}_n$ in die zweielementige Gruppe der Vorzeichen, in Formeln gilt also*

$$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau) \quad \forall \sigma, \tau \in \mathcal{S}_n$$

Erster Beweis. Wir vereinbaren speziell für diesen Beweis für das Vorzeichen einer von Null verschiedenen ganzen Zahl $a \in \mathbb{Z}\backslash 0$ die Notation $[a] \in \{1,-1\}$. Damit können wir das Signum einer Permutation σ dann auch schreiben als

$$\operatorname{sgn}(\sigma) = \prod_{i<j} [\sigma(j) - \sigma(i)]$$

Für eine beliebige weitere Permutation τ finden wir dann

$$\prod_{i<j} [\sigma\tau(j) - \sigma\tau(i)] = \prod_{i<j} \frac{[\sigma(\tau(j)) - \sigma(\tau(i))]}{[\tau(j) - \tau(i)]} \prod_{i<j} [\tau(j) - \tau(i)]$$

Da nun aber für eine beliebige weitere Permutation τ auch die $\{\tau(j), \tau(i)\}$ für $i < j$ genau die zweielementigen Teilmengen von $\{1, \ldots, n\}$ durchlaufen, gilt für eine beliebige weitere Permutation τ auch die Formel

$$\operatorname{sgn}(\sigma) = \prod_{i<j} \frac{[\sigma(\tau(j)) - \sigma(\tau(i))]}{[\tau(j) - \tau(i)]}$$

Das zeigt die Behauptung. □

SkriptenBilder/Bildsgn.png

Diese Bilder illustrieren zwei mögliche Anschauungen für die Länge einer Permutation, in diesem Fall der Permutation $\sigma \in \mathcal{S}_6$ mit $1 \mapsto 2$, $2 \mapsto 4$, $3 \mapsto 1$, $4 \mapsto 5$, $5 \mapsto 3$ und $6 \mapsto 6$: Im oberen Bild ist die Länge ganz offensichtlich die "Zahl der Kreuzungen von Abbildungspfeilen", in unserem Fall haben wir also $l(\sigma) = 4$. Im unteren Bild habe ich unter jede Zahl n jeweils $\sigma(n)$ geschrieben und dann gleiche Zahlen verbunden, und hier ist ähnlich $l(\sigma) = 4$ gerade die "Zahl der Kreuzungen solcher Verbindungslinien". Der Leser sei ermutigt, sich auch die Produktformel für das Signum 2.10.5 mithilfe dieser Bilder anschaulich zu machen.

SkriptenBilder/BildFij.png

Die Transposition, die i und j vertauscht, hat genau $2|i-j|-1$ Fehlstände. Insbesondere ist jede Transposition ungerade.

Zweiter Beweis. Wir betrachten den Polynomring $\mathbb{Z}[X_1, \ldots, X_n]$ aus 2.5.32. Für jede Permutation $\sigma \in \mathcal{S}_n$ erklären wir für diesen Ring einen Ringhomomorphismus $\sigma : \mathbb{Z}[X_1, \ldots, X_n] \to \mathbb{Z}[X_1, \ldots, X_n]$ zu sich selber vermittels der Vertauschung der Variablen, in Formeln $\sigma : X_i \mapsto X_{\sigma(i)}$. Dann gilt für jedes Polynom P sicher $\tau(\sigma P) = (\tau\sigma)P$. Betrachten wir nun speziell das Polynom

$$P = \prod_{i<j}(X_i - X_j)$$

so gilt offensichtlich weiter $\sigma P = \operatorname{sgn}(\sigma)P$. Damit folgt aber unmittelbar die von der Mitte aus zu entwickelnde Gleichungskette

$$\operatorname{sgn}(\tau)\operatorname{sgn}(\sigma)P = \tau(\sigma P) = (\tau\sigma)P = \operatorname{sgn}(\tau\sigma)P$$

und daraus folgt dann die Behauptung. □

2.10.6. Für jedes n bilden die geraden Permutationen als Kern eines Gruppenhomomorphismus nach 2.2.12 eine Untergruppe von $\mathcal{S}_n$. Diese Gruppe heißt die **alternierende Gruppe** und wird A_n notiert.

Übung 2.10.7. Die Permutation $\sigma \in \mathcal{S}_n$, die i ganz nach vorne schiebt ohne die Reihenfolge der übrigen Elemente zu ändern, hat $(i-1)$ Fehlstände und folglich das Signum $\operatorname{sgn}(\sigma) = (-1)^{i-1}$.

Übung 2.10.8. Jede Permutation einer endlichen angeordneten Menge läßt sich darstellen als eine Verknüpfung von Transpositionen benachbarter Elemente.

Ergänzende Übung 2.10.9. Ist T eine endliche Menge, so gibt es genau einen Gruppenhomomorphismus

$$\operatorname{sign} : \operatorname{Ens}^\times(T) \to \{1, -1\}$$

derart, daß für jede Bijektion $\beta : \{1, \ldots, n\} \xrightarrow{\sim} T$ und alle $\tau \in \operatorname{Ens}^\times(T)$ gilt $\operatorname{sign}(\tau) = \operatorname{sgn}(\beta^{-1} \circ \tau \circ \beta)$. Wir nennen unseren Gruppenhomomorphismus auch in dieser Allgemeinheit das **Signum** und kürzen ihn wieder mit $\operatorname{sign} = \operatorname{sgn}$ ab. Auch in dieser Allgemeinheit nennen wir eine Permutation mit Signum $+1$ **gerade**, und eine Permutation mit Signum -1 **ungerade**. Es ist allerdings nicht mehr sinnvoll, in dieser Allgemeinheit von der "Länge" einer Permutation zu reden.

Übung 2.10.10. Die symmetrische Gruppe $\mathcal{S}_n$ wird erzeugt von der Transposition τ der Elemente 1 und 2 zusammen mit der "zyklischen Vertauschung" $\sigma : i \mapsto i+1$ für $1 \le i < n$ und $n \mapsto 1$. Die symmetrische Gruppe $\mathcal{S}_5$ wird erzeugt von der "zyklischen Vertauschung" und einer beliebigen weiteren Transposition τ. Mutige zeigen stärker: Die symmetrische Gruppe $\mathcal{S}_p$ für eine beliebige Primzahl p wird erzeugt von der "zyklischen Vertauschung" und einer beliebigen weiteren Transposition τ.

3 Determinanten und Eigenwerte

3.1 Die Determinante und ihre Bedeutung

Definition 3.1.1. Sei k ein Kring und $n \in \mathbb{N}$. Die **Determinante** ist die Abbildung $\det : \mathrm{M}(n \times n; k) \to k$ von den quadratischen Matrizen mit Einträgen in unserem Kring in besagten Kring selbst, die gegeben wird durch die Vorschrift

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \quad \mapsto \quad \det A = \sum_{\sigma \in \mathcal{S}_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \dots a_{n\sigma(n)}$$

Summiert wird über alle Permutationen von n, und der Vorfaktor $\operatorname{sgn}(\sigma)$ meint das Signum der Permutation σ nach 2.10.3. Unsere Formel heißt die **Leibniz-Formel**. Für den Extremfall $n = 0$ der "leeren Matrix" ist zu verstehen, daß ihr die Determinante 1 zugeordnet wird: Formal gibt es genau eine Permutation der leeren Menge, deren Signum ist Eins, und dies Signum wird multipliziert mit dem leeren Produkt, das nach unseren Konventionen auch den Wert Eins hat.

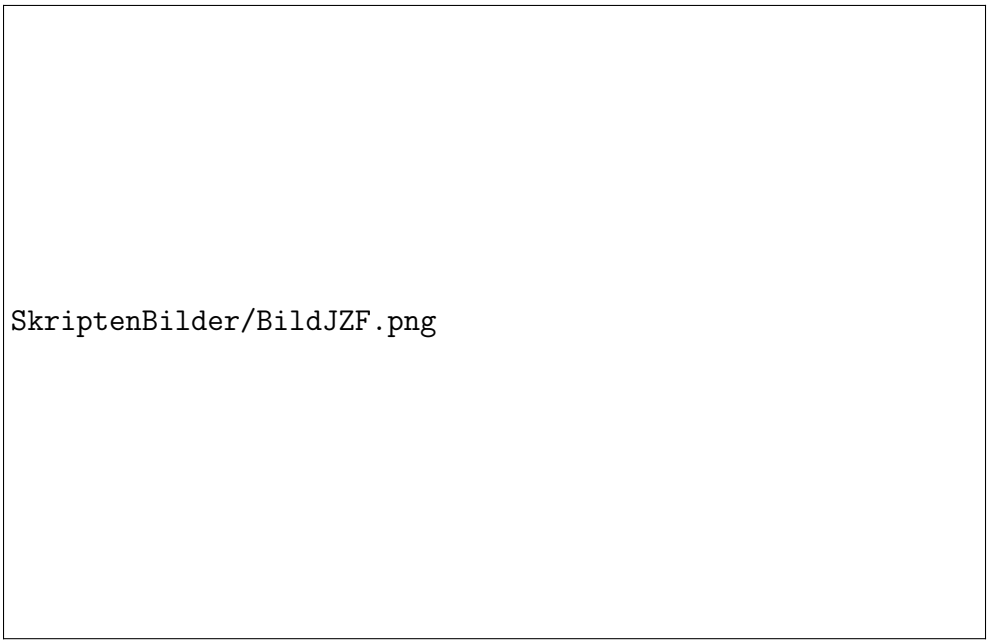
3.1.2. Wie wir in 3.4.2 sehen werden, bestimmt alias determiniert die Determinante, ob ein quadratisches lineares Gleichungssystem eindeutig lösbar ist. Daher rührt denn auch die Terminologie.

Beispiele 3.1.3. Wir erhalten etwa

$$\begin{aligned} \det(a) &= a \\ \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} &= ad - cb \\ \det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} &= \begin{array}{l} a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} \\ -a_{31}a_{22}a_{13} - a_{32}a_{23}a_{11} - a_{33}a_{21}a_{12} \end{array} \end{aligned}$$

Im Fall der (3×3)-Matrizen heißt das manchmal die **Jägerzaunformel** aus einem Grund, den die nebenstehende Abbildung illustriert. Für $n \geq 4$ macht die Berechnung der Determinante anhand der Leibniz-Formel als Summe von $n! \geq 24$ Termen keinen Spaß mehr. Wir besprechen in 3.3.8, wie man in diesen Fällen geschickter vorgehen kann.

Beispiel 3.1.4. Die Determinante einer oberen Dreiecksmatrix ist das Produkt ihrer Diagonaleinträge. In der Tat ist die Identität die einzige Permutation σ mit $\sigma(i) \leq i$ für alle i, folglich trägt im Fall einer oberen Dreiecksmatrix in der Leibniz-Formel nur der Summand mit $\sigma = \mathrm{id}$ zur Determinante bei. Dasselbe gilt für untere Dreiecksmatrizen.



Um die Determinante einer (3×3)-Matrix zu berechnen mag man die erste und zweite Spalte danebenschreiben und dann die Produkte der drei Dreierdiagonalen nach rechts unten addieren und davon die Produkte der drei Dreierdiagonalen nach rechts oben abziehen. Diese Eselsbrücke heißt auch die "Jägerzaunformel". Für (4×4)-Matrizen liefert aber die analoge Regel nicht mehr die Determinante!

Die Determinante einer Block-oberen-Dreiecksmatrix ist, wie Sie in Übung 4.5.7 zeigen, das Produkt der Determinanten ihrer Blöcke auf der Diagonalen. Dieses Bild illustriert den Fall von nur zwei Blöcken auf der Diagonalen. Das Symbol unten links ist eine Null.

Übung 3.1.5. Die Determinante einer Block-oberen-Dreiecksmatrix ist das Produkt der Determinanten ihrer Blöcke auf der Diagonalen. Hinweis: Man variiere das Argument für 3.1.4.

3.1.6 (**Betrag der Determinante und Volumen**). Vor der weiteren Entwicklung der Theorie will ich nun zuerst einmal die anschauliche Bedeutung der Determinante einer Matrix mit reellen Einträgen diskutieren. Ich beginne mit der anschauliche Bedeutung des Betrags der Determinante und beschränke mich dazu zunächst auf den Fall $n = 2$. Hoffentlich ist anschaulich klar, daß jede lineare Abbildung $L : \mathbb{R}^2 \to \mathbb{R}^2$ einen "Volumenverzerrungsfaktor" haben sollte, daß es also dazu eine reelle Konstante $c(L) \geq 0$ geben sollte derart, daß "das Bild unter L eines Flächenstücks U der Fläche $\mathrm{vol}(U)$ die Fläche $\mathrm{vol}(LU) = c(L)\,\mathrm{vol}(U)$ hat". Formal zeigt das die Transformationsformel **??**, die für besagte Konstante auch gleich die Formel

$$c(L) = |\det L|$$

liefert. Ich will diese Formel im folgenden heuristisch begründen. Anschaulich ist hoffentlich klar, daß unser $c : \mathrm{M}(2 \times 2; \mathbb{R}) \to \mathbb{R}_{\geq 0}$ die folgenden Eigenschaften haben sollte:

1. Es sollte "multiplikativ" sein, in Formeln $c(LM) = c(L)c(M)$;
2. Die Streckung einer Achse sollte die Fläche eines Flächenstücks genau durch Multiplikation mit dem Betrag des Streckfaktors ändern, in Formeln $c(\mathrm{diag}(a, 1)) = c(\mathrm{diag}(1, a)) = |a|$;
3. Scherungen sollten die Fläche eines Flächenstücks nicht ändern, in Formeln $c(D) = 1$ für D eine obere oder untere Dreiecksmatrix mit Einsen auf der Diagonale.

Da sich nun nach 1.9.6 jede Matrix als Produkt von Elementarmatrizen darstellen läßt, kann es höchstens eine Abbildung $c : \mathrm{M}(2 \times 2; \mathbb{R}) \to \mathbb{R}_{\geq 0}$ geben, die diese drei Eigenschaften hat. In 3.4.1 werden wir für unsere Determinante die "Multiplikationsformel" $\det(LM) = \det(L)\det(M)$ zeigen, und zusammen mit unserer Formel 3.1.4 für die Determinante einer oberen oder unteren Dreiecksmatrix wird dann auch umgekehrt klar, daß $M \mapsto |\det M|$ eine Abbildung mit unseren drei Eigenschaften ist. Das beendet unsere heuristische Argumentation für die Stichhaltigkeit der Anschauung $|\det L| = c(L)$ für den Betrag der Determinante von (2×2)-Matrizen. In höheren Dimensionen liefert dieselbe Argumentation analoge Resultate, insbesondere kann der Betrag der Determinante einer (3×3)-Matrix aufgefaßt werden als der Faktor, um den die zugehörige lineare Abbildung Volumina ändert. Damit sollte auch anschaulich klar werden, warum $\det L \neq 0$ gleichbedeutend ist zur Invertierbarkeit von L, was wir im allgemeinen als 3.4.2 zeigen.

3.1.7 (**Vorzeichen der Determinante und Drehsinn**). Das Vorzeichen der Determinante einer invertierbaren reellen (2×2)-Matrix zeigt anschaulich gesprochen an, "ob die dadurch gegebene lineare Selbstabbildung der Ebene $\mathbb{R}^2$ den Drehsinn erhält oder umkehrt". Formal ist das vielleicht am ehesten in **??** enthalten, und im Fall allgemeiner angeordneter Körper wird diese anschauliche Erkenntnis ihrerseits unsere Definition 3.2.2 einer "Orientierung" auf einem Vektorraum über einem angeordneten Körper motivieren. Um die Beziehung zwischen Drehsinn und Determinante heuristisch zu begründen, können wir ähnlich argumentieren wie zuvor: Zunächst einmal führen wir ganz heuristisch eine angepaßte Notation ein und erklären für eine invertierbare lineare Abbildung $L : \mathbb{R}^2 \xrightarrow{\sim} \mathbb{R}^2$ das Vorzeichen $\varepsilon(L)$ durch die Vorschrift

$$\varepsilon(L) = \begin{cases} 1 & L \text{ erhält den Drehsinn;} \\ -1 & L \text{ kehrt den Drehsinn um.} \end{cases}$$

Vereinbaren wir speziell für diesen Beweis die Notation $[a]$ für das Vorzeichen einer von Null verschiedenen reellen Zahl, so können wir unsere Behauptung schreiben als die Formel

$$\varepsilon(L) = [\det L]$$

Ich will diese Formel im folgenden heuristisch begründen. Anschaulich ist hoffentlich klar, daß unser $\varepsilon : \mathrm{GL}(2;\mathbb{R}) \to \{1,-1\}$ die folgenden Eigenschaften haben sollte:

1. Es sollte "multiplikativ" sein, in Formeln $\varepsilon(LM) = \varepsilon(L)\varepsilon(M)$;
2. Die Streckung einer Achse sollte den Drehsinn genau durch die Multiplikation mit dem Vorzeichen des Streckfaktors ändern, in Formeln $\varepsilon(\mathrm{diag}(a,1)) = \varepsilon(\mathrm{diag}(1,a)) = [a]$;
3. Scherungen sollten den Drehsinn nicht ändern, in Formeln $\varepsilon(D) = 1$ für D eine obere oder untere Dreiecksmatrix mit Einsen auf der Diagonale.

Da sich nun nach 1.9.6 jede Matrix als Produkt von Elementarmatrizen darstellen läßt, kann es höchstens eine Abbildung $\varepsilon : \mathrm{GL}(2;\mathbb{R}) \to \{1,-1\}$ geben, die diese drei Eigenschaften hat. In 3.4.1 werden wir für unsere Determinante die "Multiplikationsformel" $\det(LM) = \det(L)\det(M)$ zeigen, und zusammen mit unserer Formel 3.1.4 für die Determinante einer oberen oder unteren Dreiecksmatrix wird dann andererseits auch klar, daß $M \mapsto [\det M]$ eine Abbildung mit unseren drei Eigenschaften ist. Das beendet unsere heuristische Argumentation für die Stichhaltigkeit der Anschauung $[\det L] = \varepsilon(L)$ für das Vorzeichen der Determinante von (2×2)-Matrizen. In höheren Dimensionen liefert dieselbe Argumentation analoge Resultate, etwa zeigt das Vorzeichen der Determinante einer invertierbaren Abbildung $L : \mathbb{R}^3 \to \mathbb{R}^3$ an, ob sie die "Händigkeit" erhält oder vielmehr "Rechtsgewinde und Linksgewinde vertauscht".

Ergänzung 3.1.8. Amüsant ist in diesem Zusammenhang die naive Frage, warum ein Spiegel "rechts und links vertauscht, aber nicht oben und unten". Die korrekte Antwort lautet, daß ein Spiegel ebensowenig rechts und links vertauscht wie oben und unten, sondern vielmehr vorne und hinten. Wir versuchen nur unbewußt, uns so gut wie möglich mit unserem Spiegelbild zu identifizieren, indem wir hinter den Spiegel treten, in Formeln also durch eine $180°$-Drehung im Raum um eine geeignete vertikale Achse, die vertikal im Spiegel verläuft. Dann stellen wir fest, daß das zwar fast gelingt aber nicht ganz, und daß genauer die Verknüpfung der Spiegelung am Spiegel mit dieser Drehung gerade eine Spiegelung ist, die rechts und links vertauscht.

3.2 Orientierungen

3.2.1. Wir verwandeln unsere anschauliche Interpretation 3.1.7 des Vorzeichens der Determinante nun in eine formale Definition.

Definition 3.2.2. Eine **Orientierung eines endlichdimensionalen Vektorraums** V über einem angeordneten Körper ist eine Vorschrift ε, die jeder angeordneten Basis B unseres Vektorraums ein Vorzeichen $\varepsilon(B) \in \{+1, -1\}$ zuordnet und zwar so, daß für je zwei angeordnete Basen B, B' die Determinante der Basiswechselmatrix das Vorzeichen $\varepsilon(B)\varepsilon(B')$ hat. Das Vorzeichen $\varepsilon(B)$ nennen wir dann die **Orientierung** der angeordneten Basis B unseres orientierten Vektorraums. Eine angeordnete Basis der Orientierung $+1$ nennen wir eine **orientierte Basis**. Sprechen wir von der **durch eine angeordnete Basis gegebene Orientierung**, so meinen wir diejenige Orientierung, die besagter Basis das Vorzeichen $+1$ zuordnet. Ein Isomorphismus von orientierten endlichdimensionalen Vektorräumen heißt **orientierungserhaltend** genau dann, wenn er die Orientierung von angeordneten Basen erhält. Andernfalls heißt er **orientierungsumkehrend**. Gegeben ein angeordneter Körper k bezeichnen wir diejenige Orientierung des k^n als die **Standardorientierung**, die der Standardbasis das Vorzeichen $+1$ zuordnet.

Definition 3.2.3. Unter einer **Orientierung eines endlichdimensionalen affinen Raums** über einem angeordneten Körper verstehen wir eine Orientierung seines Richtungsraums. Ein Isomorphismus endlichdimensionaler affiner Räume heißt **orientierungserhaltend** bzw. **orientierungsumkehrend** genau dann, wenn ihr linearer Anteil die fragliche Eigenschaft hat.

Bemerkung 3.2.4. In der Literatur findet man vielfach eine Variante der Definition der Orientierung, bei der eine Orientierung eines reellen Vektorraums als eine Äquivalenzklasse von Basen unter einer geeigneten Äquivalenzrelation erklärt wird. Diese Definition liefert dasselbe in allen Fällen mit Ausnahme des Nullraums, und in diesem Fall scheint mir die hier gegebene Definition, die auch dem

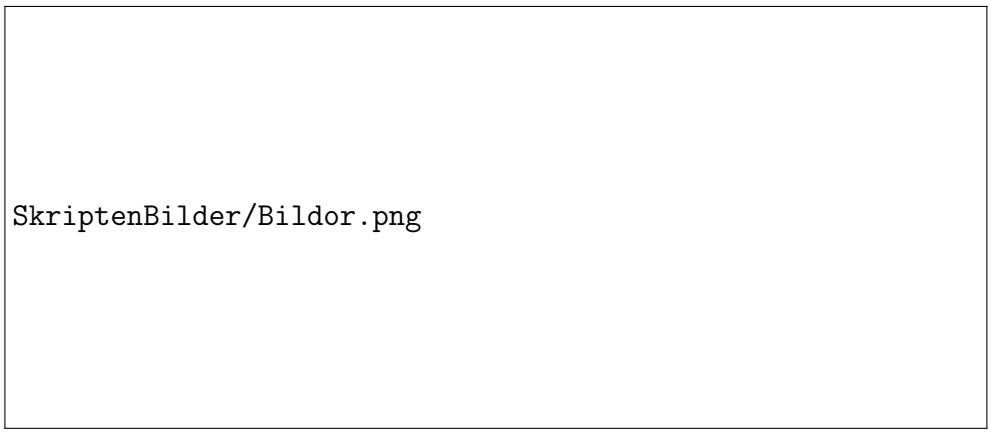
Nullraum zwei verschiedene Orientierungen erlaubt, das sinnvollere Konzept zu liefern: Diese Definition erlaubt es nämlich, den Hauptsatz der Differential- und Integralrechnung auch formal als Spezialfall des Satzes von Stokes anzusehen, vergleiche **??**.

3.2.5. Jeder endlichdimensionale Raum über einem angeordneten Körper besitzt genau zwei Orientierungen. Das gilt insbesondere auch für jeden einpunktigen Raum: Hier verwenden wir die Konvention, nach der der einzige Endomorphismus des Nullvektorraums die Determinante 1 hat. Der Nullvektorraum hat eine einzige angeordnete Basis, nämlich die leere Menge mit ihrer einzigen Anordnung, und eine Orientierung des Nullvektorraums zu wählen bedeutet schlicht, das Vorzeichen auszusuchen, das dieser Basis zugeordnet werden soll.

Beispiel 3.2.6. Eine Orientierung einer reellen Gerade anzugeben bedeutet anschaulich, auf dieser Gerade eine "Richtung" auszuwählen, eben die Richtung, in die diejenigen Vektoren zeigen, die positiv orientierte Basen ihres Richtungsraums bilden. Wir nennen diese Vektoren dann auch kurzerhand **positiv orientierte Vektoren** oder noch kürzer **positive Vektoren** und denken uns unsere Gerade mit der Anordnung versehen, für die die Addition positiver Vektoren Elemente vergrößert. Mit diesen Konventionen können wir für einen orientierten eindimensionalen Vektorraum L die Menge der positiven Vektoren mit $L_{>0}$ bezeichnen. Analog vereinbaren wir für die Elemente von $L_{<0}$ die Bezeichnung **negative Vektoren** und nennen folgerichtig die Elemente von $L_{\geq 0}$ die **nichtnegativen Vektoren**.

Ergänzende Übung 3.2.7. Sei V ein Vektorraum und L ein eindimensionaler orientierter Vektorraum. Jeder Orientierung auf V ordnen wir dann diejenige Orientierung auf $V \otimes L$ zu, für die gegeben ein positiv orientierter Vektor $l \in L$ und eine angeordnete Basis $(v_1, \ldots, v_n)$ von V der angeordneten Basis $(v_1 \otimes l, \ldots, v_n \otimes l)$ von $V \otimes L$ dasselbe Vorzeichen zugeordnet wird. Man zeige nun, daß für V von gerader Dimension die so auf $V \otimes L$ erklärte Orientierung von der auf L gewählten Orientierung gar nicht abhängt.

Beispiel 3.2.8. Denken wir uns die Tafelebene als einen zweidimensionalen reellen affinen Raum, so dürfen wir uns eine Orientierung der Tafelebene als die Auszeichnung eines Drehsinns denken, nämlich den Drehsinn derart, daß bei Drehung in diesem Drehsinn der erste Vektor einer positiv orientierten angeordneten Basis ihres Richtungsraums zuerst in ein positives Vielfaches des zweiten Vektors gedreht wird und erst dann in ein negatives Vielfaches. Wenn, wie etwa bei der Tafelebene oder bei einem vor uns liegenden Blatt Papier, zusätzlich festlegt ist, "von welcher Seite man auf eine Ebene gucken soll", so mag man diese beiden Orientierungen als "im Uhrzeigersinn" und "im Gegenuhrzeigersinn" ansprechen. Ist unsere Ebene dahingegen eine Glasscheibe und die Betrachter stehen auf beiden Seiten, so legt man eine Orientierung besser fest, indem man einen Drehsinn mit einem Wachsstift einzeichnet.



Angeordnete Basen des Raums der Richtungsvektoren der Papierebene mit den Vorzeichen, die der Orientierung “im Gegenuhrzeigersinn” entsprechen

Definition 3.2.9. Wir fixieren von nun an ein für allemal einen eindimensionalen orientierten reellen affinen Raum

$$\mathbb{T}$$

und nennen ihn die **mathematische Zeit** oder kurz **Zeit**.

3.2.10. Ich denke mir $\mathbb{T}$ als die Menge aller Zeitpunkte und denke mir die ausgezeichnete Orientierung in der Weise, daß jeder Richtungsvektor, der einen Zeitpunkt auf einen "späteren" Zeitpunkt schiebt, eine positiv orientierte Basis bildet. Das mag aber jeder halten wie er will, Sie dürfen etwa bei den Elementen von $\mathbb{T}$ etwa auch an unendlich viele verschiedene Gemüse denken, oder an was auch immer. Den Richtungsraum $\vec{\mathbb{T}}$ bezeichnen wir als den Raum aller **Zeitspannen**, seine positiv orientierten Vektoren nennen wir **Zeiteinheiten**. Sie modellieren die Zeiteinheiten der Physik: Dort wählt man üblicherweise eine feste Zeiteinheit, die **Sekunde** $\mathrm{s} \in \vec{\mathbb{T}}$. Die Einteilung eines Tages in vierundzwanzig Stunden und die Einteilung dieser Stunden in je sechzig Minuten geht wohl auf die Babylonier zurück, die angeblich mit ihren Händen bis 60 zählten, indem sie mit jedem der 5 Finger der rechten Hand der Reihe nach die 12 Fingerglieder der linken Hand an den Fingern mit Ausnahme des Daumens berührten. Die Einteilung jeder Minute in wiederum 60 Sekunden bot sich dann als natürliche Verfeinerung an.

3.2.11. Jede Orientierung auf einem Vektorraum induziert eine Orientierung auf seinem Dualraum vermittels der Vorschrift, daß die Duale einer orientierten Basis eine orientierte Basis des Dualraums sein soll. Die Elemente des positiven Teils $\vec{\mathbb{T}}^\top_{>0}$ des Dualraums des Raums $\vec{\mathbb{T}}$ der Zeitspannen mag man **Frequenzen** nennen. Eine solche Frequenz ist etwa der einzige Vektor $\mathrm{s}^\top$ der dualen Basis zur orientierten Basis $\mathrm{s} \in \vec{\mathbb{T}}$. Statt $\mathrm{s}^\top$ schreibt man meist s^{-1} oder Hz und nennt diese Frequenz ein **Hertz** nach dem Physiker Heinrich Rudolf Hertz.

Ergänzung 3.2.12. Zwei angeordnete Basen eines endlichdimensionalen reellen Vektorraums liefern dieselbe Orientierung genau dann, wenn sie sich "stetig ineinander deformieren lassen" alias in derselben "Wegzusammenhangskomponente" im Sinne von **??** des Raums aller angeordneten Basen liegen. Man kann sich davon etwa mithilfe der Iwasawa-Zerlegung 4.3.28 überzeugen. Auch die präzise Formulierung und der formale Beweis wird Ihnen davon ausgehend leicht gelingen, sobald Sie in der Analysis die Grundtatsachen über Stetigkeit in mehreren Veränderlichen kennengelernt haben. Eine äquivalente Aussage dürfen Sie in der Analysis als Übung **??** zeigen.

Ergänzung 3.2.13. Gegeben ein endlichdimensionaler Vektorraum V über einem angeordneten Körper erklären wir seine **Orientierungsmenge** $\mathrm{or}(V)$ als die zweielementige Menge seiner beiden Orientierungen. Jeder Vektorraumisomorphismus $A : V \xrightarrow{\sim} W$ liefert eine Bijektion $\mathrm{or}(A) : \mathrm{or}(V) \xrightarrow{\sim} \mathrm{or}(W)$ vermittels der von A

zwischen den Mengen der angeordneten Basen beider Räume induzierten Bijektion. Es gilt $\mathrm{or}(A \circ B) = \mathrm{or}(A) \circ \mathrm{or}(B)$ und $\mathrm{or}(\mathrm{id}) = \mathrm{id}$.

3.3 Charakterisierung der Determinante

Definition 3.3.1. Seien V, U Vektorräume über einem Körper k. Eine bilineare Abbildung $F : V \times V \to U$ heißt **symmetrisch** genau dann, wenn gilt

$$F(v, w) = F(w, v) \quad \forall v, w \in V$$

Im Fall eines Grundkörpers k mit $1_k + 1_k \neq 0_k$ alias $\mathrm{char}\, k \neq 2$ heißt sie "alternierend" genau dann, wenn gilt $F(v, w) = -F(w, v) \quad \forall v, w \in V$. Um auch den Fall eines Grundkörpers der Charakteristik $\mathrm{char}\, k = 2$ korrekt einzubinden, müssen wir uns bei unserer endgültigen Definition allerdings von der ursprünglichen Bedeutung des Wortes "alternierend" entfernen und nennen im allgemeinen eine bilineare Abbildung $F : V \times V \to U$ **alternierend** genau dann, wenn gilt

$$F(v, v) = 0 \quad \forall v \in V$$

3.3.2. Gegeben eine bilineare Abbildung $F : V \times V \to U$ mit der Eigenschaft $F(v, v) = 0 \quad \forall v \in V$, die also im Sinne unserer Definition 3.3.1 alternierend ist, gilt stets

$$F(v, w) = -F(w, v) \quad \forall v, w \in V$$

In der Tat haben wir

$$\begin{aligned} 0 &= F(v + w, v + w) \\ &= F(v, v + w) + F(w, v + w) \\ &= F(v, v) + F(v, w) + F(w, v) + F(w, v) \\ &= F(v, w) + F(w, v) \end{aligned}$$

Gilt umgekehrt $F(v, w) = -F(w, v) \quad \forall v, w \in V$, so folgt $F(v, v) = -F(v, v)$ alias $(1_k + 1_k)F(v, v) = 0_k$ für alle $v \in V$, und haben wir $1_k + 1_k \neq 0_k$ alias $\mathrm{char}\, k \neq 2$, so folgt daraus auch wieder $F(v, v) = 0$.

Definition 3.3.3. Seien $V_1, \ldots, V_n, W$ Vektorräume über einem Körper k. Eine Abbildung $F : V_1 \times \ldots \times V_n \to W$ heißt **multilinear** genau dann, wenn für alle j und alle für $i \neq j$ beliebig aber fest gewählten $v_i \in V_i$ die Abbildung $V_j \to W$, $v_j \mapsto F(v_1, \ldots, v_j, \ldots, v_n)$ linear ist. Im Fall $n = 2$ sind das genau unsere bilinearen Abbildungen aus 1.5.26.

Übung 3.3.4. Gegeben Vektorräume $V_1, V_2, \ldots, V_n, W$ über einem festen Körper bezeichne $\mathrm{Hom}^{(n)}(V_1 \times V_2 \times \ldots \times V_n, W)$ die Menge aller multilinearen Abbildungen $V_1 \times V_2 \times \ldots \times V_n \to W$. Man zeige: Ist $B_i \subset V_i$ jeweils eine Basis, so liefert die Restriktion eine Bijektion

$$\mathrm{Hom}^{(n)}(V_1 \times \ldots \times V_n, W) \xrightarrow{\sim} \mathrm{Ens}(B_1 \times \ldots \times B_n, W)$$

Jede multilineare Abbildung ist also festgelegt und festlegbar durch die Bilder von Tupeln von Basisvektoren. Den Spezialfall $n = 1$ kennen wir bereits aus 1.5.13, den Spezialfall $n = 2$ aus 1.5.27.

Definition 3.3.5. Seien V, W Vektorräume über einem Körper k. Eine multilineare Abbildung $F : V \times \ldots \times V \to W$ heißt **alternierend** genau dann, wenn sie auf jedem n-Tupel verschwindet, in dem zwei Einträge übereinstimmen, wenn also in Formeln gilt

$$(\exists i \neq j \text{ mit } v_i = v_j) \quad \Rightarrow \quad F(v_1, \ldots, v_i, \ldots, v_j, \ldots v_n) = 0$$

Das impliziert, daß sich das Vorzeichen von F ändert, wann immer man zwei Einträge vertauscht, in Formeln

$$F(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_n) = -F(v_1, \ldots, v_j, \ldots, v_i, \ldots, v_n)$$

und im Fall eines Grundkörpers einer von Zwei verschiedenen Charakteristik erhält man in derselben Weise, wie wir es in 3.3.2 für bilineare Abbildungen ausgeführt haben, auch die umgekehrte Implikation.

Satz 3.3.6 (Charakterisierung der Determinante). *Ist k ein Körper, so ist die Determinante die einzige Abbildung*

$$\det : \mathrm{M}(n \times n; k) \to k$$

die (1) multilinear und alternierend ist als Funktion der n Spaltenvektoren und die (2) der Einheitsmatrix die Eins zuordnet.

Beweis. Daß unsere in 3.1.1 durch die Leibniz-Formel definierte Determinante multilinear ist und der Einheitsmatrix die Eins zuordnet, scheint mir offensichtlich. Stimmen weiter zwei Spalten einer Matrix überein, so verschwindet ihre Determinante, denn für $\tau \in \mathcal{S}_n$ die Transposition der entsprechenden Indizes gilt $a_{1\sigma(1)} \ldots a_{n\sigma(n)} = a_{1\tau\sigma(1)} \ldots a_{n\tau\sigma(n)}$ und $\mathrm{sgn}(\sigma) = -\mathrm{sgn}(\tau\sigma)$, so daß sich in der Leibniz-Formel die entsprechenden Terme gerade wegheben. Unsere durch die Leibniz-Formel gegebene Abbildung hat also die geforderten Eigenschaften, und es gilt nur noch zu zeigen, daß es keine weiteren Abbildungen $d : \mathrm{M}(n \times n; k) \to k$

mit den besagten Eigenschaften gibt. Nach 3.3.4 kennen wir aber unsere multilineare Abbildung d bereits, wenn wir ihre Werte

$$d(\mathrm{e}_{\sigma(1)}|\dots|\mathrm{e}_{\sigma(n)})$$

kennen für alle Abbildungen $\sigma : \{1,\dots,n\} \to \{1,\dots,n\}$. Ist d zusätzlich alternierend, so gilt $d(\mathrm{e}_{\sigma(1)}|\dots|\mathrm{e}_{\sigma(n)}) = 0$, falls σ nicht injektiv ist, und $d(\mathrm{e}_{\sigma\tau(1)}|\dots|\mathrm{e}_{\sigma\tau(n)}) = -d(\mathrm{e}_{\sigma(1)}|\dots|\mathrm{e}_{\sigma(n)})$ für jede Transposition τ. Mit 2.10.8 folgt daraus

$$d(\mathrm{e}_{\sigma(1)}|\dots|\mathrm{e}_{\sigma(n)}) = \begin{cases} \operatorname{sgn}(\sigma) d(\mathrm{e}_1|\dots|\mathrm{e}_n) & \sigma \in \mathcal{S}_n; \\ 0 & \text{sonst,} \end{cases}$$

und erfüllt d dann auch noch unsere Bedingung $d(\mathrm{e}_1|\dots|\mathrm{e}_n) = 1$ für die Determinante der Einheitsmatrix, so folgt mit 3.3.4 sofort $d = \det$. □

3.3.7. Im allgemeinen folgt über einem beliebigen Körper k mit den Argumenten des vorhergehenden Beweises für jede Abbildung $d : \mathrm{M}(n \times n; k) \to k$, die multilinear und alternierend ist als Funktion der n Spaltenvektoren, die Formel

$$d = d(\mathrm{e}_1|\dots|\mathrm{e}_n) \det$$

Das brauchen wir für den vorhergehenden Beweis zwar schon gar nicht mehr zu wissen, aber es wird sich beim Beweis der Multiplikativität der Determinante als hilfreich erweisen.

3.3.8 (**Berechnung der Determinante**). Will man die Determinante einer Matrix explizit ausrechnen, so empfiehlt es sich bei größeren Matrizen, sie zunächst mit dem Gauß-Algorithmus in Zeilenstufenform zu bringen: Addieren wir ein Vielfaches einer Zeile zu einer anderen, ändert sich die Determinante nach 3.3.6 ja nicht, und vertauschen wir zwei Zeilen, so ändert sich nur ihr Vorzeichen. Bei einer Matrix in Zeilenstufenform ist dann nach 3.1.4 die Determinante schlicht das Produkt der Diagonaleinträge.

Übung 3.3.9. Gegeben ein Körper k und ein k-Vektorraum der endlichen Dimension $\dim V = n$ ist der Raum der alternierenden multilinearen Abbildungen $V^n \to k$ eindimensional.

3.4 Rechenregeln für Determinanten

Satz 3.4.1 (Multiplikativität der Determinante). *Sei k ein Kring. Gegeben quadratische Matrizen $A, B \in \mathrm{M}(n \times n; k)$ gilt*

$$\det(AB) = (\det A)(\det B)$$

Erster Beweis. Wir notieren $\mathcal{T}_n := \mathrm{Ens}(\{1,\ldots,n\})$ die Menge aller Abbildungen $\kappa : \{1,\ldots,n\} \to \{1,\ldots,n\}$ und rechnen

$$\begin{aligned}
\det(AB) &= \textstyle\sum_\sigma \operatorname{sgn}(\sigma) \prod_i (AB)_{i\sigma(i)} \\
&= \textstyle\sum_\sigma \operatorname{sgn}(\sigma) \prod_i \sum_j a_{ij} b_{j\sigma(i)} \\
&= \textstyle\sum_{\sigma\in\mathcal{S}_n,\, \kappa\in\mathcal{T}_n} \operatorname{sgn}(\sigma) a_{1\kappa(1)} b_{\kappa(1)\sigma(1)} \ldots a_{n\kappa(n)} b_{\kappa(n)\sigma(n)} \\
&= \textstyle\sum_{\kappa\in\mathcal{T}_n} a_{1\kappa(1)} \ldots a_{n\kappa(n)} \sum_{\sigma\in\mathcal{S}_n} \operatorname{sgn}(\sigma) b_{\kappa(1)\sigma(1)} \ldots b_{\kappa(n)\sigma(n)} \\
&= \textstyle\sum_{\kappa\in\mathcal{T}_n} a_{1\kappa(1)} \ldots a_{n\kappa(n)} \det(B_\kappa)
\end{aligned}$$

wo B_κ diejenige Matrix bezeichnet, deren Zeilen der Reihe nach die Zeilen mit den Indizes $\kappa(1),\ldots,\kappa(n)$ der Matrix B sind. Aus 3.3.6 folgt aber $\det B_\kappa = 0$ falls $\kappa \notin \mathcal{S}_n$ und $(\det B_\kappa) = \operatorname{sgn}(\kappa)(\det B)$ falls $\kappa \in \mathcal{S}_n$. Damit erhalten wir dann $\det(AB) = (\det A)(\det B)$ wie gewünscht. □

Zweiter Beweis im Körperfall. Die Formel ist klar, wenn eine der beiden Matrizen eine Elementarmatrix ist, also eine Matrix, die sich von der Einheitsmatrix in höchstens einem Eintrag unterscheidet. Sie folgt im allgemeinen, da nach 1.9.6 jede Matrix ein Produkt von Elementarmatrizen ist. □

Dritter Beweis im Körperfall. Man hält die Matrix A fest und betrachtet die beiden Abbildungen $\mathrm{M}(n\times n;K) \to K$ gegeben durch $B \mapsto \det(A)\det(B)$ und $B \mapsto \det(AB)$. Beide sind multilinear und alternierend als Funktion der Spalten von B, und beide ordnen der Einheitsmatrix $B = I$ den Wert $\det(A)$ zu. Aus 3.3.7 folgt damit unmittelbar, daß unsere beiden Abbildungen übereinstimmen. □

Vierter Beweis im Körperfall. Im Rahmen der Multilinearformen geben wir einen alternativen Beweis in **??** sowie ähnlich aber komplizierter in 9.5.20. □

Satz 3.4.2 (Determinantenkriterium für Invertierbarkeit). *Die Determinante einer quadratischen Matrix mit Einträgen in einem Körper ist von Null verschieden genau dann, wenn unsere Matrix invertierbar ist.*

Beweis. In Formeln behaupten wir für einen Körper K und eine beliebige Matrix $A \in \mathrm{M}(n\times n;K)$ also

$$\det A \neq 0 \quad\Leftrightarrow\quad A \text{ invertierbar}$$

Ist A invertierbar, so gibt es eine Matrix $B = A^{-1}$ mit $AB = I$. Mit der Multiplikationsformel folgt $(\det A)(\det B) = \det I = 1$ und folglich $\det A \neq 0$. Das zeigt die Implikation $\Leftarrow$. Ist A nicht invertierbar, so hat A nicht vollen Rang, die Familie der Spaltenvektoren von A ist demnach linear abhängig. Wir können also einen Spaltenvektor, ohne Beschränkung der Allgemeinheit den Ersten, durch

die Anderen ausdrücken, etwa $a_{*1} = \lambda_2 a_{*2} + \ldots + \lambda_n a_{*n}$. Dann folgt jedoch unmittelbar

$$\begin{aligned}\det A &= \det(\lambda_2 a_{*2} + \ldots + \lambda_n a_{*n} | a_{*2} | \ldots | a_{*n}) \\ &= \lambda_2 \det(a_{*2} | a_{*2} | \ldots | a_{*n}) + \ldots + \lambda_n \det(a_{*n} | a_{*2} | \ldots | a_{*n}) \\ &= \lambda_2 0 + \ldots + \lambda_n 0 \\ &= 0\end{aligned}$$

da unsere Determinante ja multilinear und alternierend ist. Damit ist auch die andere Implikation $\Rightarrow$ gezeigt. □

Ergänzende Übung 3.4.3. Man zeige die Formel für die **van-der-Monde-Determinante**

$$\det \begin{pmatrix} 1 & X_0 & X_0^2 & \ldots & X_0^n \\ \vdots & & & & \vdots \\ 1 & X_n & X_n^2 & \ldots & X_n^n \end{pmatrix} = \prod_{0 \le j < i \le n} (X_i - X_j)$$

Hinweis: Man mag von 2.5.39 und dem Fall des Grundkörpers $\mathbb{Q}$ ausgehen.

3.4.4. Aus der Multiplikationsformel folgt sofort $\det(A^{-1}) = (\det A)^{-1}$ für jede invertierbare Matrix A und damit ergibt sich für jede weitere quadratische Matrix B die Identität $\det(A^{-1}BA) = \det B$. Nach 1.10.9 hängt folglich für einen Endomorphismus $f : V \to V$ eines endlichdimensionalen Vektorraums über einem Körper k die Determinante einer darstellenden Matrix nicht von der Wahl der zur Darstellung gewählten angeordneten Basis ab, in Formeln gilt also $\det({}_{\mathcal{B}}[f]_{\mathcal{B}}) = \det({}_{\mathcal{A}}[f]_{\mathcal{A}})$ für je zwei angeordnete Basen $\mathcal{A}$ und $\mathcal{B}$ von V. Diesen Skalar notieren wir von nun an

$$\det f = \det(f|V) = \det_k(f|V)$$

und nennen ihn die **Determinante des Endomorphismus** f. Dem einzigen Automorphismus des Nullraums ist insbesondere die Determinante 1 zuzuordnen.

Definition 3.4.5. Gegeben ein endlichdimensionaler Vektorraum V über einem Körper k bilden die Automorphismen von V mit Determinante Eins eine Untergruppe der Gruppe aller Automorphismen von V. Sie heißt die **spezielle lineare Gruppe** und wird

$$\mathrm{SL}(V) \subset \mathrm{GL}(V)$$

notiert. Im Fall $V = k^n$ schreibt man auch $\mathrm{SL}(n;k) \subset \mathrm{GL}(n;k)$.

Ergänzende Übung 3.4.6. Jeder komplexe Vektorraum V kann auch als reeller Vektorraum aufgefaßt werden. Man zeige im endlichdimensionalen Fall die Formel $\det_{\mathbb{R}}(f|V) = |\det_{\mathbb{C}}(f|V)|^2$.

Lemma 3.4.7. *Die Determinante einer Matrix ändert sich nicht beim Transponieren, in Formeln*

$$\det A^\top = \det A$$

Erster Beweis. Per definitionem gilt $\det A^\top = \sum_{\sigma\in\mathcal{S}_n} \operatorname{sgn}(\sigma) a_{\sigma(1)1}\dots a_{\sigma(n)n}$. Ist nun $\tau = \sigma^{-1}$ die inverse Permutation, so haben wir $\operatorname{sgn}(\tau) = \operatorname{sgn}(\sigma)$ und darüber hinaus $a_{1\tau(1)}\dots a_{n\tau(n)} = a_{\sigma(1)1}\dots a_{\sigma(n)n}$, denn diese Produkte unterscheiden sich nur in der Reihenfolge ihrer Faktoren. Damit ergibt sich dann wie behauptet

$$\det A^\top = \sum_{\tau\in\mathcal{S}_n} \operatorname{sgn}(\tau) a_{1\tau(1)}\dots a_{n\tau(n)} \qquad \square$$

Zweiter Beweis. Arbeiten wir mit Koeffizienten in einem Körper, so können wir auch davon ausgehen, daß nach 1.9.6 jede quadratische Matrix A als ein Produkt von Elementarmatrizen $A = S_1\dots S_r$ geschrieben werden kann. Für Elementarmatrizen S prüft man die Identität $\det S^\top = \det S$ leicht explizit, und dann liefert die Multiplikationsformel

$$\begin{aligned}\det A^\top &= \det(S_r^\top \dots S_1^\top) = \det(S_r^\top)\dots\det(S_1^\top) = \det(S_r)\dots\det(S_1)\\ \det A &= \det(S_1\dots S_r) = \det(S_1)\dots\det(S_r)\end{aligned}$$

und diese Produkte sind offensichtlich gleich. $\square$

Satz 3.4.8 (Laplace'scher Entwicklungssatz). *Gegeben eine $(n\times n)$-Matrix $A = (a_{ij})$ und feste k, l bezeichne $A\langle k,l\rangle$ die* **Streichmatrix***, die aus A durch Streichen der k-ten Zeile und l-ten Spalte entsteht. So gilt für jedes feste i die* **Entwicklung der Determinante nach der i-ten Zeile**

$$\det A = \sum_{j=1}^{n} (-1)^{i+j} a_{ij}\ \det A\langle i,j\rangle$$

und für jedes feste j die **Entwicklung nach der j-ten Spalte**

$$\det A = \sum_{i=1}^{n} (-1)^{i+j} a_{ij}\ \det A\langle i,j\rangle$$

Bemerkung 3.4.9. Der folgende Beweis verwendet zwar die Sprache der Vektorräume, das Argument funktioniert jedoch ganz genauso statt für Matrizen mit Einträgen in einem Körper auch für Matrizen mit Einträgen in einem Kring.

Beweis. Wegen $\det A = \det A^\top$ reicht es, die erste unserer beiden Formeln zu zeigen. Wir wissen bereits, daß sich die Determinante einer quadratischen Matrix nur um den Faktor $(-1)^{j-1}$ ändert, wenn wir die j-te Spalte ganz nach vorne

schieben, ohne die Reihenfolge der übrigen Spalten zu ändern. Es reicht also, unsere Formel für die Entwicklung nach der ersten Spalte zu zeigen, was im folgenden Beweis insbesondere die Notation vereinfacht. Wir schreiben unsere Matrix als Folge von Spaltenvektoren $A = (a_{*1}|a_{*2}|\dots|a_{*n})$ und schreiben den ersten Spaltenvektor als Linearkombination der Standardbasisvektoren

$$a_{*1} = a_{11}\mathrm{e}_1 + \dots + a_{n1}\mathrm{e}_n$$

Die Multilinearität der Determinante liefert sofort

$$\det A = \sum_{i=1}^{n} a_{i1} \det(\mathrm{e}_i|a_{*2}|\dots|a_{*n}) = \sum_{i=1}^{n} a_{i1}(-1)^{i-1} \det A\langle i,1\rangle$$

wo wir im zweiten Schritt die i-te Zeile der Matrix $(\mathrm{e}_i|a_{*2}|\dots a_{*n})$ ganz nach oben geschoben haben, ohne die Reihenfolge der übrigen Zeilen zu ändern, um dann die Formel 4.5.7 für die Determinante von Block-oberen-Dreiecksmatrizen anzuwenden. □

Satz 3.4.10 (Cramer'sche Regel). *Bildet man zu einer quadratischen Matrix A mit Einträgen in einem Kring die sogenannte* **adjungierte Matrix** *$A^\sharp$ mit den Einträgen $A^\sharp_{ij} = (-1)^{i+j} \det A\langle j,i\rangle$ für $A\langle j,i\rangle$ die entsprechende Streichmatrix nach 3.4.8, so gilt*

$$A \circ A^\sharp = (\det A) \cdot I$$

3.4.11. Diese adjungierte Matrix ist nicht zu verwechseln mit der adjungierten Abbildung aus 4.6.9, mit der sie außer der Bezeichnung rein gar nichts zu tun hat. Man beachte auch die Indexvertauschung: In der i-ten Zeile und j-ten Spalte der adjungierten Matrix steht bis auf ein "schachbrettartig verteiltes Vorzeichen" die Determinante der Matrix, die entsteht, wenn man die j-te Zeile und i-te Spalte der ursprünglichen Matrix streicht.

3.4.12. Meist versteht man unter der **Cramer'schen Regel** die Formel

$$x_i = \frac{\det(a_{*1}|\dots|b_*|\dots|a_{*n})}{\det(a_{*1}|\dots|a_{*i}|\dots|a_{*n})}$$

für die Lösung linearen Gleichungssystems $x_1a_{*1} + \dots + x_ia_{*i} \dots + x_na_{*n} = b_*$, wenn es denn eindeutig lösbar ist. Hier ist im Zähler wie angedeutet die i-te Spalte a_{*i} der Koeffizientenmatrix durch den gewünschten Lösungsvektor b_* zu ersetzen. Besagte Formel ergibt sich unmittelbar durch Einsetzen der alternativen Darstellung von b_* in die Determinante im Zähler. Setzen wir in dieser Formel für b_* die Vektoren der Standardbasis ein, so erhalten wir die Einträge der inversen Matrix in der Form, in der sie auch im Satz beschrieben werden. Diese Formel wirkt zwar explizit, ist jedoch in der Praxis völlig unbrauchbar.

Beweis. Es gilt zu zeigen

$$\sum_i (-1)^{i+j} a_{ki} \det A\langle j,i\rangle = \delta_{kj}(\det A)$$

Im Fall $k = j$ folgt das direkt aus unserer Entwicklung der Determinante nach der j-ten Zeile 3.4.8. Im Fall $k \neq j$ steht die Formel für die Entwicklung nach der j-ten Zeile der Determinante der Matrix $\tilde{A}$ da, die aus A entsteht beim Ersetzen der j-ten Zeile durch die k-te Zeile. Da diese Matrix jedoch zwei gleiche Zeilen und damit Determinante Null hat, gilt unsere Formel auch in diesem Fall. □

Korollar 3.4.13 (Invertierbarkeit ganzzahliger Matrizen). *Eine quadratische Matrix mit Einträgen in einem Kring besitzt genau dann eine Inverse mit Einträgen in besagtem Kring, wenn ihre Determinante in unserem Kring eine Einheit ist.*

3.4.14. Eine quadratische Matrix mit ganzzahligen Einträgen besitzt insbesondere genau dann eine Inverse mit ganzzahligen Einträgen, wenn ihre Determinante 1 oder -1 ist, und eine quadratische Matrix mit Einträgen im Polynomring über einem Körper besitzt genau dann eine Inverse mit polynomialen Einträgen, wenn ihre Determinante ein von Null verschiedenes konstantes Polynom ist.

Beweis. Sei k unser Kring. Gegeben Matrizen $A, B \in \mathrm{M}(n \times n; k)$ mit $AB = I$ gilt natürlich $(\det A)(\det B) = \det I = 1$ und damit ist $\det A$ eine Einheit in k. Ist umgekehrt $\det A$ eine Einheit in k, so liefert nach der Cramer'schen Regel 3.4.10 die Formel $B = (\det A)^{-1} A^\sharp$ eine Matrix $B \in \mathrm{M}(n \times n; k)$ mit $AB = I$. Indem wir dies Argument auf die transponierte Matrix anwenden und das Resultat wieder transponieren, finden wir auch $C \in \mathrm{M}(n \times n; k)$ mit $CA = I$. Durch Multiplizieren der zweiten Gleichung mit B von rechts folgt sofort $B = C$, folglich ist A in der Tat invertierbar in $\mathrm{M}(n \times n; k)$ im Sinne von I.3.2.2. □

Ergänzende Übung 3.4.15. Es seien n^2 paarweise kommutierende Matrizen $A_{11}, \ldots, A_{nn}$ mit m Zeilen und Spalten und Einträgen in einem Kring R gegeben. Wir bilden die $(mn \times mn)$-Matrix

$$B = \begin{pmatrix} A_{11} & \ldots & A_{1n} \\ \vdots & & \vdots \\ A_{n1} & \ldots & A_{nn} \end{pmatrix}$$

Man zeige, daß gilt

$$\det B = \det \left(\sum_{\sigma \in \mathcal{S}_n} \mathrm{sgn}(\sigma) A_{1\sigma(1)} \ldots A_{n\sigma(n)} \right)$$

Hinweis: Ist A_{11} die Einheitsmatrix, so folgt die Behauptung durch Nullen der ersten Blockspalte und Induktion. Ist $\det A_{11}$ ein Nichtnullteiler unseres Krings R, so folgt die Aussage durch Multiplizieren mit $\operatorname{diag}(A_{11}^\sharp, I, \ldots, I)$ für $A_{11}^\sharp$ die adjungierte Matrix zu A_{11}. Im allgemeinen kann man eine weitere Variable X einführen und A_{11} durch die Matrix $A_{11} + XI$ ersetzen, deren Determinante ein normiertes Polynom in $R[X]$ und deshalb kein Nullteiler ist. Nachher setze man dann $X = 0$.

Ergänzende Übung 3.4.16. Man zeige dieselbe Formel wie in 3.4.15 auch für den Fall, daß die Matrizen A_{ij} alle obere Dreiecksmatrizen sind. Hinweis: Wir betrachten diejenige Abbildung

$$f : \{1, \ldots, mn\} \to \{1, \ldots, m\}$$

die verträglich ist mit der Restklassenabbildung beider Mengen auf $\mathbb{Z}/m\mathbb{Z}$, und beachten, daß für eine Permutation $\sigma \in \mathcal{S}_{mn}$ mit $f(\sigma(i)) \leq f(i) \quad \forall i$ notwendig Gleichheit gilt für alle i.

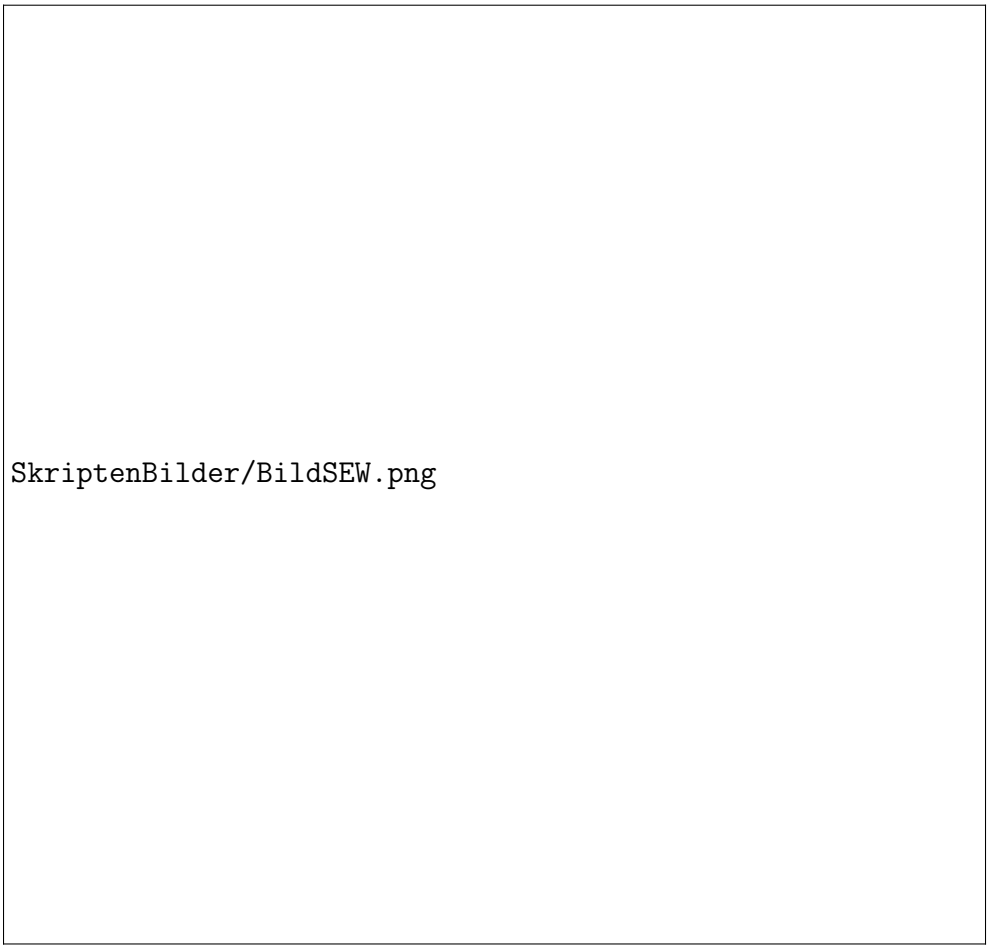
3.5 Eigenwerte und Eigenvektoren

Definition 3.5.1. Sei $f : V \to V$ ein Endomorphismus eines Vektorraums über einem Körper k. Ein Skalar $\lambda \in k$ heißt ein **Eigenwert von** f genau dann, wenn es einen von Null verschiedenen Vektor $v \neq 0$ aus V gibt mit $f(v) = \lambda v$. Jeder derartige Vektor heißt dann ein **Eigenvektor von** f **zum Eigenwert** λ.

Beispiel 3.5.2. Zunächst zwei nicht ganz mathematisch ausformulierte Beispiele: Die Drehung des Richtungsraums der Papierebene um den rechten Winkel im Uhrzeigersinn besitzt keinen reellen Eigenwert. Eine Spiegelung des Richtungsraums der Papierebene an einer Geraden besitzt stets Eigenvektoren zum Eigenwert Eins, nämlich alle Richtungsvektoren der Spiegelachse. Für das Ableiten, aufgefaßt als Endomorphismus des Raums aller reellen polynomialen Funktionen, ist der einzige Eigenwert Null und die zugehörigen Eigenvektoren sind genau die von Null verschiedenen konstanten Polynome.

Satz 3.5.3 (Existenz von Eigenwerten). *Jeder Endomorphismus eines von Null verschiedenen endlichdimensionalen Vektorraums über einem algebraisch abgeschlossenen Körper besitzt einen Eigenwert.*

3.5.4. Auf dem $\mathbb{C}$-Vektorraum $\mathbb{C}[X]$ der Polynome besitzt der Endomorphimus "Multipliziere mit X" keine Eigenwerte. Die Annahme endlicher Dimension ist also für die Gültigkeit des vorhergehenden Korollars wesentlich. Die Drehung des Richtungsraums der Papierebene um einen von $0°$ und $180°$ verschiedenen Winkel besitzt auch keinen reellen Eigenwert. Die Annahme eines algebraisch



Die anschauliche Spiegelung s an der gestrichelt einegezeichneten Achse ist eine lineare Abbildung $s : \mathbb{R}^2 \to \mathbb{R}^2$ mit den Eigenwerten ± 1. Eigenvektoren zum Eigenwert 1 sind alle von Null verschiedenen Vektoren der Spiegelachse, Eigenvektoren zum Eigenwert -1 sind alle von Null verschiedenen Vektoren, die auf der Spiegelachse senkrecht stehen. Die Matrix unserer Abbildung in Standardbasis ist nach 1.10 die Matrix

$$A = \begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix}$$

mit charakteristischem Polynom
$\chi_A(\lambda) = (\lambda - \cos 2\alpha)(\lambda + \cos 2\alpha) - \sin^2 2\alpha = \lambda^2 - 1.$

abgeschlossenen Grundkörpers ist also auch wesentlich. Für den Beweis entwickeln wir zunächst unsere Theorie etwas weiter und geben dann den Beweis im Anschluß an 3.5.10.

Definition 3.5.5. Sei k ein Körper und $A \in \mathrm{M}(n \times n; k)$ eine quadratische Matrix mit Koeffizienten in k. Das Polynom $\det(A - \lambda I)$ aus dem Polynomring $k[\lambda]$ heißt das **charakteristische Polynom der Matrix** A. Es wird auch notiert

$$\det(A - \lambda I) = \chi_A(\lambda)$$

Satz 3.5.6 (Eigenwerte und charakteristisches Polynom). *Sei k ein Körper und $A \in \mathrm{M}(n \times n; k)$ eine quadratische Matrix mit Koeffizienten in k. Die Eigenwerte der durch die Multiplikation mit unserer Matrix gegebenen linearen Abbildung $A : k^n \to k^n$ sind genau die Nullstellen ihres charakteristischen Polynoms χ_A.*

Beweis. Bezeichnet $I \in \mathrm{M}(n \times n; k)$ die Einheitsmatrix, so haben wir für $\lambda \in k$ die Äquivalenzen

$$\begin{aligned}
(\lambda \text{ ist Eigenwert von } A) &\Leftrightarrow \exists v \neq 0 \text{ mit } Av = \lambda v \\
&\Leftrightarrow \exists v \neq 0 \text{ mit } (A - \lambda I)v = 0 \\
&\Leftrightarrow \ker(A - \lambda I) \neq 0 \\
&\Leftrightarrow \det(A - \lambda I) = 0 \\
&\Leftrightarrow \chi_A(\lambda) = 0
\end{aligned}$$

□

Übung 3.5.7. Sei k ein Körper und $A \in \mathrm{M}(n \times n; k)$ eine quadratische Matrix mit Koeffizienten in k. Man zeige, daß das charakteristische Polynom von A die Gestalt

$$\chi_A(\lambda) = (-\lambda)^n + \mathrm{tr}(A)(-\lambda)^{n-1} + \ldots + \det(A)$$

hat, in Worten also den Leitkoeffizienten $(-1)^n$, als nächsten Koeffizienten bis auf ein Vorzeichen die Spur von A, und als konstanten Term die Determinante von A.

Ergänzende Übung 3.5.8. Jeder Endomorphismus eines endlichdimensionalen reellen Vektorraums ungerader Dimension besitzt einen reellen Eigenwert. Ist die Determinante unseres Endomorphismus positiv, so besitzt er sogar einen positiven reellen Eigenwert.

Ergänzende Übung 3.5.9. Sind $k \subset K$ Körper und ist k algebraisch abgeschlossen und gilt $\dim_k K < \infty$, so folgt $K = k$. Hinweis: Man betrachte für alle $a \in K$ die durch Multiplikation mit a gegebene k-lineare Abbildung $(a\cdot) : K \to K$ und deren Eigenwerte.

3.5.10. Sei k ein Körper und $f : V \to V$ ein Endomorphismus eines endlichdimensionalen k-Vektorraums. Mit demselben Argument wie in 3.4.4 sehen wir, daß bezüglich jeder angeordneten Basis von V die darstellende Matrix von f dasselbe charakteristische Polynom hat, in Formeln $\det({}_{\mathcal{B}}[f]_{\mathcal{B}} - \lambda\,\mathrm{id}) = \det({}_{\mathcal{A}}[f]_{\mathcal{A}} - \lambda\,\mathrm{id})$ für je zwei angeordnete Basen $\mathcal{A}$ und $\mathcal{B}$ von V. Dies Polynom notieren wir dann

$$\chi_f = \chi_f(\lambda)$$

und nennen es das **charakteristische Polynom des Endomorphismus** f. Die Eigenwerte von f sind nach 3.5.5 genau die Nullstellen des charakteristischen Polynoms χ_f von f.

Beweis von Satz 3.5.3. Der Satz besagt, daß jeder Endomorphismus eines endlichdimensionalen von Null verschiedenen Vektorraums über einem algebraisch abgeschlossenen Körper einen Eigenwert besitzt. Das charakteristische Polynom unseres Endomorphismus ist nicht konstant, da unser Raum nicht der Nullraum ist. Im Fall eines algebraisch abgeschlossenen Körpers besitzt es also stets eine Nullstelle, und die ist dann nach 3.5.10 auch bereits der gesuchte Eigenwert. □

3.5.11. Das charakteristische Polynom einer Block-oberen-Dreiecksmatrix ist nach 4.5.7 das Produkt der charakteristischen Polynome ihrer Blöcke auf der Diagonalen.

Proposition 3.5.12 (Trigonalisierbarkeit). *Sei $f : V \to V$ ein Endomorphismus eines endlichdimensionalen Vektorraums über einem Körper k. So sind gleichbedeutend:*

1. *Der Vektorraum V besitzt eine angeordnete Basis $\mathcal{B}$, bezüglich derer die Matrix ${}_{\mathcal{B}}[f]_{\mathcal{B}}$ von f obere Dreiecksgestalt hat. Man sagt dann auch, f sei* **trigonalisierbar**.

2. *Das charakteristische Polynom χ_f von f zerfällt bereits im Polynomring $k[\lambda]$ vollständig in Linearfaktoren.*

Beweis. $1 \Rightarrow 2$ ist klar nach unserer Formel 3.1.4 für die Determinante einer oberen Dreiecksmatrix: Hat ${}_{\mathcal{B}}[f]_{\mathcal{B}}$ obere Dreiecksgestalt mit Diagonaleinträgen $\lambda_1, \ldots, \lambda_n$, so haben wir ja $\chi_f(\lambda) = (\lambda_1 - \lambda) \ldots (\lambda_n - \lambda)$. Um $2 \Rightarrow 1$ zu zeigen, dürfen wir ohne Beschränkung der Allgemeinheit $V = k^n$ annehmen, so daß f durch die Multiplikation mit einer Matrix A gegeben ist. Zu zeigen ist dann die Existenz von $B \in \mathrm{GL}(n;k)$ mit $B^{-1}AB = D$ von oberer Dreiecksgestalt: Die Spaltenvektoren der Matrix B bilden dann nämlich die gesuchte Basis $\mathcal{B}$. Wir argumentieren mit vollständiger Induktion über n. Für $n \geq 1$ gibt es nach Voraussetzung eine Nullstelle λ_1 von χ_A und dann nach 3.5.6 ein $c_1 \in k^n \backslash 0$

mit $Ac_1 = \lambda_1 c_1$. Ergänzen wir c_1 durch $c_2, \ldots, c_n$ zu einer Basis von k^n und betrachten die Matrix $C = (c_1|\ldots|c_n)$, so gilt

$$AC = C \left(\begin{array}{c|c} \lambda_1 & * \\ \hline 0 & H \end{array}\right)$$

mit $H \in \mathrm{M}((n-1)\times(n-1);k)$. Nach Übung 4.5.7 haben wir dann $\chi_H = (\lambda_2 - \lambda)\ldots(\lambda_n - \lambda)$ und per Induktion finden wir $F \in \mathrm{GL}(n-1;k)$ mit $F^{-1}HF$ von oberer Dreiecksgestalt. Bilden wir nun $\tilde{F} = \mathrm{diag}(1, F)$, so ist offensichtlich auch $\tilde{F}^{-1}(C^{-1}AC)\tilde{F}$ von oberer Dreiecksgestalt und die Matrix $B = C\tilde{F}$ löst unser Problem. □

Ergänzende Übung 3.5.13. Gegeben ein Endomorphismus eines endlichdimensionalen reellen Vektorraums gibt es stets eine Basis derart, daß die zugehörige Matrix Block-obere Dreiecksgestalt hat mit höchstens Zweierblöcken auf der Diagonalen.

Proposition 3.5.14 (Charakterisierung nilpotenter Matrizen). *Eine Matrix mit Koeffizienten in einem Körper ist nilpotent genau dann, wenn ihr charakteristisches Polynom nur aus dem Leitterm besteht. In Formeln ist also $A \in \mathrm{M}(n\times n;k)$ nilpotent genau dann, wenn gilt $\chi_A(\lambda) = (-\lambda)^n$.*

Beweis. Ist unsere Matrix nilpotent, so ist sie nach 1.10.12 konjugiert zu einer oberen Dreiecksmatrix mit Nullen auf der Diagonalen und unsere Behauptung folgt aus 3.5.11. Besteht umgekehrt das charakteristische Polynom nur aus dem Leitterm, so existiert nach 3.5.12 oder zumindest seinem Beweis eine invertierbare Matrix $B \in \mathrm{GL}(n;k)$ mit $B^{-1}AB$ von oberer Dreiecksgestalt mit Nullen auf der Diagonale. Daraus folgt jedoch unmittelbar erst $(B^{-1}AB)^n = 0$ und dann $A^n = 0$. □

Ergänzung 3.5.15. Alternative Argumente für die Rückrichtung beim Beweis der Proposition liefern der Satz von Cayley-Hamilton 3.5.21 und der Satz über die Hauptraumzerlegung 6.3.14.

Definition 3.5.16. Ein Endomorphismus eines Vektorraums heißt **diagonalisierbar** genau dann, wenn unser Vektorraum von den Eigenvektoren des besagten Endomorphismus erzeugt wird. Im Fall eines endlichdimensionalen Vektorraums ist das gleichbedeutend dazu, daß unser Vektorraum V eine angeordnete Basis $\mathcal{B} = (v_1, \ldots, v_n)$ besitzt, für die die Matrix unserer Abbildung Diagonalgestalt hat, in Formeln ${}_{\mathcal{B}}[f]_{\mathcal{B}} = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$. In der Tat bedeutet das ja gerade $f(v_i) = \lambda_i v_i$.

Lemma 3.5.17. *Die Restriktion eines diagonalisierbaren Endomorphismus auf einen unter besagtem Endomorphismus stabilen Teilraum ist wieder diagonalisierbar.*

Beweis. Sei $f : V \to V$ unser Endomorphismus und $W \subset V$ ein unter f stabiler Teilraum. Gegeben $v \in W$ haben wir nach Annahme eine Darstellung $v = v_1 + \ldots + v_n$ mit $v_i \in V$ Eigenvektoren zu paarweise verschiedenen Eigenwerten $\lambda_1, \ldots, \lambda_n \in k$. Dann gilt aber

$$(f - \lambda_2 \operatorname{id}) \ldots (f - \lambda_n \operatorname{id}) v = (\lambda_1 - \lambda_2) \ldots (\lambda_1 - \lambda_n) v_1 \in W$$

und folglich $v_1 \in W$. Ebenso zeigt man auch $v_2, \ldots, v_n \in W$, mithin wird auch W von Eigenvektoren erzeugt. □

Definition 3.5.18. Sei k ein Körper und $n \in \mathbb{N}$. Eine quadratische Matrix $A \in \mathrm{M}(n \times n; k)$ heißt **diagonalisierbar** genau dann, wenn der durch Multiplikation mit A gegebene Endomorphismus des k^n diagonalisierbar ist. Das hinwiederum ist gleichbedeutend zur Existenz einer invertierbaren Matrix $S \in \mathrm{GL}(n; k)$ mit $S^{-1}AS = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$ diagonal alias $AS = S \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$. In den Spalten von S stehen dann die Vektoren einer Basis von k^n aus Eigenvektoren von A zu den Eigenwerten $\lambda_1, \ldots, \lambda_n$.

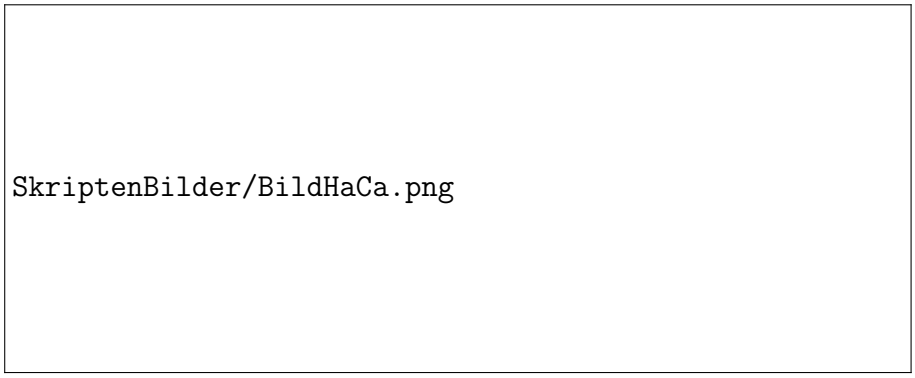
Beispiel 3.5.19. Eine nilpotente Matrix ist genau dann diagonalisierbar, wenn sie die Nullmatrix ist. Das folgende Lemma zeigt insbesondere, daß jede $(n \times n)$-Matrix, deren charakteristisches Polynom n paarweise verschiedene Nullstellen hat, diagonalisierbar sein muß. Salopp gesprochen sind also “komplexe quadratische Matrizen für gewöhnlich diagonalisierbar”.

Lemma 3.5.20. *Sei $f : V \to V$ ein Endomorphismus eines Vektorraums und seien $v_1, \ldots, v_n$ Eigenvektoren von f zu paarweise verschiedenen Eigenwerten $\lambda_1, \ldots, \lambda_n$. So sind unsere Eigenvektoren linear unabhängig.*

Beweis. Der Endomorphismus $(f - \lambda_2 \operatorname{id}) \ldots (f - \lambda_n \operatorname{id})$ macht $v_2, \ldots, v_n$ zu Null, aber nicht v_1. Gegeben $x_1, \ldots, x_n \in k$ mit $x_1 v_1 + \ldots + x_n v_n = 0$ folgt demnach durch Anwenden unseres Endomorphismus $x_1 = 0$. Ebenso zeigt man $x_2 = \ldots = x_n = 0$. □

Satz 3.5.21 (Cayley-Hamilton). *Setzt man eine quadratische Matrix in ihr eigenes charakteristisches Polynom ein, so erhält man die Nullmatrix.*

Bemerkung 3.5.22. Der folgende Beweis gefällt mir nicht. Ein alternativer Beweis, der in meinen Augen mehr Einsicht vermittelt, wird in IV.1.8.14 angedeutet.



$(F - fE)(\mathrm{e}_1^\top, \ldots, \mathrm{e}_n^\top)^\top = 0$ am Beispiel einer Matrix F mit drei Zeilen und Spalten. Alle nicht ausgeschriebenen Einträge der obigen Matrizen sind als Null zu verstehen.

Beweis. Gegeben eine quadratische Matrix A mit Koeffizienten in einem Kring gibt es nach 3.4.10 eine weitere Matrix $A^\sharp$ mit Koeffizienten in demselben Kring derart, daß im Ring der quadratischen Matrizen mit Einträgen in unserem Kring gilt

$$A^\sharp A = (\det A) \cdot E$$

für E die Einheitsmatrix. Nehmen wir speziell den Kring $k[t]$ und die Matrix $A = F - tE$ für eine vorgegebene Matrix $F \in \mathrm{M}(n \times n; k)$, so erhalten wir in $\mathrm{M}(n \times n; k[t])$ die Gleichung

$$A^\sharp(F - tE) = \chi_F(t) \cdot E$$

Bezeichne nun $f : k^n \to k^n$ die durch Multiplikation von Spaltenvektoren mit der zu F transponierten Matrix $F^\top$ gegebene lineare Abbildung. Wenden wir auf beide Seiten unserer Gleichung von Matrizen den Ringhomomorphismus $k[t] \to \mathrm{End}_k k^n$ mit $t \mapsto f$ an, so erhalten wir in $\mathrm{M}(n \times n; \mathrm{End}_k k^n)$ alias $\mathrm{M}(n^2 \times n^2; k)$ die Gleichung

$$A^\sharp(F - fE) = \chi_F(f) \cdot E$$

Betrachten wir nun die Standardbasis $\mathrm{e}_1, \ldots, \mathrm{e}_n$ aus Spaltenvektoren des k^n und wenden beide Seiten dieser Gleichung an auf den Vektor $(\mathrm{e}_1^\top, \ldots, \mathrm{e}_n^\top)^\top$, aufgefaßt als Spaltenvektor in k^{n^2}, so ergibt auf der linken Seite schon die Multiplikation mit $(F - fE)$ den Nullvektor, denn bei

$$(F - fE)(\mathrm{e}_1^\top, \ldots, \mathrm{e}_n^\top)^\top$$

steht im i-ten Block von k^{n^2} genau $F_{i1}\,\mathrm{e}_1 + \ldots + F_{in}\,\mathrm{e}_n - f(\mathrm{e}_i) = 0$. Also wird die rechte Seite auch Null und es folgt $\chi_F(f)\,\mathrm{e}_1 = \ldots = \chi_F(f)\,\mathrm{e}_n = 0$. Hier ist zwar χ_F a priori das charakteristische Polynom der zu einer Matrix von f transponierten Matrix, aber das stimmt nach 3.4.7 mit dem charakteristischen Polynom von f überein. □

Ergänzende Übung 3.5.23 (**Jordanform für** (2×2)**-Matrizen**). Sei k ein algebraisch abgeschlossener Körper. Man zeige, daß es für jede Matrix $A \in \mathrm{M}(2 \times 2; k)$ eine invertierbare Matrix $P \in \mathrm{GL}(2; k)$ gibt derart, daß $P^{-1}AP$ eine der beiden Gestalten

$$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} \quad \text{oder} \quad \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \quad \text{hat.}$$

4 Euklidische Vektorräume

4.1 Modellierung des Raums unserer Anschauung*

4.1.1. Unter einem Automorphismus eines affinen Raums verstehen wir wie in 1.7.12 eine bijektive affine Abbildung unseres affinen Raums auf sich selbst. Es ist leicht zu sehen, daß die Umkehrabbildung jedes derartigen Automorphismus wieder ein Automorphismus ist. Folglich bilden die Automorphismen eines affinen Raums eine Untergruppe der Gruppe aller Bijektionen von unserem affinen Raum auf sich selbst. Die Gruppe der Automorphismen eines affinen Raums E notieren wir $\mathrm{Aff}^\times E$.

Definition 4.1.2. Unter einer **Bewegungsgruppe** eines dreidimensionalen reellen affinen Raums E verstehen wir eine alle Translationen umfassende Untergruppe seiner Automorphismengruppe

$$B \subset \mathrm{Aff}^\times E$$

derart, daß es für je zwei Paare (H, L) von Teilmengen von E bestehend aus einer Halbebene und einer Halbgerade auf ihrem Rand genau einen Automorphismus aus B gibt, der sie ineinander überführt. In Formeln meinen wir hier Paare (H, L) von Teilmengen $L \subset H \subset E$, die in der Gestalt $L = p + \mathbb{R}_{\geq 0}\vec{v}$ und $H = p + \mathbb{R}\vec{v} + \mathbb{R}_{\geq 0}\vec{w}$ geschrieben werden können, mit $p \in E$ einem Punkt und $\vec{v}, \vec{w} \in \vec{E}$ linear unabhängigen Richtungsvektoren. Haben wir in einem dreidimensionalen reellen affinen Raum eine Bewegungsgruppe ausgezeichnet, so sprechen wir deren Elemente auch als **Bewegungen** an.

Ergänzung 4.1.3. In der Literatur wird das Wort “Bewegung” meist als Synonym für das Konzept verwendet, für das wir in 4.4.1 die Bezeichnung “bijektive Isometrie” vereinbaren. Insbesondere werden in der Literatur auch Spiegelungen als Bewegungen angesehen, genauer als “uneigentliche Bewegungen”, und unsere Bewegungen entsprechen eher dem, was in der Literatur unter “eigentlichen Bewegungen” verstanden wird. Der wesentliche Unterschied liegt jedoch woanders: Während es in der Literatur üblich ist, vom Begriff des Skalarprodukts und des zugehörigen Abstands auszugehen und dann abstandserhaltende Abbildungen zu untersuchen, gehe ich hier den umgekehrten Weg in der Hoffnung, dadurch die Beziehung unserer abstrakten Konzepte zur Anschauung zu stärken.

4.1.4. Unser mathematisches Modell des Raums unserer Anschauung als eines dreidimensionalen reellen affinen Raums

$$\mathbb{E}$$

Zwei Paare von Teilmengen des Raums bestehend aus je einer Halbebene und einer Halbgerade auf ihrem Rand.

aus 1.7.7 erweitern wir nun um das zusätzliche Datum einer ausgezeichneten Bewegungsgruppe $B \subset \mathrm{Aff}^\times \mathbb{E}$ im Sinne der vorhergehenden Definition 4.1.2. Meines Erachtens ist es diese Struktur $(\mathbb{E}, B)$, die die Bezeichnung als "euklidischer Raum" am ehesten verdient hätte, aber leider ist die fragliche Bezeichnung schon anderweitig vergeben. Zu unserem Modell des Raums unserer Anschauung 4.1.15 hingegen nehmen wir auch noch das Datum einer ausgezeichneten Orientierung hinzu, um später einmal den Elektromagnetismus behandeln zu können. Die Elemente von $\mathbb{E}$ denke ich mir als "alle möglichen Orte im Raum". Manche dieser Orte können direkt als Kirchturmspitzen, Zimmerecken und dergleichen angegeben werden, die Übrigen gilt es sich vorzustellen. Affine Geraden in $\mathbb{E}$ denke ich mir als Sichtlinien, wie in 1.7.7 und 1.7.34 besprochen. Bei Bewegungen denke ich an, nun, eben anschauliche Bewegungen. Kippen wir etwa einen Stuhl um, so werden die Enden der Stuhlbeine, die Ecken der Sitzfläche, ja überhaupt alle seine Punkte jeweils in andere Punkte des Raums unserer Anschauung überführt, und diese Abbildung läßt sich—so zeigt es unsere Erfahrung—zu einer Selbstabbildung des Raums unserer Anschauung fortsetzen, die Sichtlinien in Sichtlinien überführt und die nach 1.7.33 folglich einer affinen Abbildung $\mathbb{E} \to \mathbb{E}$ entsprechen muß. Unsere ausgezeichnete Bewegungsgruppe B modelliert die Menge aller derartigen Selbstabbildungen des Raums unserer Anschauung. Unsere Bedingung an eine Bewegungsgruppe bedeutet anschaulich, daß man etwa jedes Messer aus einer festen Position heraus durch genau eine Bewegung in eine Position bringen kann, in der der Übergang vom Griff zur Klinge an einer vorgegebenen Stelle stattfindet, die Messerspitze in eine vorgegebene Richtung zeigt und der Schnitt den Raum entlang einer vorgegebenen Halbebene zerteilen würde. An dieser Stelle möchte ich Sie am liebsten wieder einmal davon überzeugen, daß das Abstrakte das eigentlich Konkrete ist.

Ergänzung 4.1.5. Ich wage die Vermutung, daß Säuglinge nicht zuletzt deshalb so gerne herumgetragen und herumgefahren werden, weil ihnen das die Untersuchung dieser bemerkenswerten mathematischen Struktur ermöglicht, die der Raum unserer Anschauung nun einmal ist.

Definition 4.1.6. Ein **Skalarprodukt** auf einem reellen Vektorraum V ist eine bilineare Abbildung $V \times V \to \mathbb{R}$, $(\vec{v}, \vec{w}) \mapsto \langle \vec{v}, \vec{w} \rangle$ derart, daß gilt $\langle \vec{v}, \vec{w} \rangle = \langle \vec{w}, \vec{v} \rangle$ für alle $\vec{v}, \vec{w} \in V$ und $\vec{v} \neq \vec{0} \Rightarrow \langle \vec{v}, \vec{v} \rangle > 0$. Allgemeiner vereinbaren wir dieselbe Definition auch im Fall eines Vektorraums über einem beliebigen angeordneten Körper.

4.1.7. Das Skalarprodukt trägt seinen Namen, da es eben aus zwei Vektoren einen Skalar macht. Es darf nicht verwechselt werden mit der "Multiplikation mit Skalaren" aus der Axiomatik eines Vektorraums, die aus einem Skalar und einem Vektor einen Vektor macht.

Satz 4.1.8 (Bewegungsgruppen und Skalarprodukte). *Sei $(E, B, \vec{m})$ ein dreidimensionaler reeller affiner Raum E mit einer ausgezeichneten Bewegungsgruppe B im Sinne von 4.1.2 und einem ausgezeichneten von Null verschiedenen Richtungsvektor $\vec{m} \in \vec{E}$. So gibt es auf dem Richtungsraum $\vec{E}$ von E genau ein Skalarprodukt, ja sogar genau eine bilineare Abbildung $\langle\ ,\ \rangle : \vec{E} \times \vec{E} \to \mathbb{R}$ mit den beiden folgenden Eigenschaften:*

1. *Die linearen Anteile aller unserer Bewegungen lassen besagte bilineare Abbildung invariant, in Formeln*
$$\langle \vec{\varphi}(\vec{v}), \vec{\varphi}(\vec{w}) \rangle = \langle \vec{v}, \vec{w} \rangle \quad \textit{für alle } \vec{v}, \vec{w} \in \vec{E} \textit{ und } \varphi \in B;$$
2. *Für unseren ausgezeichneten von Null verschiedenen Richtungsvektor $\vec{m} \in \vec{E}$ gilt $\langle \vec{m}, \vec{m} \rangle = 1$.*

4.1.9. In 4.4.16 können Sie zur Übung zeigen, daß gegeben ein dreidimensionaler reeller affiner Raum E mit einem Skalarprodukt auf seinem Richtungsraum umgekehrt alle Automorphismen φ des affinen Raums E, deren lineare Anteile $\vec{\varphi}$ besagtes Skalarprodukt invariant lassen und positive Determinante haben, eine Bewegungsgruppe im Sinne von 4.1.2 bilden.

4.1.10. Als den ausgezeichneten Richtungsvektor $\vec{m} \in \vec{\mathbb{E}}$ des Raums unserer Anschauung mag man sich diejenige Parallelverschiebung denken, die das eine Ende des Urmeters in Paris auf sein anderes Ende schiebt. Der vorhergehende Satz 4.1.8 zusammen mit der anschließenden Bemerkung 4.1.9 soll eine Brücke bilden zwischen der meines Erachtens intuitiv besonders gut zugänglichen Modellierung des Raums unserer Anschauung als dreidimensionaler reeller affiner Raum mit einer ausgezeichneten Bewegungsgruppe und seiner algebraisch besonders eleganten wenn auch mit der Wahl eines ausgezeichneten Richtungsvektors belasteten Modellierung als dreidimensionaler reeller affiner Raum mit einem ausgezeichneten Skalarprodukt auf seinem Richtungsraum.

Beweis. Wir zeigen hier nur, daß es zu einer ausgezeichneten Bewegungsgruppe nicht mehr als eine bilineare Abbildung mit den behaupteten Eigenschaften geben kann, und daß diese, wenn es sie denn gibt, ein Skalarprodukt sein muß. Die restlichen Aussagen des Satzes und insbesondere die Existenz eines Skalarprodukts mit den behaupteten Eigenschaften zeigen wir erst in 8.5.3. Die linearen Anteile von Bewegungen $\varphi \in B$ bilden sicher eine Untergruppe $D \subset \mathrm{GL}(\vec{E})$, deren Elemente wir die zu unserer Bewegungsgruppe gehörenden **Drehungen im Richtungsraum** oder **Richtungsdrehungen** oder auch kurz **Drehungen** nennen. Gegeben $\vec{v} \in \vec{E}$ gibt es nach unseren Annahmen stets eine Drehung $d \in D$ und ein $\lambda \in \mathbb{R}$ mit $d\vec{v} = \lambda\vec{m}$, und dann haben wir notwendig
$$\langle \vec{v}, \vec{v} \rangle = \langle d\vec{v}, d\vec{v} \rangle = \langle \lambda\vec{m}, \lambda\vec{m} \rangle = \lambda^2$$

Das folgende ist eine nicht ganz mathematische Übung: Man schätze ab, ob das durch die eingezeichnete Längeneinheit und die anschauliche Bewegungsgruppe gegebene Skalarprodukt der beiden hier gezeichneten Vektoren größer ist als Zehn. Man verwende dabei nur ein Papier mit einer geraden Kante, das man kniffen darf, um einen rechten Winkel zu erzeugen, einen Bleistift zum Abtragen von Längen, und Augenmaß.

Damit legen unsere Bedingung also $\langle \vec{v}, \vec{v} \rangle$ bereits fest, und $\langle \vec{v}, \vec{v} \rangle$ ist positiv für $\vec{v} \neq 0$. Nun vereinbaren wir für Richtungsvektoren $\vec{v}, \vec{r} \in \vec{E}$ die Sprechweise, $\vec{r}$ sei **drehsenkrecht zu** $\vec{v}$ genau dann, wenn es eine Drehung d gibt mit $d(\vec{v}) = \vec{v}$ und $d(\vec{r}) = -\vec{r}$. Wegen der Drehinvarianz von $\langle\ ,\ \rangle$ muß für $\vec{r}$ drehsenkrecht zu $\vec{v}$ stets gelten $\langle \vec{v}, \vec{r} \rangle = \langle d(\vec{v}), d(\vec{r}) \rangle = \langle \vec{v}, -\vec{r} \rangle = -\langle \vec{v}, \vec{r} \rangle$ und damit

$$\langle \vec{v}, \vec{r} \rangle = 0$$

Sind nun $\vec{v}, \vec{w}$ beliebig und finden wir eine Darstellung $\vec{w} = \gamma\vec{v} + \delta\vec{r}$ mit $\vec{r}$ drehsenkrecht zu $\vec{v}$, so muß mithin sicher gelten

$$\langle \vec{v}, \vec{w} \rangle = \gamma \langle \vec{v}, \vec{v} \rangle$$

Um die Eindeutigkeit unserer Bilinearform nachzuweisen, müssen wir also nur noch zeigen, daß eine derartige Darstellung stets existiert. Ohne Beschränkung der Allgemeinheit dürfen wir dazu $\vec{v}, \vec{w}$ linear unabhängig annehmen. Dann gibt es nach unseren Annahmen genau eine Drehung d, die die Halbgerade $\mathbb{R}_{\geq 0}\vec{v}$ auf sich selber abbildet und die Halbebene $\mathbb{R}\vec{v} + \mathbb{R}_{\geq 0}\vec{w}$ auf die "gegenüberliegende" Halbebene $\mathbb{R}\vec{v} + \mathbb{R}_{\geq 0}(-\vec{w})$. Da dann d^2 sowohl unsere Halbgerade als auch unsere Halbebene auf sich selber abbilden muß, folgt wieder aus unseren Annahmen $d^2 = \mathrm{id}$ und damit $d(\vec{v}) = \vec{v}$. Weiter gilt $d(\vec{w}) = \alpha\vec{v} + \beta\vec{w}$ mit $\beta < 0$ und folglich $\vec{r} := d(\vec{w}) - \vec{w} \neq 0$. Wir haben sicher $d(\vec{r}) = -\vec{r}$, mithin ist $\vec{r}$ drehsenkrecht zu $\vec{v}$ und nach 3.5.20 sind $\vec{v}$ und $\vec{r}$ auch linear unabhängig. Folglich spannen sie bereits die Ebene $\mathbb{R}\vec{v} + \mathbb{R}\vec{w}$ auf und wir finden eine Darstellung $\vec{w} = \gamma\vec{v} + \delta\vec{r}$ der gewünschten Art. Daß unsere Bilinearform auch die Eigenschaft $\langle \vec{v}, \vec{w} \rangle = \langle \vec{w}, \vec{v} \rangle$ haben muß, folgt schließlich unmittelbar aus der Eindeutigkeit. □

4.1.11. Unser Beweis enthält insbesondere die folgende Anleitung zur Konstruktion des Skalarprodukts, ausgehend von einem dreidimensionalen reellen Raum E mit einer ausgezeichneten Bewegungsgruppe $B \subset \mathrm{Aff}^\times E$ und und einem ausgezeichneten von Null verschiedenen Richtungsvektor $\vec{m} \in \vec{E}$: Zunächst erkläre man die **Drehnorm** eines beliebigen Richtungsvektors $\vec{v}$ als diejenige nichtnegative reelle Zahl $\|\vec{v}\| = \lambda$, für die es eine Drehung d gibt mit $d(\vec{v}) = \lambda\vec{m}$. Ich vermeide, hier den Begriff "Länge" zu benutzen, da unsere Drehnorm schlicht reelle Zahlen als Werte annimmt und ich den Begriff "Länge" für die "richtige" Länge frischhalten will, die in 8.6.7 eingeführt wird und die Werte in einem noch zu erklärenden Vektorraum von "Längen" annimmt. Natürlich muß noch gezeigt werden, daß es nicht mehr als ein solches λ geben kann. Das geschieht beim Beweis unseres Satzes in 8.5.11. Dann erinnere man für Richtungsvektoren $\vec{v}, \vec{r} \in \vec{E}$ die Sprechweise, $\vec{r}$ sei drehsenkrecht zu $\vec{v}$ genau dann, wenn es eine Drehung d gibt mit $d(\vec{v}) = \vec{v}$ und $d(\vec{r}) = -\vec{r}$. Gegeben Richtungsvektoren $\vec{v}, \vec{w}$ suche man schließlich eine Darstellung $\vec{w} = \gamma\vec{v} + \delta\vec{r}$ mit $\vec{r}$ drehsenkrecht zu $\vec{v}$ und setze

$$\langle \vec{v}, \vec{w} \rangle = \gamma \|\vec{v}\|^2$$

Anschaulich mag man sich $\gamma\vec{v}$ als die orthogonale Projektion von $\vec{w}$ auf die Gerade $\mathbb{R}\vec{v}$ denken und den Betrag des Skalarprodukts als das Produkt der Drehnorm der orthogonalen Projektion von $\vec{w}$ auf $\mathbb{R}\vec{v}$ mit der Drehnorm von $\vec{v}$, in Formeln $|\langle\vec{v},\vec{w}\rangle| = \|\gamma\vec{v}\| \cdot \|\vec{v}\|$. Damit scheint mir anschaulich klar, daß $\langle\vec{v},\vec{w}\rangle$ bei festem $\vec{v}$ linear in $\vec{w}$ ist. Andererseits ist in dieser Anschauung auch die Identität $\langle\vec{v},\vec{w}\rangle = \langle\vec{w},\vec{v}\rangle$ zunächst für Vektoren gleicher Drehnorm aber dann auch für beliebige Vielfache derselben alias für beliebige Vektoren unmittelbar einleuchtend. Einen formal vollständigen Beweis geben wir jedoch erst in 8.5.11.

4.1.12. Für das solchermaßen aus einer Bewegungsgruppe nebst einem ausgezeichneten von Null verschiedenen Richtungsvektor konstruierte Skalarprodukt erkennt man unmittelbar, daß gegeben zwei Richtungsvektoren $\vec{r}$ und $\vec{v}$ der Vektor $\vec{r}$ drehsenkrecht ist zu $\vec{v}$ genau dann, wenn $\vec{r}$ **skalarproduktsenkrecht** zu $\vec{v}$ ist in dem Sinne, daß gilt $\langle\vec{v},\vec{r}\rangle = 0$. Weiter erkennt man unmittelbar, daß für jeden Richtungsvektor $\vec{v}$ seine Drehnorm übereinstimmt mit seiner **Skalarproduktnorm** $\sqrt{\langle\vec{v},\vec{v}\rangle}$. In Zukunft können wir uns also diese begrifflichen Feinheiten sparen und einfach nur von "aufeinander senkrecht stehenden Vektoren" und von der "Norm eines Vektors" reden.

Ergänzung 4.1.13. Das zweidimensionale Analogon von 4.1.8 gilt nur unter der zusätzlichen Annahme, daß unsere Bewegungsgruppe im Sinne der Topologie "abgeschlossen" sein soll in der Gruppe aller affinen Automorphismen. Die Geometrie des Raums ist erstaunlicherweise unter dem Aspekt der Symmetrie leichter algebraisch zu modellieren als die Geometrie der Ebene. Ich wage aber die Vermutung, daß auch unsere intuitive Vorstellung des Senkrechtstehens von Geraden, selbst wenn sie auf ein Papier gezeichnet sind, von ihrem Wesen her eigentlich räumlicher Natur ist und in etwa dem Konzept entspricht, das ich im vorhergehenden Beweis unter der Bezeichnung "drehsenkrecht" formalisiert habe.

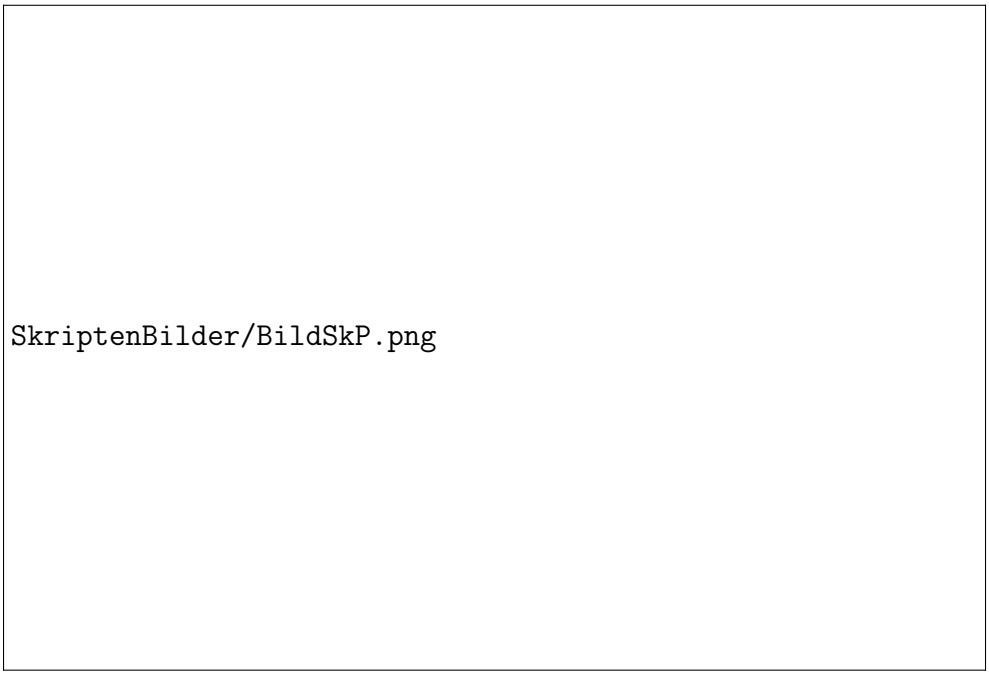
Ergänzende Übung 4.1.14. Man zeige in einem beliebigen Vektorraum mit Skalarprodukt die **Parallelogrammregel**, nach der die Summe der Quadrate der vier Seiten eines Parallelogramms gleich der Summe der Quadrate der beiden Diagonalen ist, in Formeln

$$2\|v\|^2 + 2\|w\|^2 = \|v - w\|^2 + \|v + w\|^2$$

Definition 4.1.15. Wir fixieren von nun an ein für allemal ein Tripel

$$(\mathbb{E}, B, \omega)$$

bestehend aus einem dreidimensionalen reellen affinen Raum $\mathbb{E}$, einer ausgezeichneten Bewegungsgruppe $B \subset \mathrm{Aff}^\times \mathbb{E}$ im Sinne von 4.1.2 und einer ausgezeichneten Orientierung ω im Sinne von 3.2.3. Wir nennen $\mathbb{E}$ den **Anschauungsraum**, B die Gruppe seiner **Bewegungen**, und ω die **rechte-Hand-Orientierung**.



Wählen wir die durch die Kantenlängen unserer Kästchen gegebene Längeneinheit, so ist das zugehörige anschauliche Skalarprodukt der beiden als Pfeile eingezeichneten Vektoren $\langle \vec{v}, \vec{w} \rangle = \langle (4,0), (-2,3) \rangle = -8$ sowohl nach unserer Formel als auch nach der in 4.1.11 erklärten anschaulichen Interpretation, für die Sie sich allerdings noch eine dritte Koordinate hinzudenken müssen.

4.1.16. Ich denke mir $\mathbb{E}$ als den "Raum der Anschauung", die Elemente von B als "Bewegungen", und die "rechte-Hand-Orientierung" als diejenige Orientierung, in der die durch die Abfolge "Daumen-Zeigefinger-Mittelfinger" mit der rechten Hand angedeuteten angeordneten Basen des Richtungsraums positiv orientiert sind. Das mag aber jeder halten, wie er will: Unsere Objekte sind durch die obige Definition 4.1.15 ebenso formal korrekt als Objekte der Mengenlehre eingeführt wie etwa die komplexen Zahlen. Man zeigt auch unschwer, daß es für jedes weitere Tripel $(\mathbb{E}', B', \omega')$ von Objekten der eben spezifizierten Art einen orientierungserhaltenden Isomorphismus $\phi : \mathbb{E} \xrightarrow{\sim} \mathbb{E}'$ von affinen Räumen gibt, unter dem sich die jeweiligen Bewegungsgruppen entsprechen im Sinne einer Gleichheit $B' = \phi B \phi^{-1}$. Das rechtfertigt es, ohne daß man irgendeine Anschauung bemühen müßte, den bestimmten Artikel zu verwenden, wenn wir in der Mathematik von *dem* Anschauungsraum, *der* rechte-Hand-Orientierung etc. reden.

4.2 Geometrie in euklidischen Vektorräumen

4.2.1. Gegeben ein Körper k und ein k-Vektorraum V heißt eine bilineare Abbildung $b : V \times V \to k$ auch eine **Bilinearform auf** V. Wie in 3.3.1 heißt eine Bilinearform **symmetrisch** genau dann, wenn gilt $b(\vec{v}, \vec{w}) = b(\vec{w}, \vec{v})$. Ist k ein angeordneter Körper, so heißt eine Bilinearform **positiv definit** genau dann, wenn gilt $\vec{v} \neq \vec{0} \Rightarrow b(\vec{v}, \vec{v}) > 0$. Mit diesen ganzen Begriffsbildungen kann man dann ein Skalarprodukt auch definieren als eine symmetrische positiv definite Bilinearform.

Beispiel 4.2.2. Auf $V = \mathbb{R}^n$ erhält man ein Skalarprodukt durch die Vorschrift $\langle \vec{v}, \vec{w} \rangle = v_1 w_1 + \ldots + v_n w_n$ für $\vec{v} = (v_1, \ldots, v_n)$ und $\vec{w} = (w_1, \ldots, w_n)$. Es heißt das **Standard-Skalarprodukt**. Man findet für das Standardskalarprodukt oft auch die alternative Notation $\vec{v} \cdot \vec{w}$. Mit dem Formalismus der Matrixmultiplikation können wir es auch schreiben als Produkt eines Zeilenvektors mit einem Spaltenvektor $\langle \vec{v}, \vec{w} \rangle = \vec{v}^\top \circ \vec{w}$, wo wir implizit die offensichtliche Identifikation $\mathrm{M}(1 \times 1; \mathbb{R}) \xrightarrow{\sim} \mathbb{R}$ verwendet haben.

4.2.3. Sei E ein dreidimensionaler reeller affiner Raum mit einer ausgezeichneten Bewegungsgruppe B. Wir wählen einen ausgezeichneten von Null verschiedenen Richtungsvektor $\vec{m} \in \vec{E}$ und betrachten das zugehörige Skalarprodukt $\langle\ ,\ \rangle$ auf seinem Richtungsraum $\vec{E}$ nach 4.1.8. Wählen wir weiter in $\vec{E}$ eine Basis $\vec{v}_1, \vec{v}_2, \vec{v}_3$ von paarweise aufeinander drehsenkrecht stehenden Vektoren der Drehnorm Eins und identifizieren den Richtungsraum vermittels dieser Basis mit dem Koordinatenraum $\mathbb{R}^3$, so entspricht unser Skalarprodukt aus 4.1.8 genau dem Standardskalarprodukt des $\mathbb{R}^3$. In der Tat folgt aus der Bilinearität unseres Skalarprodukts aus 4.1.8 unmittelbar

$$\langle x\vec{v}_1 + y\vec{v}_2 + z\vec{v}_3, x'\vec{v}_1 + y'\vec{v}_2 + z'\vec{v}_3 \rangle = xx' + yy' + zz'$$

4.2.4. Für die nun folgende Erweiterung des Begriffs eines Skalarprodukts ins Komplexe kenne ich ich keine anschauliche Begründung. Es wird sich jedoch erweisen, daß das Zusammenwirken der algebraischen Abgeschlossenheit der komplexen Zahlen mit den Positivitätseigenschaften eines Skalarprodukts mühelos starke Resultate liefert, die auch interessante Konsequenzen für reelle Vektorräume haben, wie etwa die Sätze über die Normalform orthogonaler Matrizen 4.3.23 oder über die Hauptachsentransformation 4.6.1.

Definition 4.2.5. Ein **Skalarprodukt** auf einem komplexen Vektorraum V ist eine Abbildung $V \times V \to \mathbb{C}$, $(\vec{v}, \vec{w}) \mapsto \langle \vec{v}, \vec{w} \rangle$ derart, daß für alle $\vec{v}, \vec{w}, \vec{v}_1, \vec{w}_1 \in V$ und $\lambda, \mu \in \mathbb{C}$ gilt:

1. $\langle \vec{v}, \vec{w} + \vec{w}_1 \rangle = \langle \vec{v}, \vec{w} \rangle + \langle \vec{v}, \vec{w}_1 \rangle$, $\langle \vec{v}, \lambda \vec{w} \rangle = \lambda \langle \vec{v}, \vec{w} \rangle$;
2. $\langle \vec{v} + \vec{v}_1, \vec{w} \rangle = \langle \vec{v}, \vec{w} \rangle + \langle \vec{v}_1, \vec{w} \rangle$, $\langle \mu \vec{v}, \vec{w} \rangle = \bar{\mu} \langle \vec{v}, \vec{w} \rangle$;
3. $\langle \vec{v}, \vec{w} \rangle = \overline{\langle \vec{w}, \vec{v} \rangle}$, insbesondere also $\langle \vec{v}, \vec{v} \rangle \in \mathbb{R}$;
4. $\vec{v} \neq \vec{0} \Rightarrow \langle \vec{v}, \vec{v} \rangle > 0$.

4.2.6. Nebenbei bemerkt folgt hier 2 schon aus 1 und 3, aber es kann auch nicht schaden, diese Formeln nochmal explizit hinzuschreiben. Ganz allgemein heißt eine Abbildung $f : V \to W$ von komplexen Vektorräumen **schieflinear** genau dann, wenn gilt $f(\vec{v} + \vec{w}) = f(\vec{v}) + f(\vec{w})$ und $f(\mu \vec{v}) = \bar{\mu} f(\vec{v})$ für alle $\vec{v}, \vec{w} \in V$ und $\mu \in \mathbb{C}$. Die ersten beiden Teile unserer Definition können also dahingehend zusammengefaßt werden, daß unser Skalarprodukt schieflinear ist im ersten Eintrag und linear im zweiten. Eine Abbildung $V \times V \to \mathbb{C}$, die nur diese beiden Bedingungen 1 und 2 erfüllt, nennt man eine **Sesquilinearform**. Gilt zusätzlich 3, so heißt die Sesquilinearform **hermitesch** nach dem französischen Mathematiker Hermite. Das Standardbeispiel ist $V = \mathbb{C}^n$ mit dem Skalarprodukt $\langle \vec{v}, \vec{w} \rangle = \bar{v}_1 w_1 + \ldots + \bar{v}_n w_n$ für $\vec{v} = (v_1, \ldots, v_n)$ und $\vec{w} = (w_1, \ldots, w_n)$. Mithilfe der Matrixmultiplikation kann dies Skalarprodukt auch geschrieben werden als

$$\langle \vec{v}, \vec{w} \rangle = \overline{\vec{v}}^{\top} \circ \vec{w}$$

wobei der Strich über einer Matrix mit komplexen Einträgen das komplexe Konjugieren aller Einträge meint. Viele Autoren verwenden auch die abweichende Konvention, nach der im komplexen Fall ein Skalarprodukt linear im ersten und schieflinear im zweiten Eintrag sein soll. Ich ziehe die hier gegebene Konvention vor, da dann bei der Interpretation von $\langle \vec{v}, \vec{w} \rangle$ als "$\vec{v}$ auf $\vec{w}$ angewendet" dieses Anwenden von $\vec{v}$ linear ist. In der physikalischen Literatur findet man meist die leicht abweichende Notation $\langle \vec{v} | \vec{w} \rangle$. Eine Anschauung für den komplexen Fall kann ich nicht anbieten, dafür wird er sich aber bei der weiteren Entwicklung der Theorie als außerordentlich nützlich erweisen.

Definition 4.2.7. Einen reellen bzw. komplexen Vektorraum mit Skalarprodukt nennt man auch einen reellen bzw. komplexen **euklidischen Vektorraum**. In einem euklidischen Vektorraum definiert man die **Länge** oder **euklidische Norm** oder kurz **Norm** $\|\vec{v}\| \in \mathbb{R}$ eines Vektors $\vec{v}$ durch $\|\vec{v}\| = \sqrt{\langle \vec{v}, \vec{v} \rangle}$. Daß das tatsächlich im Sinne von **??** eine Norm ist, werden wir gleich als 4.2.20 zeigen. Vektoren der Länge 1 heißen auch **normal**. Zwei Vektoren $\vec{v}, \vec{w}$ heißen **orthogonal** und man schreibt

$$\vec{v} \perp \vec{w}$$

genau dann, wenn gilt $\langle \vec{v}, \vec{w} \rangle = 0$. Man sagt dann auch, $\vec{v}$ und $\vec{w}$ **stehen senkrecht aufeinander**. Manchmal verwendet man das Symbol $\perp$ auch für allgemeinere Teilmengen S, T eines euklidischen Raums und schreibt $S \perp T$ als Abkürzung für $\vec{v} \perp \vec{w} \quad \forall \vec{v} \in S, \vec{w} \in T$.

4.2.8. Viele Autoren reservieren die Bezeichnung als euklidischer Vektorraum für reelle Vektorräume mit Skalarprodukt oder sogar für endlichdimensionale reelle Vektorräume mit Skalarprodukt. Ich verwende sie auch im Komplexen in der Hoffnung, durch die Verwendung dieses Begriffes die Übertragung unserer Anschauung ins Komplexe zu fördern. Üblich ist auch die Bezeichnung eines komplexen Vektorraums mit Skalarprodukt als **unitärer Raum**, im endlichdimensionalen Fall als **endlichdimensionaler Hilbertraum**, und im Kontext der Definition von allgemeinen Hilberträumen als **Prä-Hilbertraum**.

Übung 4.2.9. In einem euklidischen Vektorraum gilt $\|\lambda\vec{v}\| = |\lambda|\|\vec{v}\|$ für alle Vektoren $\vec{v}$ und alle Skalare $\lambda \in \mathbb{R}$ bzw. $\lambda \in \mathbb{C}$.

4.2.10. Stehen zwei Vektoren $\vec{v}, \vec{w}$ eines euklidischen Vektorraums senkrecht aufeinander, so gilt der **Satz des Pythagoras**

$$\|\vec{v} + \vec{w}\|^2 = \|\vec{v}\|^2 + \|\vec{w}\|^2$$

In der Tat folgt ja aus $\vec{v} \perp \vec{w}$ schon

$$\langle \vec{v} + \vec{w}, \vec{v} + \vec{w} \rangle = \langle \vec{v}, \vec{v} \rangle + \langle \vec{v}, \vec{w} \rangle + \langle \vec{w}, \vec{v} \rangle + \langle \vec{w}, \vec{w} \rangle = \langle \vec{v}, \vec{v} \rangle + \langle \vec{w}, \vec{w} \rangle$$

Definition 4.2.11. Eine Familie $(\vec{v}_i)_{i \in I}$ von Vektoren eines euklidischen Vektorraums heißt ein **Orthonormalsystem** genau dann, wenn die Vektoren $\vec{v}_i$ alle die Länge 1 haben und paarweise aufeinander senkrecht stehen, wenn also mit dem Kroneckerdelta aus 1.8.4 in Formeln gilt

$$\langle \vec{v}_i, \vec{v}_j \rangle = \delta_{ij}$$

Ein Orthonormalsystem, das eine Basis ist, heißt eine **Orthonormalbasis**.

4.2.12. Ist V ein euklidischer Vektorraum und $(\vec{v}_i)_{i\in I}$ eine Orthonormalbasis und $\vec{w} = \sum \lambda_i \vec{v}_i$ die Darstellung eines Vektors $\vec{w} \in V$, so erhalten wir durch Davormultiplizieren von $\vec{v}_j$ sofort $\lambda_j = \langle \vec{v}_j, \vec{w}\rangle$.

Proposition 4.2.13. *Jeder endlichdimensionale reelle oder komplexe euklidische Vektorraum besitzt eine Orthonormalbasis.*

Beweis. Ist unser Raum der Nullraum, so tut es die leere Menge. Sonst finden wir einen von Null verschiedenen Vektor und erhalten, indem wir ihn mit dem Kehrwert seiner Länge multiplizieren, sogar einen Vektor $\vec{v}_1$ der Länge Eins. Die lineare Abbildung $\langle \vec{v}_1, \ \rangle$ hat als Kern einen Untervektorraum einer um Eins kleineren Dimension. Eine offensichtliche Induktion beendet dann den Beweis. □

4.2.14. Gegeben ein euklidischer Vektorraum V und eine Teilmenge $T \subset V$ setzen wir

$$T^\perp = \{v \in V \mid v \perp t \ \ \forall t \in T\}$$

und nennen diese Menge den **Orthogonalraum** von T in V. Offensichtlich ist er stets ein Untervektorraum.

Proposition 4.2.15 (Orthogonale Projektion). *Gegeben ein euklidischer Vektorraum V und ein* endlichdimensionaler *Teilraum $U \subset V$ ist der Orthogonalraum von U in V auch ein Vektorraumkomplement, in Formeln*

$$V = U \oplus U^\perp$$

Beweis. Natürlich gilt $U \cap U^\perp = 0$. Es reicht also zu zeigen, daß jeder Vektor $\vec{w} \in V$ dargestellt werden kann als

$$\vec{w} = \vec{p} + \vec{r}$$

mit $\vec{p} \in U$ und $\vec{r} \in U^\perp$. Nach 4.2.13 besitzt nun U eine Orthonormalbasis $\vec{v}_1, \ldots, \vec{v}_n$. Machen wir den Ansatz $\vec{p} = \sum \lambda_i \vec{v}_i$, so folgt $\langle \vec{v}_i, \vec{w}\rangle = \langle \vec{v}_i, \vec{p}\rangle = \lambda_i$ und damit die Eindeutigkeit von $\vec{p}$. Andererseits steht aber mit diesen λ_i der Vektor $\vec{r} = \vec{w} - \sum \lambda_i \vec{v}_i$ auch tatsächlich senkrecht auf allen $\vec{v}_i$, denn wir finden

$$\langle \vec{v}_j, \vec{r}\rangle = \langle \vec{v}_j, \vec{w}\rangle - \sum \lambda_i \langle \vec{v}_j, \vec{v}_i\rangle = \langle \vec{v}_j, \vec{w}\rangle - \lambda_j = 0$$ □

4.2.16. Die Abbildung $\vec{w} \mapsto \vec{p}$ ist offensichtlich linear und heißt die **orthogonale Projektion** auf den Teilraum U. Sie ist in der Terminologie von 1.6.5 die Projektion auf U längs $U^\perp$. Man beachte, daß die orthogonale Projektion von $\vec{w}$ genau derjenige Punkt $\vec{p}$ unseres Teilraums ist, der den kleinsten Abstand zu $\vec{w}$ hat: Für jeden Vektor $\vec{v} \neq \vec{0}$ aus unserem Teilraum gilt nämlich nach Pythagoras

$$\|(\vec{p} + \vec{v}) - \vec{w}\|^2 = \|\vec{p} - \vec{w}\|^2 + \|\vec{v}\|^2 > \|\vec{p} - \vec{w}\|^2$$

4.2.17. Gegeben ein euklidischer Vektorraum V und darin zwei Teilräume $U, W \subset V$ heißt W das **orthogonale Komplement von U in V** genau dann, wenn W sowohl ein Vektorraumkomplement als auch der Orthogonalraum zu U ist. Sagen wir von zwei Teilräumen eines euklidischen Raums, sie stünden aufeinander **orthogonal**, so ist gemeint, daß jeder Vektor des einen Teilraums auf jedem Vektor des anderen Teilraums senkrecht steht.

Übung 4.2.18. Gegeben ein euklidischer Vektorraum V und ein endlichdimensionaler Teilraum $U \subset V$ gilt $U = (U^\perp)^\perp$.

Ergänzende Übung 4.2.19. Man zeige, daß die Menge $\mathrm{L}^2_{\mathbb{R}}(\mathbb{N}) \subset \mathrm{Ens}(\mathbb{N}, \mathbb{R})$ aller reellen Folgen $a_0, a_1, \ldots$ mit $\sum a_i^2 < \infty$ im Raum aller Folgen einen Untervektorraum bildet und daß wir darauf durch die Vorschrift $\langle (a_i), (b_i) \rangle = \sum a_i b_i$ ein Skalarprodukt einführen können. Dann betrachte man in $\mathrm{L}^2_{\mathbb{R}}(\mathbb{N})$ den Untervektorraum U aller Folgen mit höchstens endlich vielen von Null verschiedenen Folgengliedern und zeige $U^\perp = 0$. Insbesondere ist in diesem Fall $U^\perp$ kein orthogonales Komplement zu U. Proposition 4.2.15 gilt also im allgemeinen nicht mehr, wenn wir unendlichdimensionale Teilräume U betrachten. Sie gilt jedoch wieder und sogar genau dann, wenn besagte Teilräume U zusätzlich "vollständig" sind, vergleiche **??**.

Satz 4.2.20. *1. Für beliebige Vektoren $\vec{v}, \vec{w}$ eines euklidischen Vektorraums gilt die* **Cauchy-Schwarz'sche Ungleichung**

$$|\langle \vec{v}, \vec{w} \rangle| \leq \|\vec{v}\| \|\vec{w}\|$$

mit Gleichheit genau dann, wenn $\vec{v}$ und $\vec{w}$ linear abhängig sind.

2. Für beliebige Vektoren $\vec{v}, \vec{w}$ eines euklidischen Vektorraums gilt die **Dreiecksungleichung**

$$\|\vec{v} + \vec{w}\| \leq \|\vec{v}\| + \|\vec{w}\|$$

mit Gleichheit genau dann, wenn einer unserer Vektoren ein nichtnegatives Vielfaches des anderen ist, in Formeln $\vec{v} \in \mathbb{R}_{\geq 0}\vec{w}$ oder $\vec{w} \in \mathbb{R}_{\geq 0}\vec{v}$.

4.2.21. Anschaulich mag man versucht sein, die Dreiecksungleichung zu beweisen, indem man eine Ecke des Dreiecks orthogonal auf die gegenüberliegende Kante projiziert und bemerkt, daß die beiden anderen Kanten dabei nach Pythagoras nur kürzer werden können. Leider führt diese anschaulich überzeugende Beweisidee bei der Ausformulierung jedoch in ein unangenehmes Dickicht von Fallunterscheidungen, so daß die im folgenden gegebene weniger anschauliche Darstellung vielleicht doch vorzuziehen ist.

Illustration zum Beweis der Cauchy-Schwarz'schen Ungleichung. Wir haben darin $\vec{v} = (1, 0)$, $\vec{w} = (9, 6)$, $\langle \vec{v}, \vec{w} \rangle = 9$, $\vec{p} = (9, 0)$, $\vec{r} = (0, 6)$.

Beweis. Um Teil 1 zu zeigen, nehmen wir zunächst $\|\vec{v}\| = 1$ an. Die orthogonale Projektion eines weiteren Vektors $\vec{w}$ auf die Gerade $\mathbb{R}\vec{v}$ wird dann nach 4.2.15 oder genauer seinem Beweis gegeben durch die Formel $\vec{p} = \langle \vec{v}, \vec{w}\rangle \vec{v}$. Erklären wir $\vec{r}$ durch $\vec{w} = \vec{p} + \vec{r}$, so erhalten wir mit Pythagoras

$$\|\vec{w}\|^2 = \|\vec{p}\|^2 + \|\vec{r}\|^2 \geq \|\vec{p}\|^2 = |\langle \vec{v}, \vec{w}\rangle|^2$$

Das zeigt $|\langle \vec{v}, \vec{w}\rangle| \leq \|\vec{v}\|\|\vec{w}\|$ mit Gleichheit genau dann, wenn gilt $\vec{r} = \vec{0}$ alias wenn $\vec{w}$ ein Vielfaches von $\vec{v}$ ist. Diese Ungleichung muß aber offensichtlich erhalten bleiben, wenn wir darin $\vec{v}$ durch ein Vielfaches ersetzen, und so erhalten wir dann für beliebige Vektoren $\vec{v}, \vec{w}$ eines beliebigen euklidischen Vektorraums die Cauchy-Schwarz'sche Ungleichung $|\langle \vec{v}, \vec{w}\rangle| \leq \|\vec{v}\|\|\vec{w}\|$ mit Gleichheit genau dann, wenn $\vec{v}$ und $\vec{w}$ linear abhängig sind. Daraus hinwiederum ergibt sich sofort die Dreiecksungleichung $\|\vec{v} + \vec{w}\| \leq \|\vec{v}\| + \|\vec{w}\|$, indem man beide Seiten quadriert und die Cauchy-Schwarz'sche Ungleichung anwendet. Insbesondere ist unsere euklidische Norm auch eine Norm im Sinne der in der Analysis in **??** gegebenen Definition. Der Beweis der letzten Aussage von Teil 2 sei dem Leser zur Übung überlassen. □

4.2.22. Ist V ein euklidischer Vektorraum und $\vec{v}_1, \ldots, \vec{v}_n$ ein endliches Orthonormalsystem, so ist für jeden Vektor $\vec{w} \in V$ seine orthogonale Projektion $\vec{p}$ auf den von unserem Orthonormalsystem erzeugten Teilraum höchstens so lang wie der Vektor selbst, in Formeln $\|\vec{w}\| \geq \|\vec{p}\|$ alias $\|\vec{w}\|^2 \geq \|\vec{p}\|^2$. Setzen wir hier unsere Darstellung $\vec{p} = \sum \langle \vec{v}_i, \vec{w}\rangle \vec{v}_i$ aus dem Beweis von 4.2.15 ein, so ergibt sich die sogenannte **Bessel'sche Ungleichung**

$$\|\vec{w}\|^2 \geq \sum_{i=1}^{n} |\langle \vec{v}_i, \vec{w}\rangle|^2$$

4.3 Orthogonale und unitäre Abbildungen

Definition 4.3.1. Eine lineare Abbildung $f : V \to W$ von euklidischen Vektorräumen heißt **orthogonal** im Reellen bzw. **unitär** im Komplexen genau dann, wenn sie das Skalarprodukt erhält, in Formeln

$$\langle f(v), f(w)\rangle = \langle v, w\rangle \quad \forall v, w \in V$$

Übung 4.3.2. Eine lineare Abbildung von euklidischen Vektorräumen ist orthogonal bzw. unitär genau dann, wenn sie die Längen aller Vektoren erhält. Hinweis: Im einfacheren reellen Fall zeige man zunächst die sogenannte **Polarisierungsidentität** $2\langle v, w\rangle = \|v + w\|^2 - \|v\|^2 - \|w\|^2$. Im Komplexen gehe man ähnlich vor.

Lemma 4.3.3. *Für eine lineare Abbildung von einem euklidischen Raum in einen weiteren euklidischen Raum sind gleichbedeutend:*

1. *Unsere Abbildung überführt* eine *Orthonormalbasis des Ausgangsraums in ein Orthonormalsystem;*

2. *Unsere Abbildung überführt* jede *Orthonormalbasis des Ausgangsraums in ein Orthonormalsystem;*

3. *Unsere Abbildung ist orthogonal bzw. unitär.*

Beweis. $3 \Rightarrow 2 \Rightarrow 1$ sind offensichtlich und wir müssen nur noch $1 \Rightarrow 3$ zeigen. Bezeichne dazu $f : V \to W$ unsere Abbildung und $B \subset V$ eine Orthonormalbasis. Es gilt zu zeigen $\langle f(v), f(w)\rangle = \langle v, w\rangle \quad \forall v, w \in V$. Wir wissen nach Annahme bereits, daß das gilt für alle $v, w \in B$. Da beide Seiten bilinear bzw. sesquilinear sind als Abbildungen $V \times V \to \mathbb{R}$ bzw. $V \times V \to \mathbb{C}$, folgt es dann jedoch leicht für alle $v, w \in V$. □

Übung 4.3.4. Man zeige: Gegeben ein endlichdimensionaler reeller euklidischer Vektorraum V und darin eine lineare Hyperebene $H \subset V$ gibt es genau eine orthogonale lineare Abbildung $s : V \to V$ mit unserer Hyperebene als Fixpunktmenge, in Formeln $H = V^s$. Diese Abbildung s heißt die **orthogonale Spiegelung an der Hyperebene** H oder auch kürzer die **Spiegelung an** H.

Satz 4.3.5 (Endlichdimensionale euklidische Vektorräume). *Zwischen je zwei euklidischen reellen bzw. komplexen Vektorräumen derselben endlichen Dimension gibt es einen orthogonalen bzw. unitären Isomorphismus.*

Beweis. Wir wählen mit 4.2.13 in beiden Räumen jeweils eine Orthonormalbasis und erklären unseren Isomorphismus durch die Vorschrift, daß er von einer beliebig gewählten Bijektion zwischen den entsprechenden Basen herkommen soll. Nach 4.3.3 ist er dann orthogonal bzw. unitär. □

Definition 4.3.6. Gegeben ein reeller bzw. komplexer euklidischer Vektorraum V bilden die orthogonalen bzw. unitären Automorphismen von V jeweils eine Untergruppe der $\mathrm{GL}(V)$, die wir $\mathrm{O}(V)$ bzw. $\mathrm{U}(V)$ notieren.

Satz 4.3.7 (Matrizen orthogonaler und unitärer Endomorphismen).

1. *Eine Matrix $A \in \mathrm{M}(n \times n; \mathbb{R})$ beschreibt einen orthogonalen Endomorphismus des $\mathbb{R}^n$ mit seinem Standardskalarpodukt genau dann, wenn ihre Transponierte ihre Inverse ist, wenn also in Formeln gilt $A^\top A = I$ alias $A^\top = A^{-1}$.*

2. *Eine Matrix $A \in \mathrm{M}(n \times n; \mathbb{C})$ beschreibt einen unitären Endomorphismus des $\mathbb{C}^n$ mit seinem Standardskalarpodukt genau dann, wenn die Konjugierte ihrer Transponierten ihre Inverse ist, wenn also in Formeln gilt $\bar{A}^\top A = I$ alias $\bar{A}^\top = A^{-1}$.*

Beweis. Wir zeigen gleich den komplexen Fall. Die Identität $\langle Av, Aw\rangle = \langle v, w\rangle$ ist nach unserer Interpretation des Skalarprodukts in Termen der Matrixmultiplikation nach 4.2.6 gleichbedeutend zu $(\overline{Av})^\top (Aw) = \bar{v}^\top w$ alias zu $\bar{v}^\top \bar{A}^\top A w = \bar{v}^\top w$. Gilt $\bar{A}^\top A = I$, so stimmt das natürlich für alle $v, w \in \mathbb{C}^n$. Stimmt es umgekehrt für alle $v, w \in \mathbb{C}^n$, so insbesondere auch für die Vektoren der Standardbasis $\mathrm{e}_i, \mathrm{e}_j$. Damit erhalten wir von der Mitte ausgehend die Gleichungskette $(\bar{A}^\top A)_{ij} = \mathrm{e}_i^\top \bar{A}^\top A \, \mathrm{e}_j = \mathrm{e}_i^\top \mathrm{e}_j = \delta_{ij}$ alias $\bar{A}^\top A = I$. □

Definition 4.3.8. Eine Matrix $A \in \mathrm{M}(n \times n; \mathbb{R})$ heißt **orthogonal** genau dann, wenn gilt $A^\top A = I$. Eine Matrix $A \in \mathrm{M}(n \times n; \mathbb{C})$ heißt **unitär** genau dann, wenn gilt $\bar{A}^\top A = I$. Der vorhergehende Satz 4.3.7 oder auch direkte Rechnung zeigt, daß diese Matrizen Untergruppen von $\mathrm{GL}(n; \mathbb{R})$ bzw. $\mathrm{GL}(n; \mathbb{C})$ bilden. Sie heißen die **orthogonale Gruppe** bzw. die **unitäre Gruppe** und werden notiert

$$\mathrm{O}(n) = \{A \in \mathrm{GL}(n; \mathbb{R}) \mid A^\top A = I\}$$
$$\mathrm{U}(n) = \{A \in \mathrm{GL}(n; \mathbb{C}) \mid \bar{A}^\top A = I\}$$

Definition 4.3.9. Die Elemente der orthogonalen bzw. unitären Gruppen mit Determinante Eins bilden jeweils Untergruppen. Sie heißen die die **spezielle orthogonale Gruppe** bzw. die **spezielle unitäre Gruppe** und werden notiert als

$$\mathrm{SO}(n) = \{A \in \mathrm{O}(n) \mid \det A = 1\}$$
$$\mathrm{SU}(n) = \{A \in \mathrm{U}(n) \mid \det A = 1\}$$

Ähnlich bezeichnen wir für einen endlichdimensionalen reellen bzw. komplexen Vektorraum V mit $\mathrm{SO}(V)$ bzw. $\mathrm{SU}(V)$ die Untergruppen von $\mathrm{GL}(V)$ aller orthogonalen bzw. unitären Automorphismen mit Determinante Eins.

4.3.10. Die Determinante einer unitären oder orthogonalen Matrix hat stets den Betrag Eins. In der Tat folgt aus $\bar{A}^\top A = I$ sofort $1 = \det(\bar{A}^\top A) = \det(\bar{A}^\top) \det(A) = \det(\bar{A}) \det(A) = \overline{\det(A)} \det(A)$. Wir können insbesondere $\mathrm{SO}(n)$ auch als die Gruppe aller orientierungserhaltenden orthogonalen Automorphismen des $\mathbb{R}^n$ beschreiben.

4.3.11. Im Rahmen der Definition von Sinus und Cosinus zeigen wir in **??** folgende unter anderem auch, daß die Abbildung $\mathbb{R} \to \mathrm{M}(2 \times 2; \mathbb{R})$ gegeben durch

$$\vartheta \mapsto R_\vartheta = \begin{pmatrix} \cos\vartheta & -\sin\vartheta \\ \sin\vartheta & \cos\vartheta \end{pmatrix}$$

mit einem R für "Rotation" ein surjektiver Gruppenhomomorphismus mit Kern $2\pi\mathbb{Z}$ von der additiven Gruppe der reellen Zahlen in die Gruppe $\mathrm{SO}(2)$ ist. Das ist auch alles, was wir für die Zwecke dieser Vorlesung von den Funktionen $\sin, \cos : \mathbb{R} \to \mathbb{R}$ wissen müssen. Die Aussage, daß fragliche Abbildung ein Gruppenhomomorphismus ist, ist im übrigen gleichbedeutend zu den Additionstheoremen **??** für Sinus und Cosinus. Aus **??** folgt sogar, daß jeder stetige Gruppenhomomorphismus $\mathbb{R} \to \mathrm{SO}(2)$ von der Form $\vartheta \mapsto R_{a\vartheta}$ ist für genau ein $a \in \mathbb{R}$.

Beispiele 4.3.12. Die einzigen orthogonalen Endomorphismen von $\mathbb{R}$ sind die Identität und die Multiplikation mit (-1), in Formeln $\mathrm{O}(1) = \{1, -1\}$. Die einzigen orthogonalen Endomorphismen der Koordinatenebene $\mathbb{R}^2$ sind die Drehungen um den Ursprung und die Spiegelungen an Geraden durch den Ursprung,

$$\mathrm{O}(2) = \left\{ \begin{pmatrix} \cos\vartheta & -\sin\vartheta \\ \sin\vartheta & \cos\vartheta \end{pmatrix}, \begin{pmatrix} \cos\vartheta & \sin\vartheta \\ \sin\vartheta & -\cos\vartheta \end{pmatrix} \middle| \, 0 \le \vartheta < 2\pi \right\}$$

In der Tat muß für A orthogonal die erste Spalte $A\mathrm{e}_1$ die Länge Eins haben, also auf dem Einheitskreis liegen, also hat sie die Gestalt $(\cos\vartheta, \sin\vartheta)^\top$ für wohlbestimmtes $\vartheta \in [0, 2\pi)$. Die zweite Spalte $A\,\mathrm{e}_2$ muß auch die Länge Eins haben und auf der ersten Spalte senkrecht stehen, und damit verbleiben nur noch die beiden beschriebenen Möglichkeiten. Die erste dieser Möglichkeiten beschreibt anschaulich gesprochen eine Drehung um den Winkel ϑ im Gegenuhrzeigersinn. Die Zweite beschreibt die Spiegelung an der Gerade, die mit der positiven x-Achse in der oberen Halbebene den Winkel $\vartheta/2$ einschließt. Diese Spiegelung hat im übrigen die Eigenwerte 1 und -1. Die Gruppe $\mathrm{SO}(2)$ besteht anschaulich gesprochen gerade aus allen Drehungen der Koordinatenebene um den Ursprung, in Formeln

$$\mathrm{SO}(2) = \left\{ \begin{pmatrix} \cos\vartheta & -\sin\vartheta \\ \sin\vartheta & \cos\vartheta \end{pmatrix} \middle| \, 0 \le \vartheta < 2\pi \right\}$$

Die Gruppe $\mathrm{SO}(3)$ besteht anschaulich gesprochen aus allen Drehungen des Koordinatenraums, wir diskutieren sie gleich noch ausführlicher.

4.3.13. Jeder Eigenwert eines unitären oder orthogonalen Endomorphismus eines euklidischen Vektorraums hat den Betrag Eins, da derartige Abbildungen die Länge von Vektoren erhalten.

Übung 4.3.14. Sei V ein reeller euklidischer Vektorraum. Man zeige:

1. Eine endliche Familie $v_1, \ldots, v_n$ von Vektoren von V ist orthonormal genau dann, wenn die zugehörige Abbildung $\Phi : \mathbb{R}^n \to V$ orthogonal ist für das Standard-Skalarprodukt auf $\mathbb{R}^n$.

2. Gegeben endliche angeordnete Basen $\mathcal{A}, \mathcal{B}$ von V mit $\mathcal{A}$ orthonormal ist $\mathcal{B}$ orthonormal genau dann, wenn die Basiswechselmatrix ${}_{\mathcal{B}}[\mathrm{id}]_{\mathcal{A}}$ orthogonal ist. Hinweis: Man betrachte das kommutative Diagramm

$$\begin{array}{ccc} V & \xrightarrow{\mathrm{id}} & V \\ {\scriptstyle \Phi_{\mathcal{A}}}\uparrow & & \uparrow{\scriptstyle \Phi_{\mathcal{B}}} \\ \mathbb{R}^n & \xrightarrow{{}_{\mathcal{B}}[\mathrm{id}]_{\mathcal{A}}} & \mathbb{R}^n \end{array}$$

Man formuliere und zeige auch die analogen Aussagen im Komplexen.

Satz 4.3.15 (Satz vom Fußball). *Jede orientierungserhaltende orthogonale Selbstabbildung eines dreidimensionalen reellen euklidischen Vektorraums hat mindestens einen von Null verschiedenen Fixvektor.*

4.3.16. Anschaulich gesprochen ist unsere Abbildung demnach eine Drehung um eine Drehachse, eben um die von einem Fixvektor erzeugte Gerade. Heißt unser Raum V, so hat formal jedes $D \in \mathrm{SO}(V)$ in einer geeigneten Orthonormalbasis eine Matrix der Gestalt

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\vartheta & -\sin\vartheta \\ 0 & \sin\vartheta & \cos\vartheta \end{pmatrix}$$

Wird bei einem Fußballspiel der Ball also vor dem Anpfiff zur zweiten Halbzeit wieder in die Mitte gelegt, so befinden sich zwei gegenüberliegende Punkte auf dem Ball jeweils an genau derselben Stelle wie vor dem Anpfiff zur ersten Halbzeit.

Beweis. Sei $D : V \to V$ unsere Abbildung. Das charakteristische Polynom von D hat den Leitterm $-\lambda^3$ und konstanten Term $\det(D) = 1$. Nach dem Zwischenwertsatz hat es also mindestens eine positive reelle Nullstelle, und nach 4.3.13 muß die bei 1 liegen. Folglich hat D einen Fixvektor. Auf der zu diesem Fixvektor orthogonalen Ebene induziert unsere orthogonale Abbildung wieder eine orthogonale Abbildung, die nach Übung 4.5.7 zur Determinante blockdiagonaler Matrizen wieder Determinante Eins hat. Wählen wir also als Orthonormalbasis einen Fixvektor der Länge Eins nebst den beiden Vektoren einer Orthonormalbasis seines orthogonalen Komplements, so hat die Matrix unserer Abbildung in Bezug auf diese Basis nach 4.3.12 die behauptete Gestalt. □

4.3.17. An dieser Stelle stößt mir unangenehm auf, daß wir den Begriff einer "Drehung" bisher nur im Beweis von 4.1.8 als Abkürzung für den Begriff einer "Richtungsdrehung" spezifiziert hatten, womit hinwiederum der lineare Anteil eines beliebigen Elements einer vorgegebenen Bewegungsgruppe gemeint war.

Vereinbaren wir also, daß wir von nun an unter einer **linearen Drehung** oder kurz **Drehung** ein Element einer Gruppe der Gestalt $\mathrm{SO}(V)$ verstehen wollen, für einen beliebigen euklidischen Vektorraum, vorzugsweise der Dimension zwei oder drei, und daß wir im letzteren Fall jede von unserer Drehung punktweise festgehaltene Gerade eine **Drehachse** unserer Drehung nennen. Als Variante werden wir in 4.4.12 noch "affine Drehungen" kennenlernen und auch diese kurz "Drehungen" nennen, aber alles zu seiner Zeit.

Ergänzende Übung 4.3.18. Jede orthogonale Selbstabbildung mit Determinante (-1) eines dreidimensionalen reellen euklidischen Vektorraums ist die Verknüpfung einer Drehung um eine Achse mit einer Spiegelung an der zu dieser Achse senkrechten Hyperebene.

Ergänzende Übung 4.3.19. Jede bezüglich Inklusion maximale kommutative Untergruppe der Drehgruppe $\mathrm{SO}(3)$ ist entweder die Gruppe aller Drehungen um eine Achse oder konjugiert zur Gruppe aller Diagonalmatrizen aus $\mathrm{SO}(3)$.

Satz 4.3.20 (Spektralsatz für unitäre Endomorphismen). *Gegeben ein unitärer Endomorphismus eines endlichdimensionalen komplexen euklidischen Vektorraums gibt es stets eine Orthonormalbasis unseres Vektorraums, die aus Eigenvektoren unseres Endomorphismus besteht.*

Beweis. Ist unser Raum der Nullraum, so tut es die leere Menge. Sonst finden wir nach 3.5.3 einen Eigenvektor und durch Renormieren natürlich auch einen Eigenvektor der Länge Eins. Da unser Endomorphismus unitär ist, erhält er auch den Orthogonalraum dieses Eigenvektors und induziert auf diesem Orthogonalraum eine unitäre Abbildung. Mit Induktion über die Dimension finden wir in unserem Orthogonalraum eine Orthonormalbasis aus Eigenvektoren, und durch Hinzunehmen unseres ursprünglichen Eigenvektors der Länge Eins erhalten wir daraus die gesuchte Orthonormalbasis aus Eigenvektoren des ganzen Raums. □

Übung 4.3.21. Ein Endomorphismus eines endlichdimensionalen komplexen euklidischen Vektorraums ist genau dann unitär, wenn unser Vektorraum eine Orthonormalbasis besitzt, die aus Eigenvektoren unseres Endomorphismus besteht, und wenn zusätzlich alle Eigenwerte Betrag Eins haben.

Korollar 4.3.22. *Für jede unitäre Matrix $A \in \mathrm{U}(n)$ gibt es eine weitere unitäre Matrix $B \in \mathrm{U}(n)$ mit $B^{-1}AB = \mathrm{diag}(z_1, \ldots, z_n)$ für $z_i \in S^1 \subset \mathbb{C}$ komplexe Zahlen der Länge Eins.*

Beweis. Man findet solch eine Matrix B, indem man eine Orthonormalbasis aus Eigenvektoren von $A : \mathbb{C}^n \to \mathbb{C}^n$, die es nach 4.3.20 ja geben muß, als Spaltenvektoren hintereinanderschreibt: Dann gilt ja ganz offensichtlich $AB = \mathrm{diag}(z_1, \ldots, z_n)B$ und die Matrix B ist unitär nach Lemma 4.3.3. □

Satz 4.3.23 (Normalform für orthogonale Matrizen). *Die Matrix einer orthogonalen Abbildung D von einem endlichdimensionalen reellen euklidischen Vektorraum V in sich selber hat stets bezüglich einer geeigneten angeordneten Orthonormalbasis eine blockdiagonale Gestalt der Form*

$$\operatorname{diag}\left(1,\ldots,1,-1,\ldots,-1,\begin{pmatrix}\cos\vartheta & -\sin\vartheta\\ \sin\vartheta & \cos\vartheta\end{pmatrix},\ldots,\begin{pmatrix}\cos\varphi & -\sin\varphi\\ \sin\varphi & \cos\varphi\end{pmatrix}\right)$$

mit Winkeln $0 < \vartheta \leq \ldots \leq \varphi < \pi$, und unter den angegebenen Einschränkungen an die Winkel wird umgekehrt besagte blockdiagonale Matrix durch unsere orthogonale Abbildung D bereits eindeutig festgelegt.

4.3.24. Daraus folgt auch unmittelbar der Satz vom Fußball 4.3.15.

Beweis. Der Drehblock zu einem Winkel ϑ hat die komplexen Eigenwerte $\cos\vartheta \pm \mathrm{i}\sin\vartheta$, und das zeigt bereits die behauptete Eindeutigkeit. Die Existenz ist klar im Fall $\dim_{\mathbb{R}} V < 3$ wegen 4.3.12. Zu beachten ist hierbei, daß jede ebene Spiegelung in einer geeigneten Orthonormalbasis die darstellende Matrix $\operatorname{diag}(1,-1)$ hat und jede ebene Drehung in einer geeigneten Orthonormalbasis als darstellende Matrix entweder $\operatorname{diag}(1,1)$ oder $\operatorname{diag}(-1,-1)$ oder einen Drehblock mit einem Winkel ϑ mit $0 < \vartheta < \pi$: Bei einer Drehung um einen Winkel ϑ mit $\pi < \vartheta < 2\pi$ nehmen wir dazu als Orthonormalbasis des $\mathbb{R}^2$ die Standardbasis mit der umgekehrten Anordnung. Die Existenz folgt mit Induktion im allgemeinen, sobald wir zeigen, daß es unter der Voraussetzung $\dim_{\mathbb{R}} V \geq 3$ in V stets einen echten von Null verschiedenen unter D invarianten Teilraum gibt, indem wir nämlich die Induktionsannahme auf diesen Teilraum und sein orthogonales Komplement anwenden. Ohne Beschränkung der Allgemeinheit dürfen wir $V = \mathbb{R}^n$ annehmen. Nun hat D schon unter der Annahme $n \geq 1$ stets einen Eigenvektor $v = (v_1,\ldots,v_n)^\top \in \mathbb{C}^n$, sagen wir $Dv = \lambda v$ mit $\lambda \in \mathbb{C}$. Dann folgt für $\bar{v} = (\bar{v}_1,\ldots,\bar{v}_n)^\top$ sofort $D\bar{v} = \bar{\lambda}\bar{v}$ und das komplexe Erzeugnis $\langle v,\bar{v}\rangle_{\mathbb{C}}$ dieser beiden Vektoren ist sicher auch ein echter D-stabiler Teilraum von $\mathbb{C}^n$. Der Schnitt $\langle v,\bar{v}\rangle_{\mathbb{C}} \cap \mathbb{R}^n$ ist also ein echter D-stabiler Teilraum von $\mathbb{R}^n$. Dieser Schnitt ist aber auch nicht Null, denn er enthält sowohl $v + \bar{v}$ als auch $\mathrm{i}(v - \bar{v})$, die wegen $v \neq 0$ nicht beide verschwinden können. □

Ergänzende Übung 4.3.25. Bezeichne $R^x_\varphi \in \mathrm{SO}(3)$ die Drehung um die x-Achse $\mathbb{R}\,\mathrm{e}_1$ mit dem Winkel φ, in Formeln

$$R^x_\varphi = \begin{pmatrix}1 & 0 & 0\\ 0 & \cos\varphi & -\sin\varphi\\ 0 & \sin\varphi & \cos\varphi\end{pmatrix}$$

Bezeichne $R^z_\varphi \in \mathrm{SO}(3)$ die Drehung um die z-Achse $\mathbb{R}\,\mathrm{e}_3$ mit dem Winkel φ, in Formeln

$$R^z_\varphi = \begin{pmatrix} \cos\varphi & -\sin\varphi & 0 \\ \sin\varphi & \cos\varphi & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Man zeige: Jede Drehung $D \in \mathrm{SO}(3)$ läßt sich darstellen als

$$D = R^z_\varphi R^x_\psi R^z_\vartheta$$

mit $\psi \in [0,\pi]$ und $\varphi, \vartheta \in [0, 2\pi)$. Gilt $\mathrm{e}_3 \neq \pm D(\mathrm{e}_3)$, so ist diese Darstellung sogar eindeutig. Die fraglichen Winkel heißen dann die **Euler'schen Winkel** unserer Drehung D. Hinweis: Aus der Anschauung, deren Formalisierung Ihnen überlassen bleiben möge, finden wir $\psi \in [0,\pi]$ und $\varphi \in [0, 2\pi)$ mit $R^z_\varphi R^x_\psi(\mathrm{e}_3) = D(\mathrm{e}_3)$. Es folgt $D^{-1}R^z_\varphi R^x_\psi = R^z_{-\vartheta}$ für geeignetes $\vartheta \in [0, 2\pi)$.

Satz 4.3.26 (Gram-Schmidt). *Seien $v_1, \ldots, v_k$ linear unabhängige Vektoren eines euklidischen Vektorraums. So existiert in unserem Vektorraum genau ein Orthonormalsystem $w_1, \ldots, w_k$ mit*

$$w_i \in \mathbb{R}_{>0} v_i + \langle v_{i-1}, \ldots, v_1 \rangle \quad \forall i$$

Beweis. Nach 4.2.15 können wir v_i eindeutig zerlegen als $v_i = p_i + r_i$ mit p_i der orthogonalen Projektion von v_i auf $\langle v_{i-1}, \ldots v_1 \rangle$ und r_i im orthogonalen Komplement dieses Teilraums. Die Vektoren $w_i = r_i/\|r_i\|$ bilden dann ein Orthonormalsystem mit den geforderten Eigenschaften. Daß es auch das einzige ist, mag sich der Leser zur Übung selbst überlegen. □

4.3.27 (**Gram-Schmidt'sches Orthogonalisierungsverfahren**). In Worten läuft der Beweis also wie folgt ab: Gegeben ist eine endliche angeordnete linear unabhängige Teilmenge unseres euklidischen Vektorraums. Wir beginnen mit dem ersten Vektor und normieren ihn auf Länge Eins. Dann nehmen wir uns den zweiten Vektor vor, machen ihn senkrecht zum ersten Vektor, indem wir seine orthogonale Projektion auf die vom ersten Vektor erzeugte Gerade von ihm abziehen, und normieren den so entstehenden Vektor wieder auf Länge Eins. Dann nehmen wir uns den dritten Vektor vor, machen ihn senkrecht zu den ersten beiden Vektoren, indem wir seine orthogonale Projektion auf die von den ersten beiden Vektoren erzeugte Ebene von ihm abziehen, und normieren den so entstehenden Vektor wieder auf Länge Eins. Und so machen wir immer weiter, bis wir alle Eingaben verarbeitet haben. Mit dem Normieren eines von Null verschiedenen Vektors ist dabei das Multiplizieren unseres Vektors mit dem Inversen seiner Länge gemeint. Wir schreiben das nun noch in Formeln mit den Notationen des vorhergehenden Satzes. Für unsere Basen gilt sicher $\langle w_{i-1}, \ldots, w_1 \rangle \subset \langle v_{i-1}, \ldots, v_1 \rangle$ und Dimensionsvergleich liefert sogar die Gleichheit dieser Erzeugnisse. Nach der Formel

für orthogonale Projektionen aus dem Beweis von 4.2.15 können wir also die w_i induktiv bestimmen durch die Formeln

$$\begin{aligned} r_1 &= v_1 \\ w_1 &= r_1/\|r_1\| \\ &\vdots \\ r_i &= v_i - \textstyle\sum_{\nu=1}^{i-1} \langle w_\nu, v_i\rangle w_\nu \\ w_i &= r_i/\|r_i\| \\ &\vdots \end{aligned}$$

Das ist das "Gram-Schmidt'sche Orthogonalisierungsverfahren".

Korollar 4.3.28 (Iwasawa-Zerlegung für $\mathrm{GL}(n;\mathbb{R})$). *Bezeichne $A \subset \mathrm{GL}(n;\mathbb{R})$ die Menge aller Diagonalmatrizen mit positiven Einträgen auf der Diagonale und $N \subset \mathrm{GL}(n;\mathbb{R})$ die Menge aller oberen Dreiecksmatrizen mit Einsen auf der Diagonale. So liefert die Multiplikation eine Bijektion*

$$\mathrm{O}(n) \times A \times N \xrightarrow{\sim} \mathrm{GL}(n;\mathbb{R})$$

Beweis. Sicher gilt $A \cap N = \{I\}$, folglich definiert die Multiplikation eine Injektion

$$A \times N \hookrightarrow \mathrm{GL}(n;\mathbb{R})$$

Deren Bild AN ist nun offensichtlich eine Untergruppe, genauer die Gruppe der oberen Dreiecksmatrizen mit positiven Diagonaleinträgen, und wegen $\mathrm{O}(n) \cap AN = \{I\}$ definiert die Multiplikation schon mal eine Injektion $\mathrm{O}(n) \times AN \hookrightarrow \mathrm{GL}(n;\mathbb{R})$. Es bleibt, deren Surjektivität zu zeigen. Dazu betrachten wir in $\mathbb{R}^n$ die Standardbasis $\mathcal{S}$, eine beliebige angeordnete Basis $\mathcal{B}$ und die im Gram-Schmidt-Verfahren daraus entstehende angeordnete Basis $\mathcal{A}$. Unser Satz liefert für die zugehörige Basiswechselmatrix obere Dreiecksgestalt mit positiven Diagonaleinträgen, in Formeln

$${}_{\mathcal{B}}[\mathrm{id}]_{\mathcal{A}} \in AN$$

Aus ${}_{\mathcal{B}}[\mathrm{id}]_{\mathcal{A}} \circ {}_{\mathcal{A}}[\mathrm{id}]_{\mathcal{S}} = {}_{\mathcal{B}}[\mathrm{id}]_{\mathcal{S}}$ folgt dann die Surjektivität der Multiplikation $AN \times \mathrm{O}(n) \to \mathrm{GL}(n;\mathbb{R})$. Invertieren liefert den Rest. □

Korollar 4.3.29 (Iwasawa-Zerlegung für $\mathrm{GL}(n;\mathbb{C})$). *Bezeichne $A \subset \mathrm{GL}(n;\mathbb{C})$ die Menge aller Diagonalmatrizen mit reellen positiven Einträgen auf der Diagonale und $N \subset \mathrm{GL}(n;\mathbb{C})$ die Menge aller oberen Dreiecksmatrizen mit Einsen auf der Diagonale. So liefert die Multiplikation eine Bijektion*

$$\mathrm{U}(n) \times A \times N \xrightarrow{\sim} \mathrm{GL}(n;\mathbb{C})$$

Beweis. Der Beweis geht analog wie im Reellen. □

Übung 4.3.30. Man zeige: Für jede komplexe quadratische Matrix A gibt es eine unitäre Matrix U derart, daß UAU^{-1} obere Dreiecksgestalt hat. Hinweis: Trigonalisierbarkeit und Gram-Schmidt.

Definition 4.3.31. Eine Matrix A heißt **symmetrisch** genau dann, wenn sie mit ihrer eigenen Transponierten übereinstimmt, in Formeln $A^\top = A$. Eine symmetrische Matrix $A \in \mathrm{M}(n \times n; \mathbb{R})$ heißt **positiv definit** genau dann, wenn gilt $x^\top Ax \leq 0 \Rightarrow x = 0$. Sie heißt **positiv semidefinit** genau dann, wenn gilt $x^\top Ax \geq 0 \; \forall x \in \mathbb{R}^n$.

Korollar 4.3.32 (Cholesky-Zerlegung). *Gegeben eine positiv definite symmetrische Matrix $A \in \mathrm{M}(n \times n; \mathbb{R})$ gibt es genau eine untere Dreiecksmatrix L mit positiven Diagonaleinträgen und der Eigenschaft*

$$A = LL^\top$$

4.3.33. Das L steht hier für englisch “lower triangular”.

Beweis. Wir betrachten auf dem $\mathbb{R}^n$ das durch die Vorschrift $s(x, y) = x^\top Ay$ erklärte Skalarprodukt $s = s_A$. Wenden wir nun das Gram-Schmidt-Verfahren an auf die Standardbasis $\mathrm{e}_1, \ldots, \mathrm{e}_n$ des $\mathbb{R}^n$, so erhalten wir eine neue Basis $w_1, \ldots, w_n$ des $\mathbb{R}^n$ mit $w_i^\top Aw_j = \delta_{i,j}$ und $w_i \in \mathbb{R}_{>0}\, \mathrm{e}_i + \langle \mathrm{e}_{i-1}, \ldots, \mathrm{e}_1 \rangle$. Die Matrix $U := (w_1 | \ldots | w_n)$ mit den w_i in den Spalten ist also eine obere Dreiecksmatrix mit der Eigenschaft $U^\top AU = I$. Mit $L = (U^\top)^{-1}$ ergibt sich dann die gesuchte Zerlegung. Deren Eindeutigkeit zeigt man, indem man den Beweis rückwärts liest. □

4.3.34. Das Invertieren einer oberen Dreiecksmatrix U mit positiven Diagonaleinträgen ist im Prinzip unproblematisch. Bei der numerischen Berechnung der Cholesky-Zerlegung empfiehlt sich jedoch, das Invertieren gleich mit dem Algorithmus des Gram-Schmidt’schen Orthogonalisierungsverfahrens zu verschmelzen. Mehr dazu mögen Sie in der Numerik lernen.

4.4 Isometrien euklidischer affiner Räume

Definition 4.4.1. Ein **euklidischer Raum** oder genauer **euklidischer reeller affiner Raum** ist ein Paar bestehend aus einem reellen affinen Raum und einem Skalarprodukt auf seinem Richtungsraum. Gegeben zwei Punkte p, q eines euklidischen reellen affinen Raums definieren wir ihren **Abstand** als die Länge des durch dieses Paar von Punkten erklärten Richtungsvektors, in Formeln

$$d(p, q) = \|p - q\|$$

Eine Abbildung $f : E \to E'$ zwischen reellen euklidischen affinen Räumen, die alle Abstände erhält, nennt man auch **isometrisch** oder eine **Isometrie**. Die Terminologie geht auf griechisch $\iota\sigma o\varsigma$ für deutsch "gleich" zurück. In Formeln fordern wir von einer Isometrie also

$$d(f(p), f(q)) = d(p, q) \quad \forall p, q \in E$$

Dieselbe Begriffsbildung verwendet man auch allgemeiner für Abbildungen zwischen sogenannten "metrischen Räumen", wie sie etwa in **??** erklärt werden. Ist eine Isometrie bijektiv, so spricht man auch von einem **isometrischen Isomorphismus**. Sprechen wir von einer **Isometrie eines Raums**, so meinen wir eine Abbildung dieses Raums in sich selber, die eine Isometrie ist.

4.4.2. Ich habe auch eine alternative Terminologie gesehen, in der nur unsere isometrischen Isomorphismen als "Isometrien" bezeichnet werden und unsere Isometrien als "isometrische Abbildungen".

Übung 4.4.3. Zwischen je zwei euklidischen reellen affinen Räumen derselben endlichen Dimension gibt es einen affinen isometrischen Isomorphismus.

Satz 4.4.4 (Charakterisierung der Isometrien affiner Räume). *Eine Abbildung zwischen euklidischen reellen affinen Räumen ist eine Isometrie genau dann, wenn sie affin ist mit orthogonalem linearen Anteil.*

Beweis. Sei $\varphi : E \to F$ unsere Abbildung und sei $p \in E$ beliebig gewählt. Erklären wir die Abbildung $\vec{\varphi} : \vec{E} \to \vec{F}$ durch die Vorschrift $\varphi(p + \vec{v}) = \varphi(p) + \vec{\varphi}(\vec{v})$, so bildet $\vec{\varphi} : \vec{E} \to \vec{F}$ offensichtlich den Ursprung auf den Ursprung ab und erhält alle Abstände. Nach der Proposition 4.4.5, die wir im Anschluß beweisen, ist folglich $\vec{\varphi}$ linear und orthogonal und damit φ affin mit orthogonalem linearem Anteil. Der Beweis der Gegenrichtung kann dem Leser überlassen bleiben. □

Proposition 4.4.5. *Gegeben reelle euklidische Vektorräume V, W ist eine Abbildung $f : V \to W$ orthogonal genau dann, wenn sie den Ursprung auf den Ursprung abbildet und alle Abstände erhält, in Formeln*

$$\|f(v) - f(w)\| = \|v - w\| \quad \forall v, w \in V$$

4.4.6. Man beachte, daß hier die Linearität von f hier nicht vorausgesetzt wird. Vielmehr wird sie aus unseren Annahmen bereits folgen.

Beweis. Zunächst beachten wir die Polarisierungsidentität

$$2\langle v, w\rangle = \|v + w\|^2 - \|v\|^2 - \|w\|^2$$

oder für diesen Beweis besser ihre Variante $2\langle v,w\rangle = \|v\|^2 + \|w\|^2 - \|v-w\|^2$. Da unsere Abbildung den Ursprung und alle Abstände erhält, erhält sie auch die Norm aller Vektoren, und wir folgern schon einmal

$$\langle f(v), f(w)\rangle = \langle v, w\rangle \quad \forall v, w \in V$$

Um weiter $f(\lambda v) = \lambda f(v)$ zu zeigen, beachten wir

$$\langle f(\lambda v) - \lambda f(v), f(u)\rangle = \langle \lambda v, u\rangle - \lambda\langle v, u\rangle = 0$$

für alle $u \in V$ und folgern $\langle f(\lambda v) - \lambda f(v), z\rangle = 0$ für alle z im Erzeugnis des Bildes $f(V)$. Nehmen wir dann speziell $z = f(\lambda v) - \lambda f(v)$, so ergibt sich erst $\|f(\lambda v) - \lambda f(v)\|^2 = 0$ und dann $f(\lambda v) = \lambda f(v)$. In derselben Weise finden wir

$$\langle f(v+w) - f(v) - f(w), f(u)\rangle = \langle v+w, u\rangle - \langle v, u\rangle - \langle w, u\rangle = 0$$

und folgern $f(v+w) = f(v) + f(w)$, womit dann auch die Linearität von f gezeigt wäre. □

Übung 4.4.7. Man zeige: Gegeben ein endlichdimensionaler reeller affiner euklidischer Raum E und darin eine affine Hyperebene $H \subset V$ gibt es genau eine Isometrie $s : E \to E$ mit unserer Hyperebene als Fixpunktmenge, in Formeln $H = E^s$. Diese Abbildung s heißt die **orthogonale Spiegelung an der Hyperebene** H oder auch kürzer die **Spiegelung an** H. Hinweis: 4.4.7.

4.4.8. Aus der Schule kennen Sie vermutlich bereits **Punktspiegelungen**, die für einen beliebigen aber festen Punkt p eines affinen Raums durch die Vorschrift $p + \vec{v} \mapsto p - \vec{v}$ gegeben werden. Wir wollen jedoch vereinbaren, daß wenn ohne nähere Spezifikation von **Spiegelungen** die Rede ist, stets lineare oder affine Abbildungen mit einer Fixpunktmenge der Kodimension Eins gemeint sind, deren Quadrat die Identität ist. Unsere Punktspiegelungen heißen zwar verwirrenderweise so ähnlich, sind aber nur im eindimensionalen Fall Spiegelungen in unserem Sinne.

Satz 4.4.9 (Klassifikation der Isometrien affiner Räume). *Gegeben eine Isometrie φ eines endlichdimensionalen reellen affinen euklidischen Raums gibt es genau ein Paar $(d, \vec{w})$ bestehend aus einer Isometrie d mit mindestens einem Fixpunkt und einem Richtungsvektor $\vec{w}$ derart, daß gilt*

$$\varphi = (+\vec{w}) \circ d \quad \textit{und} \quad \vec{d}(\vec{w}) = \vec{w}$$

4.4.10. In Worten läßt sich also jede Isometrie φ eines endlichdimensionalen reellen affinen euklidischen Raums eindeutig darstellen als die Verknüpfung einer Isometrie d mit Fixpunkt gefolgt von einer Verschiebung um einen unter besagter

Isometrie mit Fixpunkt invarianten Richtungsvektor. Natürlich haben dann d und φ denselben linearen Anteil, in Formeln $\vec{d} = \vec{\varphi}$, und unsere Isometrie kann dargestellt werden durch eine Abbildungsvorschrift der Gestalt $\varphi(x+\vec{u}) = x+\vec{\varphi}(\vec{u})+\vec{w}$ mit $\vec{w}$ einem Fixvektor von $\vec{\varphi}$. Als x kann man dazu einen beliebigen Fixpunkt von d wählen.

Beweis. Gegeben ein orthogonaler Automorphismus f eines endlichdimensionalen euklidischen Vektorraums V ist $\ker(f - \mathrm{id}) = V^f$ das orthogonale Komplement von $\mathrm{im}(f - \mathrm{id})$ in V, in Formeln

$$V^f = \mathrm{im}(f - \mathrm{id})^\perp$$

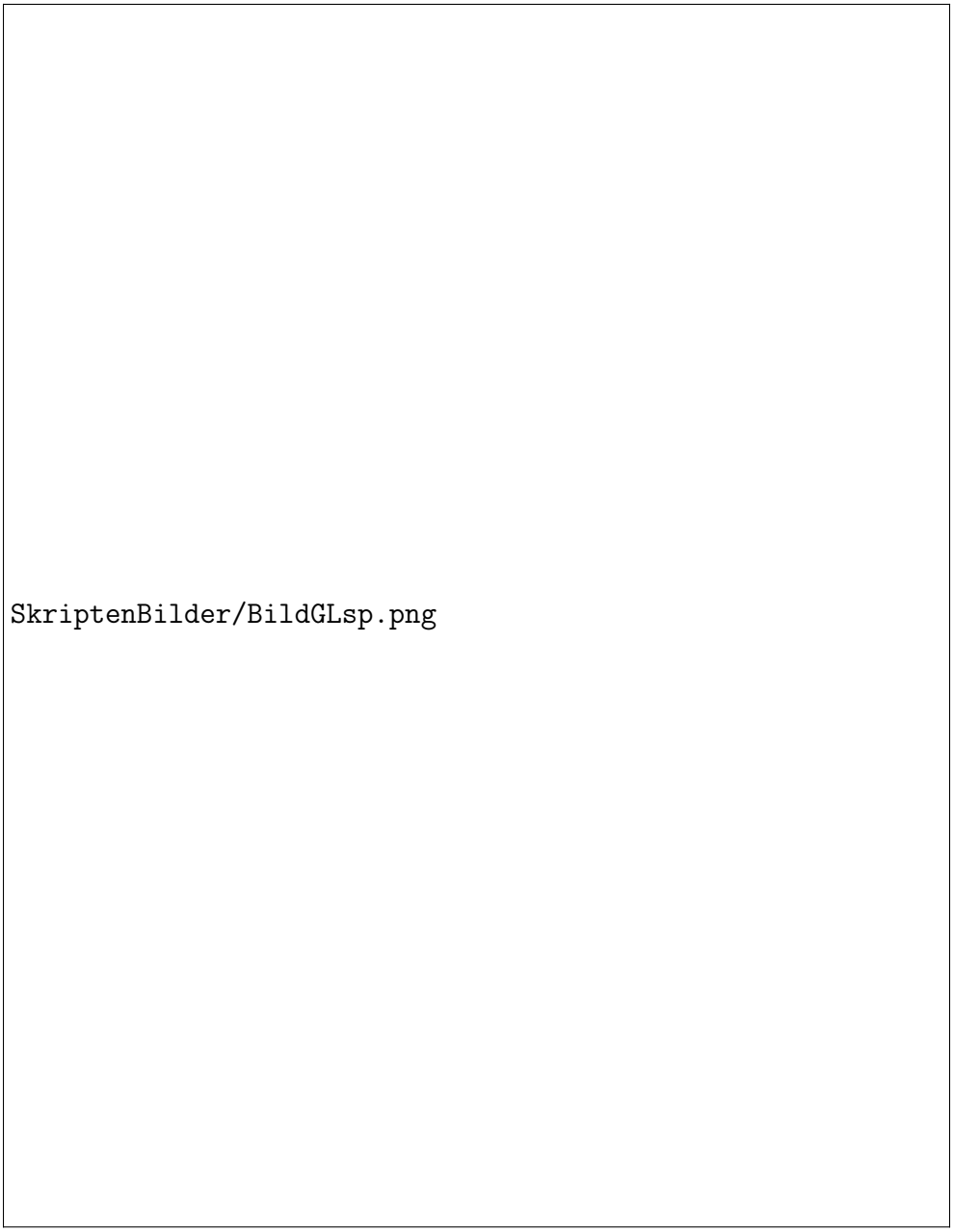
In der Tat zeigt die Dimensionsformel 1.6.12 in Verbindung mit 4.2.15, daß es ausreicht, die Inklusion $V^f \subset \mathrm{im}(f - \mathrm{id})^\perp$ zu zeigen. Aus $f(\vec{w}) = \vec{w}$ folgt aber offensichtlich $\langle \vec{w}, f(\vec{v}) - \vec{v}\rangle = \langle f(\vec{w}), f(\vec{v})\rangle - \langle \vec{w}, \vec{v}\rangle = 0$ für alle $\vec{v} \in V$. Nun kann man ja für einen beliebigen Punkt $p \in E$ stets einen Vektor $\vec{v} \in \vec{E}$ finden mit $\varphi(p+\vec{u}) = p+\vec{\varphi}(\vec{u})+\vec{v}\ \forall \vec{u}$. Genau dann besitzt damit $(-\vec{w}) \circ \varphi$ einen Fixpunkt, wenn es $\vec{u} \in \vec{E}$ gibt mit

$$p + \vec{u} = p + \vec{\varphi}(\vec{u}) + \vec{v} - \vec{w}$$

alias $\vec{u} - \vec{\varphi}(\vec{u}) + \vec{w} = \vec{v}$. Wegen der Zerlegung $\vec{E} = \mathrm{im}(\vec{\varphi} - \mathrm{id}) \oplus \vec{E}^{\vec{\varphi}}$ vom Beginn des Beweises gibt es also genau ein $\vec{w} \in \vec{E}^{\vec{\varphi}}$ derart, daß $(-\vec{w}) \circ \varphi$ einen Fixpunkt hat. □

Beispiel 4.4.11 (**Isometrien der Gerade**). Jede abstandserhaltende Selbstabbildung der reellen Zahlengeraden ist entweder eine Verschiebung $x \mapsto x + a$ oder eine Spiegelung $x \mapsto b - x$: In der Tat, ist der lineare Anteil unserer Selbstabbildung die Identität, so handelt es sich nach 4.4.10 um eine Verschiebung; ist ihr linearer Anteil dahingegen das Negative der Identität, so muß in der Darstellung nach 4.4.10 der Vektor $\vec{w}$ der Nullvektor sein und wir haben eine Abbildung der Gestalt $x + \vec{u} \mapsto x - \vec{u}$ vor uns, die man wohl elementargeometrisch eine "Spiegelung am Punkt x" nennen würde. Wir werden jedoch unter Spiegelungen stets Spiegelungen an Hyperebenen verstehen wollen.

4.4.12. Unter einer **affinen Drehung** oder kurz **Drehung** verstehen wir eine orientierungserhaltende Isometrie eines reellen affinen euklidischen Raums einer Dimension zwei oder drei, die einen Punkt bzw. eine Gerade punktweise festhält. Im ersteren Fall nennen wir jeden Fixpunkt ein **Drehzentrum**, im letzteren Fall jede von unserer Drehung punktweise festgehaltene Gerade eine **Drehachse** unserer Drehung.



Das Bild der durchgezeichneten Figur unter einer Verschiebung (gepunktelt) und unter einer Gleitspiegelung (gestrichelt). Durchgezogen eingezeichnet ist auch die Gerade, längs derer die Gleitspiegelung geschieht. Unsere Gleitspiegelung ist natürlich, wie von unserem Satz 4.4.9 vorhergesagt, die Verknüpfung einer Isometrie mit mindestens einem Fixpunkt, hier einer Spiegelung, mit einer Translation in einer unter dem linearen Anteil dieser Isometrie invarianten Richtung, hier in Richtung der Spiegelachse.

Beispiel 4.4.13 (**Isometrien der Ebene**). Jede abstandserhaltende Selbstabbildung einer reellen euklidischen Ebene ist entweder (1) eine Verschiebung oder (2) eine Drehung um einen Punkt oder (3) eine **Gleitspiegelung**, d.h. eine Spiegelung an einer Gerade gefolgt von einer Verschiebung in Richtung eben dieser Gerade. In der Tat erhalten wir nach 4.4.10 Fall (1) für die Isometrien mit der Identität als linearem Anteil; Fall (2) für die Isometrien mit einer von der Identität verschiedenen Drehung als linearem Anteil; und Fall (3) für die Isometrien mit einer Spiegelung als linearem Anteil.

Beispiel 4.4.14 (**Isometrien des Raums**). Jede abstandserhaltende Selbstabbildung eines reellen dreidimensionalen euklidischen Raums ist entweder (1) eine **Verschraubung** alias eine Drehung um eine Achse gefolgt von einer Verschiebung in Richtung eben dieser Achse, oder (2) eine Drehung um eine Achse gefolgt von einer Spiegelung an einer Ebene senkrecht zu besagter Achse, oder (3) eine Verschiebung gefolgt von einer Spiegelung an einer unter besagter Verschiebung stabilen Ebene. In der Tat erhalten wir nach 4.4.10 Fall (1) für die Isometrien mit einer Drehung als linearem Anteil; Fall (2) für die Isometrien mit linearem Anteil bestehend im Sinne von 4.3.23 aus einem Drehblock und einem Eintrag (-1) auf der Diagonalen; und Fall (3) für die Isometrien mit einer Spiegelung an einer Ebene als linearem Anteil.

Übung 4.4.15. Welcher Fall im vorhergehenden Beispiel 4.4.14 deckt die sogenannten **räumlichen Punktspiegelungen** ab, die für einen festen Punkt p durch die Vorschrift $p + \vec{v} \mapsto p - \vec{v}$ gegeben werden?

Übung 4.4.16. Man zeige, daß die orientierungserhaltenden Isometrien eines dreidimensionalen reellen affinen euklidischen Raums eine Bewegungsgruppe im Sinne von 4.1.2 bilden.

4.5 Winkel und Kreuzprodukt

Definition 4.5.1. Gegeben von Null verschiedene Vektoren $\vec{v}, \vec{w}$ eines reellen euklidischen Vektorraums ist der **von** $\vec{v}$ **und** $\vec{w}$ **eingeschlossene Winkel** $\vartheta \in [0, \pi]$ erklärt durch die Vorschrift

$$\cos\vartheta = \frac{\langle \vec{v}, \vec{w}\rangle}{\|\vec{v}\|\|\vec{w}\|}$$

Nach der Cauchy-Schwarz'schen Ungleichung 4.2.20 liegt der Quotient auf der rechten Seite dieser Gleichung stets im Intervall $[-1, 1]$ und nach **??** existiert stets genau ein Winkel $\vartheta \in [0, \pi]$ zu jedem in $[-1, 1]$ vorgegebenen Wert von $\cos\vartheta$. Man notiert diesen Winkel auch

$$\vartheta = \angle(\vec{v}, \vec{w}) = \arccos\left(\frac{\langle \vec{v}, \vec{w}\rangle}{\|\vec{v}\|\|\vec{w}\|}\right)$$

Ich verstehe stets $\cos$ im Sinne von **??** als die Abbildung $\cos : \mathbb{R} \to \mathbb{R}$, die von einem "Winkel im Bogenmaß" ausgeht, so daß etwa gilt $\cos(\pi/2) = 0$.

4.5.2. Definieren kann man viel. Wie wäre es zum Beispiel mit der Alternative, den Winkel stattdessen als den Arcustangens von $\langle \vec{v}, \vec{w} \rangle^2 / \|\vec{v}\|^3 \|\vec{w}\|^3$ zu erklären? Ich will im folgenden und insbesondere in 4.5.15 diskutieren, inwiefern die vorstehende Definition 4.5.1 unserer anschaulichen Vorstellung eines Winkels entspricht.

4.5.3. Gegeben $\lambda, \mu > 0$ gilt schon mal $\angle(\vec{v}, \vec{w}) = \angle(\lambda\vec{v}, \mu\vec{w})$. Weiter stehen zwei von Null verschiedene Vektoren aufeinander senkrecht im Sinne von 4.2.7 genau dann, wenn sie den Winkel $\pi/2$ einschließen. Damit sind schon mal einige Eigenschaften, die wir von einer vernünftigen Definition eines Winkels erwarten sollten, erfüllt.

Beispiel 4.5.4. Die drei Vektoren der Standardbasis des $\mathbb{R}^3$ bilden ja wohl ein gleichseitiges Dreieck und der Winkel an jeder Ecke sollte folglich $\pi/3$ sein. In der Tat finden wir für $\vec{v} = \vec{e}_3 - \vec{e}_1$ und $\vec{w} = \vec{e}_2 - \vec{e}_1$ als Skalarprodukt $\langle \vec{v}, \vec{w} \rangle = 1$ und wegen $\|\vec{v}\| = \|\vec{w}\| = \sqrt{2}$ ergibt sich für den Winkel $\cos\vartheta = 1/2$ alias $\vartheta = \pi/3$.

Übung 4.5.5. Gegeben zwei vom selben Punkt p ausgehende Halbgeraden L, R in einem euklidischen affinen Raum definiert man ihren Winkel $\angle(L, R)$ als $\angle(l - p, r - p)$ für beliebige $l \in L \backslash p$, $r \in R \backslash p$. Gegeben zwei Paare (L, R) und (L', R') von jeweils vom selben Punkt ausgehenden Halbgeraden in einem endlichdimensionalen euklidischen affinen Raum zeige man, daß es genau dann eine Isometrie b von unserem Raum auf sich selber gibt mit $b(L) = L'$ und $b(R) = R'$, wenn unsere beiden Paare von Halbgeraden jeweils denselben Winkel einschließen, in Formeln $\angle(L, R) = \angle(L', R')$.

Ergänzende Übung 4.5.6. Gegeben ein endlichdimensionaler reeller euklidischer affiner Raum E heißt eine affine Abbildung $\varphi : E \to E$ eine **Ähnlichkeitsabbildung** oder kurz **Ähnlichkeit** genau dann, wenn sie bijektiv ist und alle Winkel zwischen Halbgeraden im Sinne von 4.5.5 erhält. Man zeige: (1) Jede Ähnlichkeitsabbildung mit einem Fixpunkt $p \in E$ läßt sich eindeutig darstellen als die Verknüpfung einer Isometrie, die besagten Punkt p festhält, mit einer Streckung oder Stauchung der Gestalt $p + \vec{v} \mapsto p + \lambda\vec{v}$ für wohlbestimmtes $\lambda \in \mathbb{R}_{>0}$; (2) Jede Ähnlichkeitsabbildung, die keine Isometrie ist, besitzt genau einen Fixpunkt. Hinweis: Letztere Aussage kann man besonders elegant mit dem Banach'schen Fixpunktsatz **??** einsehen.

Definition 4.5.7. Gegeben ein orientierter zweidimensioaler reeller euklidischer Vektorraum V und ein Winkel ϑ sei die **orientierte Drehung um den Winkel** ϑ diejenige lineare Abbildung $R_\vartheta : V \to V$, die in einer und jeder orientierten

Orthonormalbasis von V dargestellt wird durch die Matrix

$$\begin{pmatrix} \cos\vartheta & -\sin\vartheta \\ \sin\vartheta & \cos\vartheta \end{pmatrix}$$

4.5.8. Wie bereits bei der Definition von Sinus und Cosinus in **??** erwähnt, ist $\vartheta \mapsto R_\vartheta$ ein stetig differenzierbarer Gruppenhomomorphismus $R : \mathbb{R} \to \mathrm{SO}(V)$. Sicher hat er auch die Eigenschaft, daß für jeden Vektor $\vec{v}$ der Länge Eins der Weg $\gamma_{\vec{v}} : t \mapsto R_t(\vec{v})$ mit absoluter Geschwindigkeit Eins durchlaufen wird und daß $(\vec{v}, \gamma'_{\vec{v}}(0))$ dann jeweils eine orientierte Basis von V ist. Er ist sogar der einzige stetig differenzierbare Gruppenhomomorphismus $R : \mathbb{R} \to \mathrm{SO}(V)$ mit diesen beiden Eigenschaften, nach **??** ist nämlich überhaupt jeder stetige Gruppenhomomorphismus $R : \mathbb{R} \to \mathrm{SO}(V)$ von der Form $\vartheta \mapsto R_{a\vartheta}$ für genau ein $a \in \mathbb{R}$. In diesem Sinne ist unsere Abbildung $\vartheta \mapsto R_\vartheta$ also keineswegs willkürlich gewählt, sondern durch natürliche Forderungen bereits eindeutig festgelegt. Ich habe nur deshalb nicht diese natürlichen Forderungen als Definition gewählt, um die Darstellung von der Analysis unabhängiger zu machen.

4.5.9. Denken wir uns V als eine unendliche Tafel mit einem ausgezeichneten Ursprung und der Orientierung, für die "erst ein Pfeil nach rechts, dann ein Pfeil nach oben" eine orientierte Basis ist, so müssen wir uns R_ϑ denken als die "Drehung mit Zentrum im Ursprung um den Winkel ϑ im Gegenuhrzeigersinn".

Definition 4.5.10. Gegeben ein orientierter zweidimensionaler reeller euklidischer Vektorraum und zwei von Null ausgehende Halbgeraden G, H definieren wir ihren **orientierten Winkel**

$$\vartheta = \measuredangle(G, H) \in (-\pi, \pi]$$

als das eindeutig bestimmte $\vartheta \in (-\pi, \pi]$ mit $R_\vartheta(G) = H$ für R_ϑ die orientierte Drehung um den Winkel ϑ aus 4.5.7. Gegeben zwei von Null verschiedene Vektoren v, w definieren wir ihren orientierten Winkel dann als $\measuredangle(v, w) = \measuredangle(\mathbb{R}_{\geq 0}v, \mathbb{R}_{\geq 0}w)$.

Beispiel 4.5.11. Gegeben ein von Null verschiedener Vektor $v \neq 0$ eines orientierten zweidimensionalen reellen euklidischen Vektorraums gilt für seinen orientierten Winkel mit seinem Negativen stets $\measuredangle(v, -v) = \pi$.

4.5.12. Gegeben von Null ausgehende Halbgeraden F, G, H in einem orientierten zweidimensionalen reellen euklidischen Vektorraum gilt stets die **Additivität der orientierten Winkel**

$$\measuredangle(F, H) \in \measuredangle(F, G) + \measuredangle(G, H) + 2\pi\mathbb{Z}$$

In der Tat gilt nach 4.3.11 ja $R_\vartheta R_\psi = R_{\vartheta+\psi}$, und $R_{2\pi} = \mathrm{id}$ ist eh klar.

Übung 4.5.13. Gegeben von Null verschiedene Vektoren v, w in einem orientierten zweidimensionalen reellen euklidischen Vektorraum haben wir stets $\measuredangle(v,w)+\measuredangle(w,-v) = \pm\pi$.

Übung 4.5.14. Der nichtorientierte Winkel ist in unseren Konventionen genau der Betrag des orientierten Winkels, in Formeln

$$\angle(G,H) = |\measuredangle(G,H)|$$

4.5.15. Der eigentliche Grund für unsere Winkeldefinition 4.5.1 liegt wie bereits erwähnt in seinem engen Zusammenhang 4.5.14 mit dem orientierten Winkel, dessen Definition hinwiederum durch die Additivität 4.5.12 motiviert ist. Natürlich könnten wir diese Additivität auch durch die Verwendung eines anderen Gruppenhomomorphismus $\mathbb{R} \to \mathrm{SO}(2)$ erreichen, und in der Tat sind hier in anderen Kontexten auch andere Wahlen üblich. Die meisten sind von der Gestalt $\vartheta \mapsto R_{a\vartheta}$ für $a > 0$.

1. Auf der Schule wird der Gruppenhomomorphismus meist so gewählt, daß 360 die kleinste positive Zahl ist, die auf die Identität abgebildet wird: Das hat den Vorteil, daß die Winkel vieler einfacher geometrischer Figuren ganzen Zahlen entsprechen. Man deutet es bei der Winkeldarstellung durch ein hochgestelltes $^\circ$ an, wenn man mit dieser Wahl arbeitet, und spricht von "Grad".

2. Bei Vermessungsarbeiten wird der Gruppenhomomorphismus meist so gewählt, daß 400 die kleinste positive Zahl ist, die auf die Identität abgebildet wird: Das hat den Vorteil, daß rechte Winkel der Zahl 100 entsprechen, und ist dem Arbeiten mit computergesteuerten Geräten, die ja mit ihrem Bedienungspersonal üblicherweise im Zehnersystem kommunizieren, besonders gut angepaßt. Man deutet es bei der Winkeldarstellung durch ein nachgestelltes gon an, wenn man mit dieser Wahl arbeitet, und spricht von "Neugrad" oder "Gon".

3. Mathematisch-abstrakt schiene es mir am natürlichsten, unsere orientierten Winkel schlicht als Elemente der Gruppe $\mathrm{SO}(2)$ aufzufassen, aber das wäre für die Anwender unpraktisch, die ja eben gerade eine explizite Notation für solche Elemente brauchen.

4. Die in diesem Text getroffene Wahl ist bei rechtem Licht betrachtet eigentlich die Wahl $a = \pi$: Wir drücken ja unsere Winkel in Wirklichkeit als Vielfache von π aus und kommen nicht ernsthaft auf die Idee, hier wirklich $\pi = 3{,}1415\ldots$ einzusetzen, auszumultiplizieren und die entstehende reelle Zahl mit einigen Nachkommastellen hinzuschreiben! Schreibt man diese

reelle Zahl doch aus, so sollte man rad als Abkürzung für "Radian", zu deutsch "Bogenmaß", dahinterschreiben, um klarzumachen, welcher Winkel gemeint ist.

In gewisser Weise spielt das Symbol π bei unserer Winkelbezeichnung also eine ähnliche Rolle wie das hochgestellte $^\circ$ bei der auf der Schule üblichen Bezeichnungsweise. Ich halte es nicht für besonders glücklich, daß hier π nur für den halben und nicht für den ganzen Vollkreis steht, aber so ist die Notation nun einmal geschichtlich gewachsen, und die nachträgliche Einführung eines zusätzlichen eigenen Symbols für den Umfang eines Kreises mit Radius Eins will ich nun auch wieder nicht propagieren. Es gibt jedoch Bestrebungen, das Symbol τ mit dieser Bedeutung aufzuladen.

4.5.16. Wir zeigen nun auch in diesem Rahmen, daß die Winkelsumme im Dreieck 180° alias π ist. Ich will nicht behaupten, daß der anschließende Beweis klarer sei als der anschauliche Beweis, wie Sie Ihn vermutlich in der Schule kennengelernt haben. Ich will jedoch zeigen, wie dieser anschauliche Beweis in das "Paradies der Mengenlehre" hinübergerettet werden kann, in dem wir uns ja mittlerweile die meiste Zeit bewegen. Die ungeheure Eleganz und Effizienz der Sprache der Mengenlehre kommt in diesem Beispiel schlecht zur Geltung, in dem man eher den Eindruck gewinnen mag, mit Kanonen auf Spatzen zu schießen. Es handelt sich eben auch nicht um einen Ernstfall, sondern vielmehr um eine Kanonenprobe.

Proposition 4.5.17 (Winkelsumme im Dreieck). *Für drei Punkte p, q, r einer affinen euklidischen Ebene E, die nicht auf einer Geraden liegen, gilt stets*

$$\angle(q-p, r-p) + \angle(p-r, q-r) + \angle(r-q, p-q) = \pi$$

Beweis. Zunächst wählen wir eine Orientierung auf $\vec{E}$ und beachten, daß aufgrund unserer Definitionen für $\vec{v}, \vec{w} \in \vec{E}$ linear unabhängig gilt

$$\measuredangle(\vec{v}, \vec{w}) \quad = \quad \begin{cases} \angle(\vec{v}, \vec{w}) & \text{falls } (\vec{v}, \vec{w}) \text{ eine orientierte Basis von } \vec{E} \text{ ist;} \\ -\angle(\vec{v}, \vec{w}) & \text{sonst.} \end{cases}$$

Jetzt kürzen wir die "Kantenvektoren" ab zu $\vec{v}_1 = q - p, \vec{v}_2 = p - r, \vec{v}_3 = r - q$, so daß gilt $\vec{v}_1 + \vec{v}_2 + \vec{v}_3 = \vec{0}$. Daraus folgt, daß $(\vec{v}_1, \vec{v}_2), (\vec{v}_2, \vec{v}_3)$ und $(\vec{v}_3, \vec{v}_1)$ alle drei gleich orientierte Basen sind, da nämlich die entsprechenden Basiswechselmatrizen alle positive Determinante haben. Für die orientierten Winkel wissen wir wegen der Additivität 4.5.12 bereits

$$\measuredangle(\vec{v}_1, \vec{v}_2) + \measuredangle(\vec{v}_2, \vec{v}_3) + \measuredangle(\vec{v}_3, \vec{v}_1) \in 2\pi\mathbb{Z}$$

Weiter gilt für $\vec{v} \neq \vec{0}$, $\vec{w} \neq \vec{0}$ nach 4.5.13 stets $\measuredangle(\vec{v}, \vec{w}) + \measuredangle(\vec{w}, -\vec{v}) = \pm\pi$ und damit folgt

$$\measuredangle(\vec{v}_1, -\vec{v}_2) + \measuredangle(\vec{v}_2, -\vec{v}_3) + \measuredangle(\vec{v}_3, -\vec{v}_1) \in \pi + 2\pi\mathbb{Z}$$

Der auf der Schule übliche Beweis dafür, daß die Winkelsumme im Dreieck $180°$ beträgt.

Wir wissen aber bereits, daß diese drei orientierten Winkel alle positiv oder alle negativ sind und genauer, daß sie alle in $(0, \pi)$ oder $(-\pi, 0)$ liegen. In beiden Fällen folgt unmittelbar

$$\angle(\vec{v}_1, -\vec{v}_2) + \angle(\vec{v}_2, -\vec{v}_3) + \angle(\vec{v}_2, -\vec{v}_1) = \pi \qquad \square$$

Satz 4.5.18. *Gegeben ein dreidimensionaler orientierter reeller euklidischer Vektorraum V gibt es genau eine bilineare Abbildung $V \times V \to V$ mit der Eigenschaft $(\vec{v}_1, \vec{v}_2) \mapsto \vec{v}_3$ für jede orientierte Orthonormalbasis $\vec{v}_1, \vec{v}_2, \vec{v}_3$. Sie heißt das* **Kreuzprodukt** *wegen der für unsere Abbildung allgemein gebräuchlichen Notation*

$$(\vec{v}, \vec{w}) \mapsto \vec{v} \times \vec{w}$$

4.5.19. Eine mit den benötigten Einheiten versehene Variante des Kreuzprodukts für den Richtungsraum unseres Anschauungsraums diskutieren wir in 8.6.11. Andere Autoren bezeichnen unser Kreuzprodukt als **Vektorprodukt**, da es als Resultat eben Vektoren liefert im Gegensatz zum Skalarprodukt, das Skalare liefert. Ich habe für das Kreuzprodukt alias Vektorprodukt auch schon die alternative Notation $[\vec{v}, \vec{w}]$ gesehen, die aber erst im Kontext von **??** ihre Verträglichkeit mit an wieder anderer Stelle üblichen Notationen zeigt. Noch seltener sieht man die Notation $\vec{v} \wedge \vec{w}$, die hinwiederum in 9.5.27 ihre Verträglichkeit mit dem dort eingeführten "Dachprodukt" $\wedge$ zeigt.

Beweis. Ohne Beschränkung der Allgemeinheit dürfen wir anehmen, V sei der $\mathbb{R}^3$ mit seinem Standard-Skalarprodukt und seiner Standard-Orientierung. Wenn es in diesem Fall überhaupt eine bilineare Abbildung $\mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$ mit den im Satz geforderten Eigenschaften gibt, dann muß diese offenichtlich durch die Vorschrift

$$\left(\begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix}, \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} \right) \mapsto \begin{pmatrix} v_2 w_3 - v_3 w_2 \\ v_2 w_1 - v_1 w_3 \\ v_1 w_2 - v_2 w_1 \end{pmatrix}$$

gegeben werden. Es bleibt damit nur noch zu zeigen, daß die durch diese Formel definierte bilineare Abbildung, die wir schon mal $(\vec{v}, \vec{w}) \mapsto \vec{v} \times \vec{w}$ notieren und für den Rest dieses Beweises das **konkrete Kreuzprodukt** nennen, auch wirklich die im Satz geforderte Eigenschaft hat. In Anbetracht der Jägerzaunformel 3.1.3 gilt für unser konkretes Kreuzprodukt offensichtlich schon mal die Identität

$$\langle \vec{u}, \vec{v} \times \vec{w} \rangle = \det(\vec{u}|\vec{v}|\vec{w})$$

und umgekehrt legt diese Eigenschaft für alle $\vec{u} \in \mathbb{R}^3$, ja sogar schon für $\vec{u} = \vec{e}_1, \vec{e}_2, \vec{e}_3$ auch bereits den Vektor $\vec{v} \times \vec{w}$ fest. Daraus folgt hinwiederum für alle

Drehungen $A \in \mathrm{SO}(3)$ die Identität

$$(A\vec{v}) \times (A\vec{w}) = A(\vec{v} \times \vec{w})$$

In der Tat, da für alle $A \in \mathrm{SO}(3)$ gilt $\langle A\vec{u}, A(\vec{v}\times\vec{w})\rangle = \langle \vec{u}, \vec{v}\times\vec{w}\rangle = \det(\vec{u}|\vec{v}|\vec{w}) = \det A(\vec{u}|\vec{v}|\vec{w}) = \det(A\vec{u}|A\vec{v}|A\vec{w}) = \langle A\vec{u}, (A\vec{v})\times(A\vec{w})\rangle$, ergibt sich ohne Schwierigkeiten $A(\vec{v} \times \vec{w}) = (A\vec{v}) \times (A\vec{w})$ für alle $A \in \mathrm{SO}(3)$. Da sich aber je zwei orientierte Orthonormalbasen des $\mathbb{R}^3$ durch eine Drehung $A \in \mathrm{SO}(3)$ ineinander überführen lassen, folgt unmittelbar, daß unser konkretes Kreuzprodukt die im Satz geforderte Eigenschaft hat. □

Ergänzung 4.5.20. Für den Ausdruck $\langle \vec{u}, \vec{v} \times \vec{w}\rangle = \det(\vec{u}|\vec{v}|\vec{w})$ aus dem vorhergehenden Beweis mit $\vec{u}, \vec{v}, \vec{w} \in \mathbb{R}^3$ findet man manchmal auch die Notation $\langle \vec{u}, \vec{v}, \vec{w}\rangle$ und die Bezeichnung als **Spatprodukt**, die darauf anspielt, daß diese Determinante ja nach 3.1.6 bis auf ein Vorzeichen gerade das Volumen des durch die fraglichen drei Vektoren gegebenen Parallelpipeds angibt. Die Kristalle des Feldspats haben aber nun oft die Gestalt eines Parallelpipeds, weswegen derartige Körper auch als **Spate** bezeichnet werden. In 8.6.10 diskutieren wir eine Variante des Spatprodukts für den Richtungsraum des Anschauungsraums.

Übung 4.5.21. Man zeige, am besten direkt von der Definition in Satz 4.5.18 ausgehend, die folgenden Eigenschaften des Kreuzprodukts:

1. Es gilt $\vec{v} \times \vec{w} = -\vec{w} \times \vec{v}$, als da heißt, das Kreuzprodukt ist alternierend.
2. $\vec{v} \times \vec{w}$ steht senkrecht auf $\vec{v}$ und $\vec{w}$;
3. Genau dann gilt $\vec{v} \times \vec{w} = \vec{0}$, wenn $(\vec{v}, \vec{w})$ ein linear abhängiges Paar von Vektoren ist.
4. Ist $(\vec{v}, \vec{w})$ ein linear unabhängiges Paar von Vektoren, so ist das Tripel $(\vec{v} \times \vec{w}, \vec{v}, \vec{w})$ in dieser Anordnung eine orientierte Basis.

4.5.22. Nehmen wir im Fall eines linear unabhängigen Paares $(\vec{v}, \vec{w})$ in obiger Formel $\vec{u} = (\vec{v} \times \vec{w})/\|\vec{v} \times \vec{w}\|$, so erkennen wir aus der anschaulichen Bedeutung 3.1.6 der Determinante als Volumen, daß wir uns die Länge von $\vec{v} \times \vec{w}$ gerade als das Volumen des von $\vec{u}, \vec{v}, \vec{w}$ aufgespannten Spats alias die Fläche des von $\vec{v}, \vec{w}$ aufgespannten Parallelograms denken dürfen. Damit erkennen wir, daß das Kreuzprodukt anschaulich wie folgt interpretiert werden kann: Für $\vec{v}, \vec{w}$ linear abhängig gilt $\vec{v} \times \vec{w} = \vec{0}$; Sonst ist $\vec{v} \times \vec{w}$ der Vektor, der senkrecht steht auf $\vec{v}$ und $\vec{w}$, dessen Länge der anschaulichen Fläche des von $\vec{v}$ und $\vec{w}$ aufgespannten Parallelogramms entspricht, und dessen Richtung dadurch festgelegt wird, daß $(\vec{v} \times \vec{w}, \vec{v}, \vec{w})$ eine orientierte Basis ist.

Übung 4.5.23. Man zeige: Gegeben ein dreidimensionaler reeller euklidischer Vektorraum V bilden die bilinearen Abbildungen $\varphi : V \times V \to V$ mit der Eigenschaft $\varphi(Av, Aw) = A\varphi(v, w)$ für alle $v, w \in V$ und $A \in \mathrm{SO}(V)$ einen eindimensionalen Untervektorraum des Vektorraums aller Abbildungen $V \times V \to V$. Es besteht insbesondere keine Hoffnung, neben dem Kreuzprodukt noch weitere "geometrisch bedeutsame" Verknüpfungen auf V zu finden! Hinweis: Ohne Beschränkung der Allgemeinheit sei V der $\mathbb{R}^3$ mit dem Standardskalarprodukt. Es gibt eine Drehung mit $\mathrm{e}_1 \mapsto \mathrm{e}_2$ und $\mathrm{e}_2 \mapsto -\mathrm{e}_1$. Man folgere, daß φ alternierend sein muß. Es gibt eine Drehung mit $\mathrm{e}_1 \mapsto \mathrm{e}_2$ und $\mathrm{e}_2 \mapsto \mathrm{e}_1$ und Drehachse $\mathrm{e}_2 + \mathrm{e}_1$. Man folgere, daß $\varphi(\mathrm{e}_1, \mathrm{e}_2)$ auf $\mathrm{e}_2 + \mathrm{e}_1$ senkrecht stehen muß.

Übung 4.5.24. Man zeige $\vec{u} \times (\vec{v} \times \vec{w}) = \langle \vec{u}, \vec{w} \rangle \vec{v} - \langle \vec{u}, \vec{v} \rangle \vec{w}$.

Ergänzende Übung 4.5.25. Gegeben ein endlichdimensionaler Vektorraum V über einem angeordneten Körper erinnern wir seine Orientierungsmenge $\mathrm{or}(V)$ aus 3.2.13 und erklären seine **Orientierungsgerade** als den eindimensionalen Vektorraum

$$\mathrm{or}_k(V) := \{f : \mathrm{or}(V) \to k \mid \text{Die Summe der beiden Werte von } f \text{ ist Null}\}$$

Wir erhalten eine Einbettung $\mathrm{or}(V) \hookrightarrow \mathrm{or}_k(V)$, indem wir jeder Orientierung $\varepsilon \in \mathrm{or}(V)$ die Funktion $f \in \mathrm{or}_k(V)$ mit $f(\varepsilon) = 1$ zuordnen. Besagte Einbettung behandeln wir von nun an in der Notation wie die Einbettung einer Teilmenge. Für jeden Vektorraumisomorphismus $A : V \xrightarrow{\sim} W$ läßt sich unsere Bijektion $\mathrm{or}(A)$ zwischen den Orientierungsmengen auf genau eine Weise zu einem Isomorphismus $\mathrm{or}_k(A) : \mathrm{or}_k(V) \xrightarrow{\sim} \mathrm{or}_k(W)$ der Orientierungsgeraden ausdehnen. Man zeige nun: Gegeben ein dreidimensionaler reeller euklidischer Vektorraum V gibt es genau eine bilineare Abbildung $V \times V \to V \otimes \mathrm{or}_k(V)$ mit der Eigenschaft $(\vec{v}_1, \vec{v}_2) \mapsto \vec{v}_3 \otimes \varepsilon$ für jede Orthonormalbasis $\vec{v}_1, \vec{v}_2, \vec{v}_3$ der Orientierung ε. Wir nennen sie auch ein **Kreuzprodukt** und notieren sie wieder

$$(\vec{v}, \vec{w}) \mapsto \vec{v} \times \vec{w}$$

Für jeden Isomorphismus $A : V \xrightarrow{\sim} W$ in einen weiteren dreidimensionalen reellen euklidischen Vektorraum gilt dann $A(\vec{v}) \times A(\vec{w}) = (A \otimes \mathrm{or}_k(A))(\vec{v} \times \vec{w})$ mit der Notation aus 2.7.8.

4.6 Spektralsatz und Hauptachsentransformationen

Satz 4.6.1 (Hauptachsentransformation). *Gegeben eine* **quadratische Form** *auf dem $\mathbb{R}^n$ alias eine Funktion $q : \mathbb{R}^n \to \mathbb{R}$ der Gestalt $q(x_1, \ldots, x_n) = \sum_{i \le j} c_{ij} x_i x_j$ gibt es stets eine Drehung $D \in \mathrm{SO}(n)$ und Skalare $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$ mit*

$$(q \circ D)(x_1, \ldots, x_n) = \lambda_1 x_1^2 + \ldots + \lambda_n x_n^2$$

Dieses Bild zeigt die Ellipse, auf der die positiv definite quadratische Form $17x^2 - 12xy + 8y^2$ bei einer geeigneten Wahl des Maßstabs den Wert Eins annimmt. Gestrichelt sind die Hauptachsen eingetragen, die in diesem Fall die Richtungsvektoren $(2, 1)$ und $(-1, 2)$ haben.

4.6.2. Man kann sich die Bedeutung dieses Satzes auf zwei Weisen veranschaulichen: Entweder "aktiv" in dem Sinne, daß der Graph unserer Funktion q unter der Drehung D^{-1} oder präziser der Abbildung $D^{-1} \times \mathrm{id}$ in den Graphen unserer Linearkombination von Quadraten übergeht; Oder "passiv" in dem Sinne, daß unsere Funktion beim Einführen neuer Koordinaten mit Koordinatenachsen in Richtung der Spaltenvektoren von D in den neuen Koordinaten ausgedrückt die fragliche Form annimmt, in Formeln $q(y_1\vec{v}_1 + \ldots + y_n\vec{v}_n) = \lambda_1 y_1^2 + \ldots + \lambda_n y_n^2$ für $\vec{v}_i$ die Spalten von D, also für $D = (\vec{v}_1|\ldots|\vec{v}_n)$. Die von den Spalten der Matrix D erzeugten Geraden bilden dann ein System von **Hauptachsen** für unsere quadratische Form q. Beim Beweis wird sich herausstellen, daß die Multimenge der λ_i durch unsere quadratische Form bereits eindeutig bestimmt ist. Wir nennen sie die Multimenge der **Eigenwerte** unserer quadratischen Form.

Definition 4.6.3. Gegeben ein Körper k und ein k-Vektorraum V versteht man unter einer **quadratischen Form** auf V ganz allgemein eine Abbildung

$$q : V \to k$$

die sich darstellen läßt in der Gestalt $q(v) = f_1(v)g_1(v) + \ldots + f_r(v)g_r(v)$ mit $f_i, g_i \in V^\top$ Linearformen auf V.

Übung 4.6.4. Sei k ein Körper und V ein endlichdimensionaler k-Vektorraum. Eine Abbildung $q : V \to k$ ist eine quadratische Form auf V genau dann, wenn gilt $q(\alpha v) = \alpha^2 q(v) \quad \forall \alpha \in k,\, v \in V$ und wenn außerdem die Abbildung $V \times V \to k$, $(v, w) \mapsto q(v + w) - q(v) - q(w)$ bilinear ist.

Übung 4.6.5. Man zeige: Gegeben ein endlichdimensionaler reeller euklidischer Vektorraum V und eine quadratische Form $q : V \to \mathbb{R}$ existieren stets eine Orthonormalbasis $\vec{v}_1, \ldots, \vec{v}_n$ von V und Skalare $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$ mit

$$q(x_1\vec{v}_1 + \ldots + x_n\vec{v}_n) = \lambda_1 x_1^2 + \ldots + \lambda_n x_n^2$$

Die von den $\vec{v}_i$ erzeugten Geraden nennen wir dann wieder ein System von **Hauptachsen** für unsere quadratische Form q. Beim Beweis wird sich wieder herausstellen, daß die Multimenge der λ_i durch unsere quadratische Form bereits eindeutig bestimmt ist, und wir nennen sie wieder die Multimenge der **Eigenwerte** unserer quadratischen Form. Natürlich hängen in diesem Fall sowohl die Hauptachsen als auch die Eigenwerte von der auf dem zugrundeliegenden Vektorraum gewählten euklidischen Struktur ab.

Ergänzung 4.6.6. In der Analysis, etwa in **??**, können Sie lernen, wie man eine hinreichend differenzierbare Funktion $\mathbb{R}^n \to \mathbb{R}$ etwa um den Ursprung bis zu zweiter Ordnung approximieren kann durch eine polynomiale Funktion vom

Totalgrad höchstens Zwei alias eine Summe von einer Konstanten, einer Linearform und einer quadratischen Form. Ist die fragliche Linearform Null alias hat der Graph unserer Funktion am Ursprung eine horizontale Tangentialebene alias hat unsere Funktion am Ursprung eine "kritische Stelle", so wird sie dort bis zur Ordnung Zwei approximiert durch die fragliche quadratische Form plus die Konstante. So führt dann das Studium der Minima und Maxima von Funktionen mehrerer Veränderlichen auf das Studium quadratischer Formen.

Beweis. Wir finden eine symmetrische Matrix $A \in \mathrm{M}(n \times n; \mathbb{R})$ mit

$$q(x) = x^\top A x$$

für den Spaltenvektor $x = (x_1, \ldots, x_n)^\top$, indem wir als diagonale Matrixeinträge $a_{ii} = c_{ii}$ nehmen und außerhalb der Diagonalen $a_{ij} = a_{ji} = c_{ij}/2$ setzen. Nach 4.6.8 gibt es dann eine Drehung $D \in \mathrm{SO}(n)$ mit $D^{-1}AD = D^\top AD = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ für geeignete $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$, nämlich die Eigenwerte von A mit ihren Vielfachheiten. Es folgt

$$q(Dx) = x^\top D^\top ADx = \lambda_1 x_1^2 + \ldots + \lambda_n x_n^2 \qquad \square$$

Übung 4.6.7. Man zeige: Gegeben eine Polynomfunktion vom Grad höchstens zwei mit reellen Koeffizienten, also eine Abbildung $q : \mathbb{R}^n \to \mathbb{R}$ der Gestalt

$$q(x_1, \ldots, x_n) = \sum_{i \le j} a_{ij} x_i x_j + \sum_i b_i x_i + c$$

gibt es eine abstandserhaltende Selbstabbildung $D : \mathbb{R}^n \to \mathbb{R}^n$ mit

$$(q \circ D)(x_1, \ldots, x_n) = \lambda_1 x_1^2 + \ldots + \lambda_k x_k^2 + \lambda_{k+1} x_{k+1} + \ldots + \lambda_n x_n + \lambda_0$$

für geeignetes k und geeignete reelle λ_i. Man sagt dann, die Quadrik gehe "unter unserer Bewegung D in ihre Standardform über".

Proposition 4.6.8. *Gegeben eine symmetrische Matrix $A \in \mathrm{M}(n \times n; \mathbb{R})$ gibt es eine orthogonale Matrix mit Determinante Eins $D \in \mathrm{SO}(n)$ derart, daß $D^\top AD = D^{-1}AD$ diagonal ist.*

Beweis. Das folgt sofort aus dem Spektralsatz für "selbstadjungierte" Abbildungen 4.6.18, indem wir als Spalten von D die Vektoren einer Orthonormalbasis von $\mathbb{R}^n$ aus Eigenvektoren von $A : \mathbb{R}^n \to \mathbb{R}^n$ nehmen, und notfalls noch eine Spalte mit (-1) multiplizieren, um $\det D = 1$ zu erreichen. $\square$

Gärtner erstellen elliptische Beete wie folgt: Sie schlagen zwei Pfosten ein, legen eine Seilschlinge darum, und fahren mit einem dritten Pfosten soweit außen, wie die Seilschlinge es erlaubt, um die beiden fest eingeschlagenen Pfosten herum. Eine einfache Rechnung zeigt, daß man so die Lösungsmenge einer quadratischen Gleichung und, da unsere Lösungsmenge beschränkt ist und nicht nur aus einem Punkt besteht, notwendig eine Ellipse erhält: Wenn man definieren müßte, welche Teilmengen einer affinen reellen Ebene denn nun Ellipsen heißen sollen, würde man nämlich genau diese Eingenschaft zur Definition erheben, und 4.6.7 zeigt, daß das auch unserer Anschauung entspricht, nach der eine Ellipse eine "zusammengedrückte Kreislinie" sein sollte. Die beiden Pfosten heißen die **Brennpunkte** unserer Ellipse. Das hat hinwiederum mit dem Grenzfall der Parabel zu tun, zu dem wir gelangen, indem wir einen Pfosten vom anderen Pfosten weg auf geradem Wege ins Unendliche schieben und gleichzeitig das Seil so verlängern, daß immer gleich viel Spiel bleibt. Wäre die Ellipse ein Spiegel, so sollte anschaulich klar sein, daß sich das von einer Laterne auf einem der Pfosten ausgesandte Licht beim anderen Pfosten wieder sammeln muß. Im Grenzfall der Parabel wird sich folglich parallel aus der Richtung des unendlich fernen Pfostens einfallendes Licht beim anderen Pfosten sammeln und ihn, wenn auf dem unendlich fernen Pfosten statt einer Laterne die Sonne steht, möglicherweise sogar entzünden: Deshalb heißt er der Brennpunkt der Parabel, und von diesem Beispiel überträgt man das Wort auf Ellipsen und Hyperbeln, bei denen statt der Summe die Differenz der Abstände zu den beiden "Brennpunkten" konstant ist.

Definition 4.6.9. Seien V, W euklidische Vektorräume und $A : V \to W$ und $B : W \to V$ lineare Abbildungen. Unsere Abbildungen heißen zueinander **adjungiert** genau dann, wenn gilt

$$\langle Av, w\rangle = \langle v, Bw\rangle \quad \forall v \in V, w \in W$$

Ich kann leider für das Konzept adjungierter Abbildungen keinerlei Anschauung anbieten.

4.6.10. Diese adjungierte Abbildung ist nicht zu verwechseln mit der adjungierten Matrix aus 3.4.10, mit der sie außer der Bezeichnung rein gar nichts zu tun hat.

4.6.11. Jede lineare Abbildung A wie oben hat höchstens eine Adjungierte, denn sind B, C beide adjungiert zu A, so folgt $\langle v, Bw - Cw\rangle = 0 \quad \forall v, w$ und damit $Bw = Cw \quad \forall w$. Versehen wir $\mathbb{R}^n, \mathbb{R}^m$ jeweils mit dem Standardskalarprodukt, so wird für $A \in \mathrm{M}(m \times n; \mathbb{R})$ die adjungierte Abbildung zu $A : \mathbb{R}^n \to \mathbb{R}^m$ gegeben durch die transponierte Matrix als $A^\top : \mathbb{R}^m \to \mathbb{R}^n$. Ebenso ist im Komplexen $\bar{A}^\top : \mathbb{C}^m \to \mathbb{C}^n$ adjungiert zu $A : \mathbb{C}^n \to \mathbb{C}^m$. In der Tat finden wir mühelos

$$\langle Ax, y\rangle = (\overline{Ax})^\top y = \bar{x}^\top \bar{A}^\top y = \langle x, \bar{A}^\top y\rangle$$

für alle $x \in \mathbb{C}^m$, $y \in \mathbb{C}^n$. Wir folgern mit 4.3.5, daß jede lineare Abbildung von endlichdimensionalen reellen oder komplexen euklidischen Vektorräumen genau eine Adjungierte hat. Für die Adjungierte einer Abbildung A verwendet man in der Mathematik meist die Notation A^* und in der Physik meist die Notation $A^\dagger$.

Übung 4.6.12. Bei einem unitären Isomorphismus zwischen euklidischen Vektorräumen ist die adjungierte Abbildung die inverse Abbildung.

Ergänzung 4.6.13. Lineare Abbildungen f, g zwischen komplexen euklidischen Vektorräumen sind in anderen Formeln ausgedrückt adjungiert genau dann, wenn das Diagramm

$$\begin{array}{ccc} V & \xrightarrow{\mathrm{can}} & V^\top \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g^\top} \\ W & \xrightarrow{\mathrm{can}} & W^\top \end{array}$$

kommutiert, mit $g^\top : V^\top \to W^\top$ der "transponierten" alias "dualen" Abbildung zu $g : W \to V$ und $\mathrm{can} : V \to V^\top$ der Abbildung $v \mapsto \langle v, \ \rangle$ und $\mathrm{can} : W \to W^\top$ der analog definierten Abbildung. Diese "kanonischen" Abbildungen can landen zwar wie behauptet im Dualraum, da unsere Skalarprodukte linear sind im zweiten Eintrag, sie sind jedoch selbst nur im reellen Fall linear und im komplexen Fall vielmehr schieflinear im Sinne von 4.2.6. Man überzeugt sich dennoch leicht, daß diese kanonischen Abbildungen im endlichdimensionalen Fall Isomorphismen sein müssen, und das liefert dann einen alternativen Beweis für die Existenz und Eindeutigkeit der adjungierten Abbildung im endlichdimensionalen Fall.

Noch bequemer wird die Argumentation, wenn man wie im nächsten Abschnitt den komplex konjugierten Vektorraum einführt.

Ergänzung 4.6.14. Zu jedem komplexen Vektorraum V bilden wir zunächst den **komplex konjugierten Vektorraum** $\overline{V}$, indem wir dieselbe unterliegende additive Gruppe nehmen, die Operation von $a \in \mathbb{C}$ auf $v \in V$ jedoch abändern zu einer Operation $a \cdot v$, die mit der ursprünglichen Operation av verknüpft ist durch die Formel $a \cdot v = \bar{a}v$ alias $\bar{a} \cdot v = av$. Es ist in diesem Zusammenhang praktisch, für jedes Element $v \in V$ dasselbe Element in seiner Eigenschaft als Element des komplex konjugierten Vektorraums $\bar{v} \in \overline{V}$ zu notieren, so daß wir unseren Punkt für die neue Operation der Skalare gleich wieder weglassen können und unsere zweite Formel besonders suggestiv in der Form

$$\bar{a}\bar{v} = \overline{av}$$

geschrieben werden kann. Für jede $\mathbb{C}$-lineare Abbildung $f : V \to W$ von komplexen Vektorräumen ist dieselbe Abbildung auch eine $\mathbb{C}$-lineare Abbildung $\overline{V} \to \overline{W}$. Wir bezeichnen diese Abbildung dennoch mit dem neuen Symbol $\bar{f} : \overline{V} \to \overline{W}$ und nennen sie die **konjugierte Abbildung**, weil ihre Matrix anders aussieht: Sind genauer $\mathcal{A}$ und $\mathcal{B}$ angeordnete Basen von V und W, so hat die konjugierte Abbildung nämlich die konjugierte Matrix, in Formeln

$$_{\bar{\mathcal{B}}}[\bar{f}]_{\bar{\mathcal{A}}} = \overline{{}_{\mathcal{B}}[f]_{\mathcal{A}}}$$

wo die Basen wie die einzelnen Vektoren nur einen Querstrich kriegen, um daran zu erinnern, daß sie im konjuguierten Vektorraum zu denken sind. Eine koordinatenfreie Konstruktion der adjungierten Abbildung erhält man nun wie folgt: Jedes Skalarprodukt $\langle\ ,\ \rangle$ auf V liefert eine injektive lineare Abbildung

$$\begin{array}{rccc} \mathrm{can}: & \overline{V} & \hookrightarrow & V^\top \\ & \bar{v} & \mapsto & \langle v,\ \rangle \end{array}$$

des konjugierten Raums zu V in den Dualraum von V. Lineare Abbildungen f, g zwischen komplexen euklidischen Vektorräumen sind in diesem Formalismus adjungiert genau dann, wenn das Diagramm

$$\begin{array}{ccc} \overline{V} & \xrightarrow{\mathrm{can}} & V^\top \\ {\scriptstyle \bar{f}}\downarrow & & \downarrow{\scriptstyle g^\top} \\ \overline{W} & \xrightarrow{\mathrm{can}} & W^\top \end{array}$$

kommutiert, mit $g^\top : V^\top \to W^\top$ der "transponierten" alias "dualen" Abbildung zu $g : W \to V$. Im endlichdimensionalen Fall sind unsere kanonischen Abbildungen can in den Horizontalen jedoch nach Dimensionsvergleich Isomorphismen. In diesem Fall liefert also das obige kommutative Diagramm auch einen alternativen Beweis für die Existenz und Eindeutigkeit adjungierter Abbildungen.

Definition 4.6.15. Ein Endomorphismus eines reellen oder komplexen euklidischen Vektorraums heißt **selbstadjungiert** genau dann, wenn er zu sich selbst adjungiert ist.

Ergänzung 4.6.16. Die tiefere Bedeutung dieser Bedingung wird meines Erachtens erst in **??** sichtbar, wo Sie zeigen werden, daß die "schiefadjungierten" als da heißt zu ihrem Negativen adjungierten Endomorphismen im endlichdimensionalen Fall genau den "Tangentialraum" an die Gruppe der unitären Automorphismen bilden.

Beispiele 4.6.17. Eine reelle $(n \times n)$-Matrix X beschreibt eine selbstadjungierte Abbildung $X : \mathbb{R}^n \to \mathbb{R}^n$ genau dann, wenn sie symmetrisch ist, in Formeln $X = X^\top$. Eine komplexe $(n \times n)$-Matrix X beschreibt eine selbstadjungierte Abbildung $X : \mathbb{C}^n \to \mathbb{C}^n$ genau dann, wenn sie die Identität $X = \bar{X}^\top$ erfüllt. Solche Matrizen heißen auch **hermitesch**.

Satz 4.6.18 (Spektralsatz für selbstadjungierte Abbildungen). *Für jeden selbstadjungierten Endomorphismus eines endlichdimensionalen euklidischen Vektorraums besitzt unser Vektorraum eine Orthonormalbasis aus Eigenvektoren, und auch im komplexen Fall sind alle Eigenwerte unseres Endomorphismus reell.*

4.6.19. Einen noch allgemeineren Spektralsatz für "normale" Endomorphismen dürfen Sie später als Übung 6.3.11 selbst beweisen.

Erster Beweis. Sei V unser euklidischer Vektorraum und $A : V \to V$ selbstadjungiert. Gegeben $0 \neq v \in V$ und $\lambda \in \mathbb{C}$ mit $Av = \lambda v$ folgern wir von der Mitte ausgehend die Gleichungskette

$$\bar{\lambda}\langle v, v\rangle = \langle v, v\rangle = \langle Av, v\rangle = \langle v, Av\rangle = \langle v, \lambda v\rangle = \lambda\langle v, v\rangle$$

und daraus folgt bereits $\lambda \in \mathbb{R}$. Weiter ist das orthogonale Komplement $v^\perp$ eines Eigenvektors v stabil unter A, denn aus $\langle v, w\rangle = 0$ folgt $\langle v, Aw\rangle = \langle Av, w\rangle = \bar{\lambda}\langle v, w\rangle = 0$. Bis hierher brauchen wir nicht einmal V als endlichdimensional vorraussetzen. Nun können wir den Beweis im Komplexen mit Induktion beenden. Im Fall $V = 0$ ist der Satz klar. Sonst finden wir einen Eigenvektor v_1, den wir ohne Beschränkung der Allgemeinheit normiert annehmen dürfen. Dann wenden wir auf die auf seinem orthogonalen Komplement induzierte Abbildung $A : v_1^\perp \to v_1^\perp$ die Induktionsvoraussetzung an und finden darin eine Orthonormalbasis $v_2, \ldots, v_n$ aus Eigenvektoren von A. Damit ist $v_1, \ldots, v_n$ die gesuchte Orthonormalbasis von V aus Eigenvektoren von A. Das erledigt den komplexen Fall. Im reellen Fall überlegen wir uns zunächst, daß die darstellende Matrix von A in Bezug auf eine Orthonormalbasis von V symmetrisch sein muß. Diese Matrix hat im Fall $\dim_{\mathbb{R}} V > 0$ in $\mathbb{C}$ mindestens einen Eigenwert, der dann aber nach

unseren Überlegungen zu Beginn des Beweises sogar reell sein muß. Dazu finden wir dann wieder einen Eigenvektor aus V, und der Beweis läuft von hier an wie im komplexen Fall. □

Zweiter Beweis im Reellen. Man betrachte auf $V\backslash 0$ die Funktion

$$v \mapsto R(v) = \frac{\langle Av, v\rangle}{\langle v, v\rangle}$$

Sie heißt der **Raleigh-Quotient**, deshalb der Buchstabe R. Schränken wir diese Funktion ein auf die Einheitssphäre $\{v \mid \|v\| = 1\}$, so nimmt sie dort nach Heine-Borel **??** und **??** ihr Maximum an, etwa an einer Stelle v_+. Da unsere Funktion konstant ist auf jeder Geraden durch den Nullpunkt, muß sie an derselben Stelle auch als Funktion $V\backslash 0 \to \mathbb{R}$ ihr Maximum annehmen. Wir betrachten wir nun für $w \in V$ die für hinreichend kleines $t \in \mathbb{R}$ wohldefinierte Funktion $t \mapsto R_w(t) = R(v_+ + tw)$, ausgeschrieben

$$R_w(t) = \frac{\langle A(v_+ + tw), v_+ + tw\rangle}{\langle v_+ + tw, v_+ + tw\rangle}$$

Sie ist offensichtlich differenzierbar, folglich muß ihre Ableitung bei $t = 0$ verschwinden. Dann verschwindet also auch der Zähler, wenn wir diese Ableitung $R'_w(0)$ mithilfe der Quotientenregel berechnen, und wir folgern

$$(\langle Aw, v_+\rangle + \langle Av_+, w\rangle)\langle v_+, v_+\rangle - 2\langle Av_+, v_+\rangle\langle v_+, w\rangle = 0$$

für alle $w \in V$. Mithilfe der Selbstadjungiertheit von A folgern wir insbesondere

$$w \perp v_+ \quad \Rightarrow \quad w \perp Av_+$$

Das liefert offensichtlich $Av_+ \in \mathbb{R}v_+$ und wir haben einen Eigenvektor gefunden. Der Rest des Arguments läuft von da an wie beim ersten Beweis. □

4.6.20. Der zweite Beweis vermeidet zwar den Fundamentalsatz der Algebra, benutzt jedoch einen wesentlichen Teil der Resultate der reellen Analysis, aus denen wir in **??** auch den Fundamentalsatz der Algebra herleiten werden. Anschaulich scheint mir die im zweiten Beweis versteckte Erkenntnis recht klar: Durch den Punkt der Ellipse, der am nächsten am Ursprung liegt, geht in der Tat eine Hauptachse. Dasselbe gilt natürlich für den Punkt, der dem Ursprung am fernsten liegt, als da heißt, der kleinstmögliche Wert des Raleigh-Quotienten ist auch ein Eigenwert und jede Stelle, an der er angenommen wird, ist ein Eigenvektor unseres selbstadjungierten Operators zu diesem Eigenwert.

Ergänzende Übung 4.6.21. Man zeige: Ein Endomorphismus eines endlichdimensionalen euklidischen Vektorraums ist genau dann selbstadjungiert, wenn es dazu eine Orthonormalbasis aus Eigenvektoren gibt und alle Eigenwerte reell sind.

Satz 4.6.22 (Polar-Zerlegung in $\mathrm{GL}(n;\mathbb{R})$). *Jede Matrix $A \in \mathrm{GL}(n;\mathbb{R})$ besitzt eine eindeutige Darstellung als Produkt $A = DP$ mit $D \in \mathrm{O}(n)$ orthogonal und P symmetrisch positiv definit.*

Beispiel 4.6.23. Im Fall $\mathrm{GL}(1;\mathbb{R})$ ist das die vielleicht noch nicht sehr aufregende Zerlegung $a = (a/|a|) \cdot |a|$ einer von Null verschiedenen reellen Zahl als das Produkt von einem Vorzeichen mit einer positiven reellen Zahl.

4.6.24. Im Fall $n = 3$ beschreibt A eine Abbildung $A : \mathbb{R}^3 \to \mathbb{R}^3$, und nimmt man A orientierungserhaltend an, so mag man sich denken, daß sich unsere Abbildung in eindeutiger Weise darstellen läßt als Verknüpfung einer Abbildung, die entlang geeigneter paarweise orthogonaler Koordinatenachsen dehnt oder staucht, mit einer Abbildung, die dreht. Wenden wir etwa A auf den mit Schaumgummi oder was auch immer gefüllt gedachten Raum an, so ist allein der positiv definite Faktor P für die Materialspannungen verantwortlich: Eine Kugel unseres Materials wird bei Anwenden von A "erst mit P zu einem Ellipsoid verzerrt und dann noch mit D gedreht".

Beweis. Wir beginnen mit dem Nachweis der Eindeutigkeit. Gegeben eine Zerlegung $A = DP$ wie oben haben wir sicher $A^\top A = P^\top D^\top DP = P^\top P = P^2$ und folglich muß P die Matrix sein, die auf den Eigenräumen von $A^\top A$ zum Eigenwert λ jeweils operiert durch den Eigenwert $\sqrt{\lambda}$. Das zeigt die Eindeutigkeit unserer Zerlegung. Andererseits folgt aus $A^\top Av = \lambda v$ sofort $v^\top A^\top Av = \lambda\|v\|^2 = \|Av\|^2$ und somit $\lambda > 0$, so daß wir P symmetrisch und positiv definit finden können mit $P^2 = A^\top A$. Für $D = AP^{-1}$ folgt dann $D^\top D = P^{-1}A^\top AP^{-1} = I$ und folglich ist D orthogonal. □

Definition 4.6.25. Unter einer **partiellen Isometrie** eines Raums mit Skalarprodukt versteht man eine lineare Abbildung, deren Restriktion auf den Orthogonalraum ihres Kerns isometrisch ist.

Satz 4.6.26 (Polar-Zerlegung eines Endomorphismus). *Jeder Endomorphismus A eines endlichdimensionalen reellen euklidischen Vektorraums V besitzt eine eindeutige Darstellung als Produkt $A = DP$ mit P selbstadjungiert positiv semidefinit und D einer partiellen Isometrie derart, daß gilt $(\ker D)^\perp = \operatorname{im} P$.*

Übung 4.6.27. Sei V ein endlichdimensionaler reeller euklidischer Vektorraum. Man zeige, daß jeder Endomorphismus $A \in \operatorname{End} V$ auch eine eindeutige Darstellung als Produkt $A = PD$ besitzt mit P selbstadjungiert positiv semidefinit und D einer partiellen Isometrie derart, daß gilt $\operatorname{im} D = (\ker P)^\perp$.

Die Polarzerlegung der Scherung $(x, y) \mapsto (x, y - x)$ stellt diese Abbildung dar als Verknüpfung einer Streckung bzw. Stauchung längs orthogonaler Achsen mit einer Drehung. Im unteren Bild sieht man durchgezogen den Einheitskreis, und gestrichelt sein Bild unter dem selbstadjungiertem Faktor der Verscherung nebst den Hauptachsen, längs derer der Einheitskreis dabei gestreckt bzw. gestaucht wird. Im oberen Bild dann der verscherte Einheitskreis alias die mit dem orthogonalen Faktor der Verscherung verdrehte Ellipse aus dem unteren Bild. Auch noch gestrichelt eingezeichnet die Hauptachsen dieser Ellipse.

Beweis. Wir beginnen mit der Eindeutigkeit. Gegeben eine derartige Zerlegung $A = DP$ können wir sicher auch eine orthogonale Abbildung M finden mit $A = MP$. Es folgt $A^\top A = P^2$ und folglich ist P eindeutig bestimmt als die einzige positiv semidefinite selbstadjungierte Abbildung P mit $P^2 = A^\top A$. Dann ist auch D eindeutig festgelegt auf $\operatorname{im} P$, und unsere letzte Bedingung impliziert $D = 0$ auf $(\operatorname{im} P)^\perp$ und legt damit auch D eindeutig fest. Um die Existenz zu zeigen, gehen wir diese Argumentation rückwärts durch. Das Argument des vorhergehenden Beweises zeigt, daß es ein selbstadjungiertes positiv semidefinites P gibt mit $P^2 = A^\top A$. Wegen $\langle Av, Av\rangle = \langle v, A^\top Av\rangle = \langle v, P^2v\rangle = \langle Pv, Pv\rangle$ gilt $\ker A = \ker P$. Das ist aber auch das orthogonale Komplement des Bildes $U := \operatorname{im} P$, und bezeichnet $Q : V \twoheadrightarrow U$ die orthogonale Projektion auf U und $J : U \hookrightarrow V$ die Einbettung, so haben wir mithin $A = AJQ$. Nun induziert P einen Isomorphismus $P_U : U \xrightarrow{\sim} U$ und wir können die Komposition $C = AJP_U^{-1} : U \to V$ betrachten. Dann gilt einerseits $CQP = CP_UQ = AJQ = A$ und andererseits ist C isometrisch. Dann ist $D = CQ$ eine partielle Isometrie mit den gewünschten Eigenschaften. □

Definition 4.6.28. Eine hermitesche Matrix $A \in \mathrm{M}(n\times n;\mathbb{C})$ heißt **positiv definit** genau dann, wenn gilt $\bar x^\top Ax \le 0 \Rightarrow x = 0$. Sie heißt **positiv semidefinit** genau dann, wenn gilt $\bar x^\top Ax \ge 0\ \forall x \in \mathbb{C}^n$.

Übung 4.6.29. Man zeige, daß eine reelle symmetrische Matrix positiv definit bzw. positiv semidefinit ist im Sinne unserer ursprünglichen Definition 4.3.31 genau dann, wenn sie als hermitische Matrix aufgefaßt diese Eigenschaft im Sinne von 4.6.28 hat.

Korollar 4.6.30 (Polar-Zerlegung in $\mathrm{M}(n\times n;\mathbb{R})$). *Jede reelle quadratische Matrix A besitzt eine eindeutige Darstellung als Produkt $A = DP$ mit P symmetrisch positiv semidefinit und D einer partiellen Isometrie derart, daß gilt $(\ker D)^\perp = \operatorname{im} P$.*

Definition 4.6.31. Eine hermitesche Matrix $A \in \mathrm{M}(n\times n;\mathbb{C})$ heißt **positiv definit** genau dann, wenn gilt $\bar x^\top Ax \le 0 \Rightarrow x = 0$. Sie heißt **positiv semidefinit** genau dann, wenn gilt $\bar x^\top Ax \ge 0\ \forall x$.

Satz 4.6.32 (Polar-Zerlegung in $\mathrm{GL}(n;\mathbb{C})$). *Jede Matrix $A \in \mathrm{GL}(n;\mathbb{C})$ hat eine eindeutige Darstellung als Produkt $A = DP$ mit $D \in \mathrm{U}(n)$ unitär und P hermitesch positiv definit.*

Beweis. Analog wie im Reellen. □

Beispiel 4.6.33. Im Fall $\mathrm{GL}(1;\mathbb{R})$ ist das die Zerlegung $a = (a/|a|)\cdot|a|$ einer von Null verschiedenen komplexen Zahl in eine Zahl der Länge Eins und eine positive reelle Zahl.

Beispiel 4.6.34. Im Fall $\mathrm{GL}(1;\mathbb{C})$ ist das die Zerlegung $a = (a/|a|) \cdot |a|$.

Übung 4.6.35 (**Polar-Zerlegung in** $\mathrm{M}(n \times n;\mathbb{C})$). Man zeige analog zu 4.6.30, daß jede Matrix $A \in \mathrm{M}(n \times n;\mathbb{C})$ eine eindeutige Darstellung als Produkt $A = DP$ hat mit P hermitesch positiv semidefinit und D einer komplexlinearen partiellen Isometrie mit $(\ker D)^\perp = \operatorname{im} P$.

Übung 4.6.36. Man gebe eine von Null verschiedene komplexe symmetrische nilpotente (2×2)-Matrix an. Gibt es auch eine von Null verschiedene reelle symmetrische nilpotente (2×2)-Matrix?

Ergänzende Übung 4.6.37. Bezeichne $S \subset \mathrm{M}(n \times n;\mathbb{R})$ den Untervektorraum der symmetrischen Matrizen. Gegeben eine weitere symmetrische Matrix P betrachte man die lineare Abbildung $f_P : S \to S$ gegeben durch die Vorschrift $f_P : A \mapsto PAP$. Man zeige für die Determinante von f_P im Sinne von 3.4.4 die Formel $\det(f_P) = (\det P)^{n+1}$. Hinweis: Man ziehe sich auf den Fall zurück, daß P diagonal ist.

5 Bilinearformen

5.1 Fundamentalmatrix

Definition 5.1.1. Gegeben ein Körper k und ein k-Vektorraum V erinnern wir daran, daß wir in 4.2 bilineare Abbildungen $b : V \times V \to k$ auch Bilinearformen auf V genannt hatten. Die Menge aller Bilinearformen auf einem k-Vektorraum V notiere ich

$$\mathrm{Bil}_k(V) = \mathrm{Bil}(V)$$

Sie bilden einen Untervektorraum im Vektorraum $\mathrm{Ens}(V \times V, k)$ aller Abbildungen von $V \times V$ nach k. In der alternativen in 1.5.26 eingeführten Notation hätten wir $\mathrm{Bil}_k(V) = \mathrm{Hom}^{(2)}(V \times V, k)$.

Satz 5.1.2 (Fundamentalmatrix einer Bilinearform auf k^n). *Gegeben ein Körper k und eine natürliche Zahl $n \in \mathbb{N}$ erhalten wir eine Bijektion*

$$\begin{array}{ccc} \mathrm{Bil}(k^n) & \xrightarrow{\sim} & \mathrm{M}(n \times n; k) \\ b & \mapsto & F(b) \end{array}$$

indem wir die **Fundamentalmatrix** $F(b)$ *unserer Bilinearform erklären duch die Vorschrift $F(b)_{ij} = b(\mathrm{e}_i, \mathrm{e}_j)$. Die Umkehrabbildung kann beschrieben werden durch die Abbildungsvorschrift $F \mapsto b_F$ mit $b_F(x, y) = x^\top F y$.*

Beweis. Die erste Aussage folgt unmittelbar aus Übung 1.5.27, nach der eine bilineare Abbildung festgelegt und festlegbar ist durch ihre Werte auf Paaren von Basisvektoren. Um zu prüfen, daß unsere Beschreibung der Umkehrabbildung korrekt ist, reicht es aus, für jede Matrix F zu zeigen $F(b_F) = F$ alias $b_F(\mathrm{e}_i, \mathrm{e}_j) = F_{ij} \quad \forall i, j$. Das hinwiederum folgt jedoch unmittelbar aus $b_F(\mathrm{e}_i, \mathrm{e}_j) = \mathrm{e}_i^\top F \mathrm{e}_j$. □

Satz 5.1.3 (Fundamentalmatrix einer abstrakten Bilinearform). *Gegeben ein Körper k und ein k-Vektorraum V liefert jede angeordnete Basis $\mathcal{B} = (v_1, \ldots, v_n)$ von V eine Bijektion*

$$\begin{array}{ccc} \mathrm{Bil}(V) & \xrightarrow{\sim} & \mathrm{M}(n \times n; k) \\ b & \mapsto & F_{\mathcal{B}}(b) \end{array}$$

indem wir die **Fundamentalmatrix** $F = F_{\mathcal{B}}(b)$ *unserer Bilinearform b bezüglich unserer Basis $\mathcal{B}$ erklären durch die Vorschrift $F_{ij} = b(v_i, v_j)$. Die Umkehrabbildung kann in diesem Fall beschrieben werden durch die Abbildungsvorschrift $F \mapsto b_F$ mit*

$$b_F(v, w) = {}_{\mathcal{B}}[v]^\top \circ F \circ {}_{\mathcal{B}}[w]$$

Beweis. Die erste Aussage folgt wieder unmittelbar aus der Erkenntnis 1.5.27, daß eine bilineare Abbildung festgelegt und festlegbar ist durch ihre Werte auf Paaren von Basisvektoren. Für die zweite Aussage zeigen wir nun zur Abwechslung einmal $b_{F(b)} = b$ alias $b_{F(b)}(v, w) = b(v, w)$ für alle v, w. Dazu müssen wir ja nur zeigen $b_{F(b)}(v_i, v_j) = b(v_i, v_j)$ für alle i, j alias

$$ {}_{\mathcal{B}}[v_i]^\top \circ F_{\mathcal{B}}(b) \circ {}_{\mathcal{B}}[v_j] = (F_{\mathcal{B}}(b))_{ij} $$

Das ist jedoch klar wegen ${}_{\mathcal{B}}[v_i] = \mathrm{e}_i$. □

5.1.4. Eine Bilinearform ist symmetrisch genau dann, wenn ihre Fundamentalmatrix bezüglich einer gegebenen Basis symmetrisch ist. Ist also in Formeln V ein k-Vektorraum und $\mathcal{B}$ eine angeordnete Basis von V und $b : V \times V \to k$ eine Bilinearform, so gilt

$$ b \text{ symmetrisch} \quad \Leftrightarrow \quad F_{\mathcal{B}}(b) \text{ symmetrisch} $$

In der Tat, ist $(v_1, \ldots, v_n)$ unsere angeordnete Basis, so gilt für symmetrisches b ja $b(v_i, v_j) = b(v_j, v_i)$ und damit die Identität $F_{ij} = F_{ji}$ für die Einträge $F_{ij} = b(v_i, v_j)$ der Fundamentalmatrix $F = F_{\mathcal{B}}(b)$. Bezeichnet ganz allgemein $\tau : V \times V \xrightarrow{\sim} V \times V$ das Vertauschen $\tau : (v, w) \mapsto (w, v)$, so haben wir für jede Bilinearform b offensichtlich die Identität $F_{\mathcal{B}}(b \circ \tau) = F_{\mathcal{B}}(b)^\top$. Ist also die Fundamentalmatrix symmetrisch, in Formeln $F_{\mathcal{B}}(b)^\top = F_{\mathcal{B}}(b)$, so folgt mit 5.1.3 sofort $b \circ \tau = b$ alias b symmetrisch.

Proposition 5.1.5 (Fundamentalmatrix und Basiswechsel). *Gegeben ein Körper k und ein endlichdimensionaler k-Vektorraum V mit zwei angeordneten Basen $\mathcal{A}, \mathcal{B}$ gilt zwischen den Fundamentalmatrizen einer Bilinearform b in Bezug auf unsere beiden Basen die Beziehung*

$$ {}_{\mathcal{A}}[\mathrm{id}]_{\mathcal{B}}^\top \circ F_{\mathcal{A}}(b) \circ {}_{\mathcal{A}}[\mathrm{id}]_{\mathcal{B}} = F_{\mathcal{B}}(b) $$

5.1.6. Man berechnet also in Worten gesagt die Fundamentalmatrix einer Bilinearform bezüglich einer Basis aus ihrer Fundamentalmatrix bezüglich einer anderen Basis, indem man von rechts die Basiswechselmatrix dranmultipliziert und von links ihre Transponierte.

Beweis. Gegeben $v, w \in V$ gilt eben

$$ \begin{aligned} b(v, w) &= {}_{\mathcal{B}}[v]^\top \circ F_{\mathcal{B}}(b) \circ {}_{\mathcal{B}}[w] \\ b(v, w) &= {}_{\mathcal{A}}[v]^\top \circ F_{\mathcal{A}}(b) \circ {}_{\mathcal{A}}[w] \\ &= \left({}_{\mathcal{A}}[\mathrm{id}]_{\mathcal{B}} \circ {}_{\mathcal{B}}[v]\right)^\top \circ F_{\mathcal{A}}(b) \circ {}_{\mathcal{A}}[\mathrm{id}]_{\mathcal{B}} \circ {}_{\mathcal{B}}[w] \\ &= {}_{\mathcal{B}}[v]^\top \circ {}_{\mathcal{A}}[\mathrm{id}]_{\mathcal{B}}^\top \circ F_{\mathcal{A}}(b) \circ {}_{\mathcal{A}}[\mathrm{id}]_{\mathcal{B}} \circ {}_{\mathcal{B}}[w] \end{aligned} $$

Gilt für Matrizen $F, G \in \mathrm{M}(n \times m; k)$ jedoch $x^\top F y = x^\top G y$ für alle Spaltenvektoren $x \in k^n$, $y \in k^m$, so folgt durch Einsetzen der Vektoren der Standardbasis $F = G$. Damit liefern unsere Gleichungen die gewünschte Identität ${}_{\mathcal{A}}[\mathrm{id}]^\top_{\mathcal{B}} \circ F_{\mathcal{A}}(b) \circ {}_{\mathcal{A}}[\mathrm{id}]_{\mathcal{B}} = F_{\mathcal{B}}(b)$. □

5.2 Klassifikation symmetrischer Bilinearformen

5.2.1. Unter einer **Klassifikation** einer gewissen Art von mathematischen Strukturen versteht man im allgemeinen die Angabe einer Liste von "Standardstrukturen" derart, daß jede Struktur der vorgegebenen Art zu genau einer der Strukturen besagter Liste "isomorph" ist.

Beispiel 5.2.2. Zum Beispiel bilden für die Struktur eines endlich erzeugten Vektorraums über einem vorgegebenen Körper k die Vektorräume k^n für $n \in \mathbb{N}$ eine solche Liste, denn jeder endlich erzeugte k-Vektorraum ist isomorph zu genau einem k^n. Man sagt deshalb auch, die endlich erzeugten Vektorräume werden "klassifiziert durch ihre Dimension". Ähnlich und noch einfacher werden die endlichen Mengen klassifiziert durch ihre Kardinalität.

Beispiel 5.2.3. Lneare Abbildungen zwischen endlich erzeugten Vektorräumen werden etwa "klassifiziert durch die Dimensionen der beteiligten Vektorräume und den Rang der Abbildung". Nennen wir genauer lineare Abbildungen $f : V \to W$ und $f' : V' \to W'$ "isomorph" genau dann, wenn es Vektorraumisomorphismen $\phi : V \xrightarrow{\sim} V'$ und $\psi : W \xrightarrow{\sim} W'$ gibt mit $\psi f = f' \phi$, so daß also das Diagramm

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ {\scriptstyle\wr}\downarrow{\scriptstyle\phi} & & {\scriptstyle\wr}\downarrow{\scriptstyle\psi} \\ V' & \xrightarrow{f'} & W' \end{array}$$

kommutiert, so ist jede lineare Abbildung isomorph zu genau einer linearen Abbildung $k^n \to k^m$ mit einer Matrix in Smith-Normalform 1.9.7.

5.2.4 (**Physikalische Motivation**). In der speziellen Relativitätstheorie modelliert man die Welt, in der wir leben, als als einen vierdimensionalen reellen affinen Raum X aller "Raum-Zeit-Punkte" alias "Ereignisse". Wählen wir ein räumliches Koordinatensystem und einen Beginn der Zeitrechnung und eine Zeiteinheit, so können wir X mit dem $\mathbb{R}^4$ identifizieren und jedes Ereignis wird spezifiziert durch eine Zeitkoordinate und drei Raumkoordinaten, also ein Viertupel von reellen Zahlen (t, x, y, z). Das Licht breitet sich mit Lichtgeschwindigkeit aus. Genau dann wird also eine Explosion am Raumzeitpunkt $p = (t, x, y, z)$ gesehen bei $p' = (t', x', y', z')$, wenn gilt

$$t' \geq t \text{ und } c^2(t'-t)^2 - (x'-x)^2 - (y'-y)^2 - (z'-z)^2 = 0$$

für c die Lichtgeschwindigkeit. Betrachten wir auf dem Raum $\mathbb{R}^4$ die sogenannte **Lorentz-Metrik** alias die symmetrische Bilinearform l mit der Fundamentalmatrix

$$\operatorname{diag}(c^2, -1, -1, -1)$$

so kann die zweite unserer Bedingungen auch umgeschrieben werden zur Bedingung $l(\vec{v}, \vec{v}) = 0$ für $\vec{v} = p' - p$. Wenn Sie bereits die Definition einer Metrik kennen, seien Sie gewarnt, daß diese Lorentz-Metrik im Sinne der in der Mathematik üblichen Terminologie keine Metrik ist. Nun vergessen wir wieder unsere Koordinaten und modellieren die Welt, in der wir leben, als einen vierdimensionalen reellen affinen Raum X mitsamt einer symmetrischen Bilinearform

$$l : \vec{X} \times \vec{X} \to \mathbb{R}$$

auf seinem Richtungsraum. Wir fordern, daß deren Fundamentalmatrix bezüglich mindestens einer Basis die oben angegebene Gestalt hat und daß sie die Ausbreitung des Lichts in der Weise beschreibt, daß $l(\vec{v}, \vec{v}) = 0$ gleichbedeutend ist dazu, daß eine Explosion am Raumzeitpunkt $p \in X$ entweder bei $p + \vec{v}$ oder bei $p - \vec{v}$ gesehen werden kann. Wir werden später zeigen, daß jede weitere symmetrische Bilinearform l' mit der Eigenschaft $l'(\vec{v}, \vec{v}) = 0 \quad \Leftrightarrow \quad l(\vec{v}, \vec{v}) = 0$ bereits ein Vielfaches von l sein muß. Die Wahl eines möglichen l bedeutet die Wahl einer Längeneinheit oder gleichbedeutend einer Zeiteinheit in der speziellen Relativitätstheorie. Das ist jedoch nicht, was an dieser Stelle diskutiert werden soll. Wir stellen uns die viel einfachere Frage, ob unsere Bilinearform nicht etwa bezüglich einer anderen Basis auch $\operatorname{diag}(1, 1, 1, -1)$ als Fundamentalmatrix haben könnte. Das geht nun zwar nicht, aber wir wollen eben unter anderem verstehen, warum es nicht geht, und entwickeln dazu die Anfänge der allgemeinen Theorie der symmetrischen Bilinearformen.

5.2.5 (**Mathematische Motivation**). Gegeben ein Körper k interessiert man sich für die **Klassifikation der symmetrischen Bilinearformen über** k. Damit ist gemeint, daß wir eine Familie $(V_i, b_i)_{i \in I}$ von endlichdimensionalen k-Vektorräumen mit symmetrischer Bilinearform suchen mit der Eigenschaft, daß für jedes Paar (V, b) bestehend aus einem endlichdimensionalen k-Vektorraum V mit einer symmetrischen Bilinearform b genau ein $i \in I$ existiert derart, daß es einen Isomorphismus $V \xrightarrow{\sim} V_i$ gibt, unter dem unser b dem vorgegebenen b_i entspricht. Eine derartige Klassifikation ist eng mit der Struktur des Körpers verknüpft und im allgemeinen sehr schwierig zu erreichen. Wir geben zumindest im Fall eines algebraisch abgeschlossenen Körpers einer Charakteristik ungleich Zwei in 5.2.11 sowie im Fall $k = \mathbb{R}$ in 5.2.24 Klassifikationen an.

5.2.6. Gegeben ein Körper k und ein k-Vektorraum V verstehen wir wie in 4.6.3 unter einer **quadratischen Form** auf V eine Abbildung $q : V \to k$ die sich

darstellen läßt in der Gestalt $q(v) = f_1(v)g_1(v) + \ldots + f_r(v)g_r(v)$ mit $f_i, g_i \in V^\top$ Linearformen auf V.

5.2.7. Man erhält für jeden Körper k eine Bijektion

$$\begin{array}{ccc} \left\{ \begin{array}{c} \text{obere } (n \times n)\text{-Dreiecksmatrizen} \\ \text{mit Einträgen aus } k \end{array} \right\} & \xrightarrow{\sim} & \left\{ \begin{array}{c} \text{Quadratische Formen} \\ \text{auf } k^n \end{array} \right\} \\ (b_{ij}) & \mapsto & \sum_{i \geq j} b_{ij} x_i x_j \end{array}$$

Für jeden Körper einer Charakteristik $\operatorname{char} k \neq 2$ erhält man darüberhinaus auch eine Bijektion

$$\begin{array}{ccc} \left\{ \begin{array}{c} \text{symmetrische } (n \times n)\text{-Matrizen} \\ \text{mit Einträgen in } k \end{array} \right\} & \xrightarrow{\sim} & \left\{ \begin{array}{c} \text{Quadratische Formen} \\ \text{auf } k^n \end{array} \right\} \\ (a_{ij}) & \mapsto & \sum a_{ij} x_i x_j \end{array}$$

und koordinatenfrei formuliert ergibt sich für jeden endlichdimensionalen Vektorraum V über einem Körper einer Charakteristik $\operatorname{char} k \neq 2$ eine Bijektion

$$\begin{array}{ccc} \left\{ \begin{array}{c} \text{symmetrische Bilinearformen} \\ \text{auf } V \end{array} \right\} & \xrightarrow{\sim} & \left\{ \begin{array}{c} \text{Quadratische Formen} \\ \text{auf } V \end{array} \right\} \\ b & \mapsto & (v \mapsto b(v,v)) \end{array}$$

Ich erwähne das hier im Wesentlichen deshalb, weil in der Literatur das bei uns als Frage nach der "Klassifikation der symmetrischen Bilinearformen" formulierte Ziel meist als die Frage nach der "Klassifikation der quadratischen Formen" formuliert wird. Wenn man vom Fall der Charakteristik Zwei einmal absieht, sind diese beiden Fragen also äquivalent, und ich selbst jedenfalls kann mir quadratische Formen besser vorstellen als symmetrische Bilinearformen.

Beispiel 5.2.8. Über dem Körper $k = \mathbb{R}$ kann jede quadratische Form auf $\mathbb{R}^2$ durch linearen Koordinatenwechsel in genau eine der folgenden fünf Formen überführt werden: Den "parabolischen Topf" $x^2 + y^2$, die "Sattelfläche" $x^2 - y^2$, den "umgestülpten parabolischen Topf" $-x^2 - y^2$, das "Tal" x^2 und die "Ebene" 0. Formal sagt uns das der Trägheitssatz von Sylvester 5.2.24. Lassen wir nur orthogonale Koordinatenwechsel zu, so kann jede quadratische Form in genau eine Form der Gestalt $\lambda x^2 + \mu y^2$ überführt werden mit $\lambda \leq \mu$ reell: Das sagt uns der Satz über die Hauptachsentransformation 4.6.1.

Satz 5.2.9 (Existenz einer Orthogonalbasis). *Sei V ein endlichdimensionaler Vektorraum über einem Körper k mit $\operatorname{char} k \neq 2$. So gibt es für jede symmetrische Bilinearform b auf V eine* **Orthogonalbasis** *alias eine Basis $\mathcal{B} = (v_1, \ldots, v_n)$ von V mit*

$$i \neq j \quad \Rightarrow \quad b(v_i, v_j) = 0$$

5.2.10. Der Wortbestandteil “orthogonal” möge Sie nicht dazu verleiten, sich hier für b ein Skalarprodukt vorzustellen. Dieser Fall wurde eh bereits durch 4.2.13 erledigt. Sie mögen stattdessen etwa an die Nullform $b = 0$ denken oder an die Lorentzmetrik 5.2.4.

Beweis. Gilt für jeden Vektor $v \in V$ bereits $b(v,v) = 0$, so folgt $2b(v,w) = b(b+w, v+w) - b(v,v) - b(w,w) = 0$ für alle v, w. Wegen $2 \neq 0$ in k folgt $b = 0$ und jede Basis ist orthogonal. Sonst gibt es einen Vektor $v_1 \in V$ mit $b(v_1, v_1) \neq 0$. Dann ist

$$\begin{array}{rccc} \varphi: & V & \to & k \\ & w & \mapsto & b(v_1, w) \end{array}$$

eine lineare Abbildung mit $v_1 \notin \ker \varphi$. Aus Dimensionsgründen gilt sicher $kv_1 \oplus \ker \varphi = V$. Mit Induktion über die Dimension dürfen wir annehmen, daß $\ker \varphi$ eine Orthogonalbasis $(v_2, \ldots, v_n)$ besitzt. Dann ist aber $(v_1, v_2, \ldots, v_n)$ eine Orthogonalbasis von V. □

5.2.11. Ist $\operatorname{char} k \neq 2$ und k algebraisch abgeschlossen oder allgemeiner das Quadrieren eine Surjektion $k \twoheadrightarrow k$, $x \mapsto x^2$, so können wir die im Satz gefundene Basis sogar so abändern, daß die Fundamentalmatrix die Gestalt $\operatorname{diag}(1, \ldots, 1, 0, \ldots, 0)$ hat. Die Zahl der Einsen ist hierbei wohldefiniert, denn der Rang der der Fundamentalmatrix einer Bilinearform hängt von der gewählten Basis nach 5.1.5 überhaupt nicht ab.

Definition 5.2.12. Ist V ein endlichdimensionaler Vektorraum und b eine Bilinearform auf V, so erklären wir den **Rang** von b als den Rang einer Fundamentalmatrix

$$\operatorname{rk}(b) = \operatorname{rk} F_{\mathcal{B}}(b)$$

in Bezug auf eine und jede angeordnete Basis $\mathcal{B}$ von V. Nach 5.1.5 hängt diese Zahl in der Tat nicht von der Basis $\mathcal{B}$ ab.

Definition 5.2.13. Eine Bilinearform auf einem Vektorraum V oder allgemeiner eine **bilineare Paarung** alias eine bilineare Abbildung

$$b : V \times W \to k$$

vom Produkt zweier Vektorräume in den Grundkörper heißt **nichtausgeartet** genau dann, wenn es für jedes $v \in V \backslash 0$ ein $w \in W$ gibt mit $b(v,w) \neq 0$ und umgekehrt auch für jedes $w \in W \backslash 0$ ein $v \in V$ mit $b(v,w) \neq 0$. Andernfalls heißt unsere Bilinearform oder allgemeiner unsere Paarung **ausgeartet**.

Ergänzende Übung 5.2.14 (**Mackey**). Gegeben eine nichtausgeartete Paarung $b : V \times W \to k$ zwischen zwei Vektorraümen V, W unendlicher Dimension mit

abzählbarer Basis gibt es stets eine Basis $(v_n)_{n\in\mathbb{N}}$ von V und eine Basis $(w_n)_{n\in\mathbb{N}}$ von W derart, daß gilt $b(v_i, w_j) = \delta_{ij}$. Hinweis: Man beginne mit zwei beliebigen Basen und wechsle geeignet Basen.

Definition 5.2.15. Gegeben ein Körper k und ein k-Vektorraum V und eine Bilinearform $b : V \times V \to k$ erklären wir den **Ausartungsraum** alias das **Radikal** von V als den Untervektorraum

$$\operatorname{rad} b = \{v \in V \mid b(w, v) = 0 \quad \forall w \in V\}$$

Wir werden dieses Konzept im Wesentlichen nur für symmetrische oder alternierende Bilinearformen verwenden und verzichten deshalb darauf, unseren Ausartungsraum feiner "Rechtsausartungsraum" zu nennen und zusätzlich noch einen "Linksausartungsraum" einzuführen.

Satz 5.2.16 (Rang und Radikal). *Der Rang und das Radikal einer Bilinearform b auf einem endlichdimensionalen Vektorraum V sind verknüpft durch die Beziehung*

$$\operatorname{rk}(b) + \dim(\operatorname{rad}(b)) = \dim V$$

5.2.17. Eine Bilinearform auf einem endlichdimensionalen Vektorraum ist also insbesondere genau dann nichtausgeartet, wenn sie maximalen Rang hat.

Beweis. Ist $\mathcal{B}$ eine angeordnete Basis von V, so können wir $F_{\mathcal{B}}(b)$ auch verstehen als die Transponierte der Matrix der Abbildung $\hat{b} : V \to V^\top$, die jedem $w \in V$ die Linearform "paare mit w unter b" alias $(\hat{b}(w))(v) := b(w, v)$ zuordnet. Genauer und in Formeln haben wir

$$_{\mathcal{B}^\top}[\hat{b}]_{\mathcal{B}} = F_{\mathcal{B}}(b)^\top$$

In der Tat, setzen wir $\mathcal{B} = (v_1, \ldots, v_n)$ und machen den Ansatz $\hat{b}(v_i) = a_{1i}v_1^\top + \ldots + a_{ni}v_n^\top$, so liefert das Auswerten der Linearformen auf beiden Seiten dieser Gleichung auf dem Basisvektor v_j die Identität $b(v_i, v_j) = (\hat{b}(v_i))(v_j) = a_{ji}$ und damit die Gleichheit aller Einträge unserer beiden Matrizen. Insbesondere gilt $\operatorname{rk}(b) = \operatorname{rk}(\hat{b}) = \dim(\operatorname{im}\hat{b})$. Wegen $\operatorname{rad}(b) = \ker(\hat{b})$ folgt unsere Identität damit aus der Dimensionsformel 1.6.12, angewandt auf die lineare Abbildung $\hat{b} : V \to V^\top$. □

Ergänzung 5.2.18. Die Identität $_{\mathcal{B}^\top}[\hat{b}]_{\mathcal{B}} = F_{\mathcal{B}}(b)^\top$ aus dem vorhergehenden Beweis liefert auch einen zweiten Zugang zu unserer Formel 5.1.5 über das Verhalten der Fundamentalmatrix unter Basiswechsel: Wir rechnen einfach

$$F_{\mathcal{B}}(b)^\top = {}_{\mathcal{B}^\top}[\hat{b}]_{\mathcal{B}} = {}_{\mathcal{B}^\top}[\mathrm{id}]_{\mathcal{A}^\top} \circ {}_{\mathcal{A}^\top}[\hat{b}]_{\mathcal{A}} \circ {}_{\mathcal{A}}[\mathrm{id}]_{\mathcal{B}} = ({}_{\mathcal{A}}[\mathrm{id}]_{\mathcal{B}})^\top \circ F_{\mathcal{A}}(b)^\top \circ {}_{\mathcal{A}}[\mathrm{id}]_{\mathcal{B}}$$

unter Verwendung unserer Formel 1.11.15 für die Matrix der transponierten Abbildung. Transponieren liefert dann ein weiteres Mal unsere Formel 5.1.5.

Ergänzung 5.2.19. Übung 1.5.29 liefert uns für jeden Vektorraum V einen kanonischen Isomorphismus

$$\begin{array}{ccc} \mathrm{Bil}(V) & \xrightarrow{\sim} & \mathrm{Hom}(V, V^\top) \\ b & \mapsto & \hat{b} \end{array}$$

zwischen dem Raum der Bilinearformen auf V und dem Raum der linearen Abbildungen von V in seinen Dualraum $V^\top$, gegeben durch die Abbildungsvorschrift $b \mapsto \hat{b}$ mit $\hat{b} : v \mapsto b(v, \ )$ alias $(\hat{b}(v))(w) = b(v, w)$. In **??** verwende ich die alternative Notation $\hat{b} = \mathrm{can}_b^1$ und betrachte zusätzlich auch noch $\mathrm{can}_b^2 : V \to V^\top$ gegeben durch $v \mapsto b(\ , v)$.

5.2.20. Gegeben zwei Vektorräume V, W mit einer bilinearen Paarung $b : V \times W \to k$ und eine Teilmenge $T \subset W$ setzen wir ganz allgemein

$$T^\perp = \{v \in V \mid b(v, t) = 0 \quad \forall t \in T\}$$

und nennen $T^\perp$ wie in 4.2.14 den **Orthogonalraum von** U.

Ergänzende Übung 5.2.21. Gegeben zwei Vektorräume V, W mit einer nichtausgearteten Paarung $b : V \times W \to k$ und ein Untervektorraum $U \subset W$ zeige man für die Dimension des Orthogonalraums $U^\perp$ von U die Formel $\dim U + \dim U^\perp = \dim V$.

Definition 5.2.22. Sei k ein angeordneter Körper. Eine symmetrische quadratische Matrix $A \in M(n \times n; k)$ heißt

1. **positiv definit** genau dann, wenn gilt $x^\top Ax \leq 0 \Rightarrow x = 0$;
2. **positiv semidefinit** genau dann, wenn gilt $x^\top Ax \geq 0 \quad \forall x \in k^n$;
3. **negativ definit** genau dann, wenn gilt $x^\top Ax \geq 0 \Rightarrow x = 0$;
4. **negativ semidefinit** genau dann, wenn gilt $x^\top Ax \leq 0 \quad \forall x \in k^n$;
5. **indefinit** genau dann, wenn es $x, y \in k^n$ gibt mit $x^\top Ax > 0$ und $y^\top Ay < 0$;

5.2.23. Um die Definitheitseigenschaften einer symmetrischen quadratischen Matrix zu bestimmen, bringt man sie am einfachsten durch Basiswechsel in Diagonalgestalt, wie im Beweis von 5.2.9 erklärt. Bei kleineren Matrizen kann auch das Hurwitz-Kriterium 5.2.27 ein guter Trick sein.

Satz 5.2.24 (Sylvester'scher Trägheitssatz). *Gegeben ein endlichdimensionaler reeller Vektorraum V mit einer symmetrischen Bilinearform gibt es stets eine Basis $\mathcal{B} = (v_1, \ldots, v_n)$, in der die Fundamentalmatrix die Gestalt*

$$\mathrm{diag}(1, \ldots, 1, -1, \ldots, -1, 0, \ldots, 0)$$

annimmt. Die Zahl der Einsen, Minus-Einsen und Nullen wird hierbei durch besagte Bilinearform bereits eindeutig festgelegt.

5.2.25. Die Differenz zwischen der Zahl der Minus-Einsen und der Zahl der Einsen heißt in diesem Kontext die **Signatur** unserer symmetrischen Bilinearform.

Beweis. Die Existenz einer Basis mit den geforderten Eigenschaften folgt unmittelbar aus der Existenz einer Orthogonalbasis 5.2.9, indem wir deren Vektoren mit geeigneten Skalaren multiplizieren. Die Zahl der Nullen ist wohlbestimmt als die Dimension des Radikals V_0. Ich behaupte, daß die Zahl der Einsen bzw. Minus-Einsen beschrieben werden kann als die jeweils maximal mögliche Dimension für einen Teilraum, auf dem unsere Bilinearform positiv definit bzw. negativ definit ist. Sind in der Tat $V_+ \subset V$ und $V_- \subset V$ Teilräume der maximal möglichen Dimension mit dieser Eigenschaft, ja sogar irgendwelche Teilräume mit dieser Eigenschaft, so folgt $V_- \cap V_0 = 0$ und $V_+ \cap (V_- \oplus V_0) = 0$ und damit

$$\dim V_+ + \dim V_- + \dim V_0 \leq \dim V$$

Für jede Orthogonalbasis B bezeichne nun B_+, B_- und B_0 die Basisvektoren, deren Paarung mit sich selber eine positive Zahl bzw. eine negative Zahl bzw. Null ergibt. So haben wir natürlich

$$|B_+| + |B_-| + |B_0| = \dim V$$

Da aber wegen der Maximalität von $V_\pm$ offensichtlich gilt $|B_\pm| \leq \dim V_\pm$, und da $|B_0| \leq \dim V_0$ eh klar ist, muß bei diesen letzten Ungleichungen überall Gleichheit gelten. □

5.2.26. Gegeben ein Vektorraum über einem angeordneten Körper mit einer symmetrischen Bilinearform nennt man das Supremum über die Dimensionen aller "negativ definiten" Teilräume den **Index** unserer Bilinearform. Er ist auch im Fall unendlichdimensionaler Räume noch sinnvoll definiert, kann aber dann den Wert ∞ annehmen.

Satz 5.2.27 (Hurwitz-Kriterium). *Eine symmetrische $(n \times n)$-Matrix mit Einträgen in einem angeordneten Körper K ist positiv definit genau dann, wenn für alle $k \leq n$ die quadratische Untermatrix, die man durch Wegstreichen der letzten k Spalten und der untersten k Zeilen erhält, eine positive Determinante hat.*

Beweis. Wählen wir eine Orthogonalbasis der zu unserer Matrix gehörigen symmetrischen Bilinearform auf K^n, so hat die Determinante der zugehörigen diagonalen Fundamentalmatrix nach 5.1.5 dasselbe Vorzeichen wie die Determinante unserer Ausgangsmatrix. Ist also unsere Ausgangsmatrix nicht positiv definit und hat positive Determinante, so existiert ein zweidimensionaler Teilraum, auf dem sie negativ definit ist. Dieser Teilraum schneidet die Hyperebene $(K^{n-1} \times 0) \subset K^n$ nach dem Dimensionssatz 1.6.15 nicht nur in Null. Ist also unsere Ausgangsmatrix nicht positiv definit und hat positive Determinante, so ist die quadratische

Untermatrix, die man durch Wegstreichen der letzten Spalte und der untersten Zeile erhält, nicht positiv definit. Eine offensichtliche Induktion beendet den Beweis. □

Ergänzende Übung 5.2.28. Gegeben zwei verschiedene Punkte der Ebene $p, q \in \mathbb{R}^2$ und eine positive Zahl $b < \|p - q\|$ zeige man, daß die Punkte $r \in \mathbb{R}^2$ mit $\|r - p\| - \|r - q\| = b$ einen Hyperbelast bilden, als da heißt, daß die Menge dieser Punkte unter einer geeigneten Bewegung in die Menge der Lösungen mit positiver x-Koordinate eines Gleichungssystems der Gestalt $x^2 - \mu y^2 = c$ mit μ, c positiv übergeht. Gegeben zwei verschiedene Punkte der Ebene $p, q \in \mathbb{R}^2$ und eine positive Zahl $a > \|p - q\|$ zeige man weiter, daß die Punkte $r \in \mathbb{R}^2$ mit $\|r - p\| + \|r - q\| = a$ eine Ellipse bilden, als da heißt, daß die Menge dieser Punkte unter einer geeigneten Bewegung in die Menge der Lösungen eines Gleichungssystems der Gestalt $x^2 + \mu y^2 = c$ mit μ, c positiv übergeht. So erstellen übrigends Gärtner elliptische Beete: Sie rammen zwei Pflöcke ein, legen um diese eine Seilschlaufe und fahren mit einem dritten Pflock in der Schlaufe um diese beiden Pflöcke herum, soweit außen wie möglich.

Satz 5.2.29 (Satz über Hauptachsentransformationen, Variante). *Gegeben ein endlichdimensionaler reeller Vektorraum mit zwei symmetrischen Bilinearformen, von denen die Erste ein Skalarprodukt ist, besitzt unser Vektorraum eine Basis, die sowohl orthonormal ist für die erste als auch orthogonal für die zweite Bilinearform.*

5.2.30. Ist also in Formeln V unser endlichdimensionaler reeller Vektorraum und s ein Skalarprodukt auf V und b eine weitere symmetrische Bilinearform, so besitzt V eine Basis $(v_1, \ldots, v_n)$ mit $s(v_i, v_j) = \delta_{ij}$ und $b(v_i, v_j) = 0$ für $i \neq j$.

Beweis. Wir wählen eine Orthonormalbasis $\mathcal{B}$ in Bezug auf s. Die Fundamentalmatrix $A = F_{\mathcal{B}}(b)$ ist symmetrisch, nach dem Spektralsatz finden wir folglich $D \in \mathrm{SO}(n)$ mit $D^\top A D = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$. Jetzt können wir aber eine Basis $\mathcal{A}$ in V finden derart, daß $D = {}_{\mathcal{B}}[\mathrm{id}]_{\mathcal{A}}$ die Basiswechselmatrix von $\mathcal{A}$ nach $\mathcal{B}$ ist, und mit $\mathcal{B}$ ist nach 4.3.14 dann auch $\mathcal{A}$ eine Orthonormalbasis von V in Bezug auf s. Es folgt

$$F_{\mathcal{A}}(b) = D^\top F_{\mathcal{B}}(b) D = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$$

und wir haben in $\mathcal{A}$ unsere Basis gefunden, die für s orthonormal und für b orthogonal ist. □

Satz 5.2.31 (Satz über Hauptachsentransformationen, Variante). *Gegeben ein endlichdimensionaler komplexer Vektorraum mit zwei hermiteschen Bilinearformen, von denen die Erste ein Skalarprodukt ist, besitzt unser Vektorraum eine Basis, die sowohl orthonormal ist für die erste als auch orthogonal für die zweite Bilinearform.*

5.2.32. Ist also in Formeln V unser endlichdimensionaler komplexer Vektorraum und s ein Skalarprodukt auf V und b eine weitere hermitesche Bilinearform, so besitzt V eine Basis $(v_1, \ldots, v_n)$ mit $s(v_i, v_j) = \delta_{ij}$ und $b(v_i, v_j) = 0$ für $i \neq j$.

Beweis. Analog zum Beweis der reellen Variante 5.2.29. □

Korollar 5.2.33 (Singulärwertzerlegung). *Gegeben eine lineare Abbildung zwischen endlichdimensionalen reellen oder komplexen euklidischen Vektorräumen gibt es eine Orthonormalbasis des Ausgangsraums, die auf eine Familie von paarweise orthogonalen Vektoren abgebildet wird.*

5.2.34. In geeigneten Orthonormalbasen ist die Matrix unserer Abbildung mithin eine Diagonalmatrix mit nichtnegativen Einträgen auf der Diagonalen. Diese Einträge sind im übrigen wohldefiniert als die Quadratwurzeln der Eigenwerte des Produkts unserer Abbildung mit ihrer Adjungierten. Sie heißen die **Singulärwerte** unserer Abbildung.

5.2.35. Die Singulärwertzerlegung verallgemeinert die Polarzerlegung: Wir erhalten genauer eine Polarzerlegung aus einer Singulärwertzerlegung, indem wir "zunächst die Vektoren unserer Orthonormalbasis mit einer positiv semidefiniten Abbildung auf die Länge ihrer Bilder strecken oder stauchen, und die so auf die richtige Länge gebrachten Vektoren durch eine Drehung in die richtigen Richtungen bringen".

5.2.36. In der Sprache der Matrizen ausgedrückt besagt unser Satz, daß es für jede reelle bzw. komplexe Matrix A orthogonale bzw. unitäre quadratische Matrizen C, K gibt derart, daß $CAK = D$ diagonal ist mit nichtnegativen Einträgen. Diese Einträge sind dann wieder wohldefiniert und heißen die **Singulärwerte** unserer Matrix. Die Darstellung als Produkt $A = C^{-1}DK^{-1}$ schließlich heißt eine **Singulärwertzerlegung** unserer Matrix A.

Beweis. Sei $f : V \to W$ unsere Abbildung. Wir betrachten auf V zusätzlich zum Skalarprodukt $s = s_V$ auf V noch die positiv semidefinite symmetrische bzw. hermitesche Bilinearform $b(u, v) := s_W(f(u), f(v))$. Die vorhergehenden Varianten des Satzes über Hauptachsentransformationen liefern dann unmittelbar die Behauptung. □

Übung 5.2.37. Ist s ein Skalarprodukt auf einem Vektorraum über einem angeordneten Körper und $v_1, \ldots, v_n$ eine endliche Familie von Vektoren von V, so ist die Matrix $(s(v_i, v_j))_{ij}$ positiv semidefinit. Es reicht hierfür sogar, die Bilinearform s symmetrisch und positiv semidefinit anzunehmen. Hinweis: Man betrachte den Beweis von Satz 5.2.33 zur Singulärwertzerlegung.

5.3 Alternierende Bilinearformen

5.3.1. Ich erinnere daran, daß nach 3.3.1 eine Bilinearform **alternierend** heißt genau dann, wenn Null herauskommt, sobald wir an beiden Stellen denselben Vektor einsetzen. Ich kann für dieses Konzept leider keinerlei Anschauung anbieten.

Satz 5.3.2 (**Klassifikation alternierender Bilinearformen**). *Gegeben ein endlichdimensionaler Vektorraum V über einem Körper k und eine alternierende Bilinearform $\omega : V \times V \to k$ besitzt V stets eine Basis, bezüglich derer die Fundamentalmatrix von ω die Gestalt*

$$\begin{pmatrix} \boxed{\begin{matrix} 0 & -1 \\ 1 & 0 \end{matrix}} & & & & & \\ & \ddots & & & & \\ & & \boxed{\begin{matrix} 0 & -1 \\ 1 & 0 \end{matrix}} & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$

annimmt. Die Zahl der Zweierblöcke hängt hierbei nicht von der Wahl der Basis ab.

Beweis. Ist unsere Form nicht Null, so finden wir $v, w \in V$ mit $\omega(v, w) \neq 0$. Durch Multiplikation von v mit einem Skalar erreichen wir sogar $\omega(v, w) = 1$ und damit $\omega(w, v) = -1$. Diese beiden Vektoren v, w können wir schon einmal als die ersten beiden Vektoren unserer Basis in spe festhalten. Wir betrachten nun die Linearformen $\omega(v, \ ) : V \to k$ und $\omega(w, \ ) : V \to k$. Sie sind beide nicht Null und ihre Kerne sind verschieden, genauer liegt v im Kern der ersten, nicht aber der zweiten Abbildung und w im Kern der zweiten, nicht aber der ersten. Für den Schnitt

$$S = \{u \in V \mid \omega(v, u) = 0 = \omega(w, u)\}$$

haben wir also $\dim S = \dim V - 2$ und $(kv \oplus kw) \cap S = 0$. Aus Dimensionsgründen folgt

$$V = (kv \oplus kw) \oplus S$$

und eine offensichtliche Induktion über die Dimension beendet den Beweis der Existenz. Die Zahl der Nullen nach den Zweierkästchen kann nun aber beschrieben werden als die Dimension des Radikals unserer Bilinearform und ist deshalb ebenso wie die Zahl der Zweierkästchen von der Wahl der Basis unabhängig. □

5.3.3. Eine alternierende Bilinearform auf einem Vektorraum heißt **nicht ausgeartet** genau dann, wenn ihr Radikal Null ist. Eine nichtausgeartete alternierende Bilinearform heißt auch eine **symplektische Form**, und ein mit einer symplektischen Form versehener Vektorraum heißt ein **symplektischer Vektorraum**. Symplektische Vektorräume spielen in der Hamilton'schen Mechanik eine wichtige Rolle. Nach 1.4.23 ist die Dimension eines endlichdimensionalen symplektischen Vektorraums stets gerade.

6 Jordan'sche Normalform

6.1 Motivation durch Differentialgleichungen

6.1.1. Wie etwa in **??** erklärt wird, kann man die Exponentialabbildung auf komplexen quadratischen Matrizen erklären durch die Exponentialreihe

$$\begin{array}{rccc} \exp: & \mathrm{M}(n\times n;\mathbb{C}) & \to & \mathrm{M}(n\times n;\mathbb{C}) \\ & A & \mapsto & \sum_{k=0}^{\infty} \frac{1}{k!}A^k \end{array}$$

Wie etwa in **??** erklärt wird, spielt diese Abbildung eine zentrale Rolle bei der Lösung von Systemen linearer Differentialgleichungen mit konstanten Koeffizienten. Ist genauer $A \in \mathrm{M}(n\times n;\mathbb{C})$ eine quadratische Matrix und $c \in \mathbb{C}^n$ ein Spaltenvektor, so gibt es genau eine differenzierbare Abbildung $\gamma : \mathbb{R} \to \mathbb{C}^n$ mit Anfangswert $\gamma(0) = c$ derart, daß gilt $\dot\gamma(t) = A\gamma(t)$ für alle $t \in \mathbb{R}$, und zwar die Abbildung

$$\gamma(t) = \exp(tA)c$$

Diese Erkenntnis soll dazu motivieren, nach einem möglichst guten Verständnis von $\exp A$ zu suchen. Die Formal $\exp(PAP^{-1}) = P(\exp A)P^{-1}$ für P invertierbar folgt ziemlich direkt aus der Definition, wie Sie in der Analysis als Übung **??** ausführen dürfen. Des weiteren erklären wir in **??**, warum für kommutierende quadratische Matrizen A, B stets gilt $\exp(A+B) = (\exp A)(\exp B)$. In 6.4.1 werden wir im folgenden unter der Überschrift "Jordan-Zerlegung" zeigen, daß sich jede komplexe quadratische Matrix A auf genau eine Weise zerlegen läßt als eine Summe $A = D+N$ mit D diagonalisierbar und N nilpotent und $DN = ND$. Ist dann noch P invertierbar mit $PDP^{-1} = \mathrm{diag}(\lambda_1,\ldots,\lambda_n)$, so folgt

$$\begin{array}{rcl} \exp A & = & \exp D \ \exp N \\ & = & P^{-1}\exp(\mathrm{diag}(\lambda_1,\ldots,\lambda_n))P \ \exp N \\ & = & P^{-1}\,\mathrm{diag}(\mathrm{e}^{\lambda_1},\ldots,\mathrm{e}^{\lambda_n})P \ \exp N \\ \exp tA & = & P^{-1}\,\mathrm{diag}(\mathrm{e}^{t\lambda_1},\ldots,\mathrm{e}^{t\lambda_n})P \ \exp tN \end{array}$$

Hierbei bricht die Reihe für $\exp tN$ ab. Wir erhalten so ein recht befriedigendes qualitatives Bild und mit etwas mehr Rechnen auch eine sehr explizite Beschreibung der Lösungen.

Ergänzende Übung 6.1.2. Die Exponentialabbildung von Matrizen liefert eine Bijektion

$$\exp : \{\text{symmetrische Matrizen}\} \xrightarrow{\sim} \{\text{positiv definite symmetrische Matrizen}\}$$

6.2 Summen und Produkte von Vektorräumen

6.2.1 (**Produkte von Mengen**). Allgemeiner als in 1.2.1 diskutiert kann man auch für eine beliebige Familie von Mengen $(X_i)_{i\in I}$ eine neue Menge, ihr **Produkt**, bilden als die Menge aller Tupel $(x_i)_{i\in I}$ mit $x_i \in X_i$ für alle $i \in I$. Dieses Produkt notiert man

$$\prod_{i\in I} X_i$$

und die Projektionsabbildungen werden mit $\mathrm{pr}_j : \left(\prod_{i\in I} X_i\right) \to X_j$ oder ähnlich bezeichnet. Wieder können wir für beliebige Abbildungen $f_i : Z \to X_i$ eine Abbildung $f = (f_i)_{i\in I} : Z \to \prod_{i\in I} X_i$ definieren durch die Vorschrift $f(z) = (f_i(z))_{i\in I}$ und jede Abbildung von einer Menge Z in ein Produkt ist von dieser Form mit $f_i = \mathrm{pr}_i \circ f$. In Formeln ausgedrückt liefert das Nachschalten der Projektionen also für jede Menge Z eine Bijektion

$$\begin{array}{ccc} \mathrm{Ens}\left(Z, \prod_{i\in I} X_i\right) & \xrightarrow{\sim} & \prod_{i\in I} \mathrm{Ens}(Z, X_i) \\ f & \mapsto & (\mathrm{pr}_i \circ f) \end{array}$$

6.2.2 (**Disjunkte Vereinigungen von Mengen**). Dual kann man für eine beliebige Familie $(X_i)_{i\in I}$ von Mengen auch ihre **disjunkte Vereinigung**

$$\bigsqcup_{i\in I} X_i = \bigcup_{i\in I} (X_i \times \{i\})$$

bilden. Das Anhängen der Indizes auf der rechten Seite ist hier nur eine Vorsichtsmaßnahme für den Fall, daß unsere Mengen nicht disjunkt gewesen sein sollten. Jede derartige disjunkte Vereinigung ist versehen mit Inklusionsabbildungen $\mathrm{in}_j : X_j \to \left(\bigsqcup_{i\in I} X_i\right)$. Weiter können wir für beliebige Abbildungen $f_i : X_i \to Z$ in eine Menge Z die Abbildung $f : \bigsqcup_{i\in I} X_i \to Z$ bilden durch die Vorschrift $f(x) = f_i(x)$ für $x \in X_i$, und jede Abbildung der disjunkten Vereinigung in eine Menge Z ist von dieser Form mit $f_i = f \circ \mathrm{in}_i$. In Formeln ausgedrückt liefert das Vorschalten der Injektionen also für jede Menge Z eine Bijektion

$$\begin{array}{ccc} \mathrm{Ens}\left(\bigsqcup_{i\in I} X_i, Z\right) & \xrightarrow{\sim} & \prod_{i\in I} \mathrm{Ens}(X_i, Z) \\ f & \mapsto & (f \circ \mathrm{in}_i) \end{array}$$

Die disjunkte Vereinigung von endlich vielen Mengen $X_1, \ldots, X_n$ notieren wir auch $X_1 \sqcup \ldots \sqcup X_n$.

Definition 6.2.3. Gegeben eine Familie $(V_i)_{i\in I}$ von Vektorräumen über einem Körper k bilden wir zwei neue k-Vektorräume, ihr **Produkt** $\prod V_i$ und ihre **direkte Summe** oder kurz **Summe** $\bigoplus V_i$ durch die Regeln

$$\begin{array}{rcl} \prod_{i\in I} V_i & = & \{(v_i)_{i\in I} \mid v_i \in V_i\} \\ \bigoplus_{i\in I} V_i & = & \{(v_i)_{i\in I} \mid v_i \in V_i \text{ und nur endlich viele } v_i \text{ sind nicht null}\} \end{array}$$

mit der offensichtlichen komponentenweisen Addition und Multiplikation mit Skalaren aus k. Dieselben Konstruktionen sind auch im Fall vonm Gruppen sinnvoll, wenn wir "null" als das jeweilige neutrale Element verstehen, und wir werden beide Konstruktionen auch in diesem Kontext verwenden.

6.2.4. Für eine endliche Familie von Gruppen oder Vektorräumen $V_1, \ldots, V_s$ stimmen die direkte Summe und das Produkt überein. Wir benutzen dann alternativ die Notationen

$$V_1 \oplus \ldots \oplus V_s = V_1 \times \ldots \times V_s$$

Beispiel 6.2.5. Im Fall der konstanten Familie $(k)_{x\in X}$ erhalten wir einen Isomorphismus des freien Vektorraums über X im Sinne von 1.3.21 mit unserer direkten Summe

$$kX \xrightarrow{\sim} \bigoplus_{x\in X} k$$

vermittels der Abbildungsvorschrift $\sum_{x\in X} a_x x \mapsto (a_x)_{x\in X}$. Auch im Fall einer allgemeineren konstanten Familie $(V)_{x\in X}$ erhalten wir einen Vektorraumisomorphismus

$$\mathrm{Ens}(X, V) \xrightarrow{\sim} \prod_{x\in X} V$$

vermittels der Abbildungsvorschrift $f \mapsto (f(x))_{x\in X}$.

6.2.6. Das Produkt bzw. die Summe haben im Fall von Vektorräumen oder allgemeiner von abelschen Gruppen die folgenden Eigenschaften: Die offensichtlichen Einbettungen und Projektionen sind Homomorphismen

$$\mathrm{in}_i : V_i \hookrightarrow \bigoplus_{i\in I} V_i \qquad \text{bzw.} \qquad \mathrm{pr}_i : \prod_{i\in I} V_i \twoheadrightarrow V_i$$

und ist V ein weiterer k-Modul, so induzieren die durch Vorschalten der in_i bzw. Nachschalten der pr_i gegebenen Abbildungen Bijektionen, ja sogar Isomorphismen

$$\begin{array}{rcl} \mathrm{Hom}_k\left(\bigoplus_{i\in I} V_i, V\right) & \xrightarrow{\sim} & \prod_{i\in I} \mathrm{Hom}_k(V_i, V) \\ f & \mapsto & (f \circ \mathrm{in}_i)_{i\in I} \end{array}$$

$$\begin{array}{rcl} \mathrm{Hom}_k\left(V, \prod_{i\in I} V_i\right) & \xrightarrow{\sim} & \prod_{i\in I} \mathrm{Hom}_k(V, V_i) \\ f & \mapsto & (\mathrm{pr}_i \circ f)_{i\in I} \end{array}$$

Im Fall nichtabelscher Gruppen ist nur die zweite dieser Abbildungen eine Bijektion. Ich gebe zu, daß das Symbol in_i nun in zweierlei Bedeutung verwendet wird: Einmal bei Mengen für die Einbettung in eine disjunkte Vereinigung und ein andermal bei Vektorräumen für die Einbettung in eine direkte Summe. Was jeweils gemeint ist, muß aus dem Kontext erschlossen werden. Betrachten wir im

Fall des ersten Isomorphismus speziell den Fall $V = k$, so erhalten wir einen Isomorphismus zwischen dem Dualraum einer direkten Summe und dem Produkt der Dualräume der Summanden.

6.2.7. Gegeben eine Familie $(V_i)_{i\in I}$ von Untervektorräumen eines Vektorraums V bezeichnet man den von ihrer Vereinigung erzeugten Untervektorraum auch als ihre **Summe** und notiert ihn $\sum_{i\in I} V_i$. Diese Summe kann auch interpretiert werden als das Bild des natürlichen Homomorphismus $\bigoplus_{i\in I} V_i \to V$ von der direkten Summe nach V. Ist dieser Homomorphismus injektiv, so sagen wir, die **Summe der Untervektorräume** V_i **sei direkt** und schreiben statt $\sum_{i\in I} V_i$ auch $\bigoplus_{i\in I} V_i$.

Lemma 6.2.8. *Gegeben eine Familie $(V_i)_{i\in I}$ von Untervektorräumen eines Vektorraums V ist der natürliche Homomorphismus $\bigoplus_{i\in I} V_i \hookrightarrow V$ eine Injektion genau dann, wenn für jede endliche Teilmenge $J \subset I$ und jedes $i \in I\backslash J$ gilt*

$$V_i \cap \sum_{j\in J} V_j = 0$$

Beweis. Ist der natürliche Homomorphismus eine Injektion, so folgt aus $i \in I\backslash J$ offensichtlich $V_i \cap \sum_{j\in J} V_j = 0$, und das sogar für beliebiges $J \subset I$. Ist der natürliche Homomorphismus keine Injektion, so liegt ein von Null verschiedener Vektor $v = (v_i)_{i\in I} \neq 0$ der direkten Summe in seinem Kern. Dieser hat nur in endlich vielen Summanden eine von Null verschiedene Komponente, die Menge $K = \{i \mid v_i \neq 0\}$ ist also endlich und nicht leer. Per definitionem gilt nun $\sum_{k\in K} v_k = 0$. Wählen wir $i \in K$ und nehmen $J = K\backslash i$, so folgt $0 \neq -v_i = \sum_{j\in J} v_j$ und damit $V_i \cap \sum_{j\in J} V_j \neq 0$. □

Ergänzende Übung 6.2.9. Ist $(V_i)_{i\in I}$ eine Familie von Vektorräumen und $B_i \subset V_i$ jeweils eine Basis, so ist die Vereinigung $\bigcup_{i\in I} \mathrm{in}_i(B_i)$ der Bilder ihrer Basen eine Basis der direkten Summe $\bigoplus_{i\in I} V_i$. Diese Basis ist auch in offensichtlicher Bijektion zur disjunkten Vereinigung von Basen $\bigsqcup_{i\in I} B_i$.

6.3 Hauptraumzerlegung

Definition 6.3.1. Gegeben eine Abbildung $f : X \to X$ von einer Menge in sich selber nennen wir eine Teilmenge $Y \subset X$ **stabil unter** f genau dann, wenn gilt $x \in Y \Rightarrow f(x) \in Y$.

Definition 6.3.2. Gegeben ein Vektorraum V und dazu ein Endomorphismus $f : V \to V$ und ein Skalar λ aus dem Grundkörper erklären wir den **Eigenraum von** f **zum Eigenwert** λ durch

$$\mathrm{Eig}(f;\lambda) = \mathrm{Eig}(f|V;\lambda) = \ker(f - \lambda\,\mathrm{id})$$

und den **Hauptraum von f zum Eigenwert λ** durch

$$\mathrm{Hau}(f;\lambda) = \mathrm{Hau}(f|V;\lambda) = \bigcup_{n\geq 0} \ker(f-\lambda\,\mathrm{id})^n$$

Der Eigenraum zum Eigenwert λ besteht also genau aus allen Eigenvektoren zum Eigenwert λ und dem Nullvektor. Die von Null verschiedenen Elemente des Hauptraums zum Eigenwert λ heißen die **Hauptvektoren zum Eigenwert** λ.

6.3.3. Diese Räume sind beide Untervektorräume unseres ursprünglichen Vektorraums V. Sie sind auch offensichtlich stabil unter unserem Endomorphismus f, ja sogar unter jedem Endomorphismus $g : V \to V$, der mit f kommutiert, in Formeln impliziert $gf = fg$ also

$$g(\mathrm{Eig}(f;\lambda)) \subset \mathrm{Eig}(f;\lambda) \qquad \text{und} \qquad g(\mathrm{Hau}(f;\lambda)) \subset \mathrm{Hau}(f;\lambda).$$

Eine noch allgemeinere Aussage formuliert Übung 6.3.5.

Beispiel 6.3.4. Der Eigenraum zum Eigenwert Null einer linearen Abbildung $f : V \to V$ ist gerade ihr Kern $\mathrm{Eig}(f|V;0) = \ker f$. Der Eigenraum zum Eigenwert Eins einer linearen Abbildung $f : V \to V$ besteht genau aus allen Fixpunkten unserer Abbildung, in Formeln $\mathrm{Eig}(f|V;1) = V^f$. Der Hauptraum zum Eigenwert Null des durch Ableiten gegebenen Endomorphismus des Raums der Polynomfunktionen $\partial : \mathbb{R}[x] \to \mathbb{R}[x]$ ist der ganze Raum, in Formeln $\mathrm{Hau}(\partial;0) = \mathbb{R}[x]$. Allgemeiner hat ein Endomorphismus $f : V \to V$ eines Vektorraums die Eigenschaft $\mathrm{Hau}(f;0) = V$ genau dann, wenn es für jeden Vektor $v \in V$ ein $N \in \mathbb{N}$ gibt mit $f^N(v) = 0$. Man sagt dann auch, f sei **lokal nilpotent**.

Übung 6.3.5. Gegeben ein kommutatives Diagramm von Vektorräumen der Gestalt

$$\begin{array}{ccc} V & \xrightarrow{g} & W \\ x\downarrow & & \downarrow y \\ V & \xrightarrow{g} & W \end{array}$$

alias Vektorräume V, W und lineare Abbildungen $g : V \to W$ und $x : V \to V$ und $y : W \to W$ mit $gx = yg$ bildet g Eigenräume in Eigenräume und Haupträume in Haupträume ab. In Formeln gilt also für alle λ aus dem jeweiligen Grundkörper $g(\mathrm{Eig}(x;\lambda)) \subset \mathrm{Eig}(y;\lambda)$ und $g(\mathrm{Hau}(x;\lambda)) \subset \mathrm{Hau}(y;\lambda)$.

6.3.6. Ist der Hauptraum zu einem Eigenwert λ nicht Null, so ist auch der zugehörige Eigenraum nicht Null: Ist in der Tat ein Vektor $v \neq 0$ gegeben mit $(f-\lambda\,\mathrm{id})^n v = 0$ für ein $n \in \mathbb{N}$, so gibt es auch ein kleinstmögliches derartiges $n \geq 1$, und dann ist $(f-\lambda\,\mathrm{id})^{n-1}v$ ein Eigenvektor zum Eigenwert λ.

6.3.7. Ist $U \subset V$ ein unter einer linearen Abbildung $f : V \to V$ stabiler Untervektorraum, so gilt für die Einschränkung von f auf U offensichtlich

$$\begin{aligned} \operatorname{Eig}(f|U;\lambda) &= \operatorname{Eig}(f;\lambda) \cap U \\ \operatorname{Hau}(f|U;\lambda) &= \operatorname{Hau}(f;\lambda) \cap U \end{aligned}$$

6.3.8. Ist $V = U \oplus W$ die direkte Summe zweier unter f stabiler Untervektorräume, so gilt offensichtlich

$$\begin{aligned} \operatorname{Eig}(f|V;\lambda) &= \operatorname{Eig}(f|U;\lambda) \oplus \operatorname{Eig}(f|W;\lambda) \\ \operatorname{Hau}(f|V;\lambda) &= \operatorname{Hau}(f|U;\lambda) \oplus \operatorname{Hau}(f|W;\lambda) \end{aligned}$$

Ergänzende Übung 6.3.9. Gegeben eine Menge von paarweise kommutierenden Endomorphismen eines von Null verschiedenen endlichdimensionalen Vektorraums über einem algebraisch abgeschlossenen Körper gibt es stets einen simultanen Eigenvektor. Hinweis: 6.3.3

Ergänzende Übung 6.3.10. Sei V ein Vektorraum und $T \subset \operatorname{End} V$ ein endlichdimensionaler Untervektorraum seines Endomorphismenraums, der aus diagonalisierbaren und paarweise kommutierenden Abbildungen besteht. So besitzt V unter T eine "simultane Eigenraumzerlegung"

$$V = \bigoplus_{\lambda \in T^*} V_\lambda$$

in die "simultanen Eigenräume" $V_\lambda = \{v \in V \mid xv = \lambda(x)v \ \forall x \in T\}$. Hinweis: Sei $x_0, \ldots, x_n$ eine Basis von T. Da x_0 diagonalisierbar ist, zerfällt V in Eigenräume unter x_0. Da die x_i für $i \geq 1$ mit x_0 kommutieren, stabilisieren sie dessen Eigenräume. Eine Induktion unter Verwendung von 3.5.17 beendet den Beweis.

Ergänzende Übung 6.3.11. Ein Endomorphismus eines euklidischen Vektorraums heißt **normal** genau dann, wenn er einen Adjungierten besitzt und mit seinem Adjungierten kommutiert. Man zeige: Ein Endomorphismus eines endlichdimensionalen euklidischen Vektorraums ist genau dann normal, wenn es dazu eine Orthonormalbasis aus Eigenvektoren gibt. Hinweis: Kommutierende Endomorphismen stabilisieren die Eigenräume aller beteiligten Endomorphismen. Ist A^* adjungiert zu A, so sind $A + A^*$ und $\mathrm{i}(A - A^*)$ selbstadjungiert. Alternativer Zugang: Man beginne mit einem gemeinsamen Eigenvektor von A und A^* und wiederhole von dort ausgehend den Beweis des Spektralsatzes für selbstadjungierte Endomorphismen.

Proposition 6.3.12. *Die Summe der Haupträume ist stets direkt, d.h. für jeden Endomorphismus eines k-Vektorraums $f : V \to V$ liefern die Einbettungen der Haupträume eine Injektion*

$$\bigoplus_{\lambda \in k} \operatorname{Hau}(f;\lambda) \hookrightarrow V$$

Beweis. Wir zeigen zunächst, daß der Schnitt von je zwei Haupträumen zu verschiedenen Eigenwerten $\mu \neq \lambda$ der Nullraum ist. Sonst müßte es nämlich, da jeder Hauptraum nach 6.3.3 unter dem fraglichen Endomorphismus stabil ist und der Schnitt beider Haupträume folglich der Hauptraum zu μ im Hauptraum zu λ ist, nach 6.3.6 im Schnitt auch einen Eigenvektor $v \neq 0$ zum Eigenwert μ geben. Für diesen Vektor gälte jedoch $(f - \lambda\,\mathrm{id})^n v = (\mu - \lambda)^n v$, und das ist nicht Null für alle $n \geq 0$ im Widerspruch zu unserer Annahme $v \in \mathrm{Hau}(f;\lambda)$. Also ist der Schnitt von je zwei Haupträumen zu verschiedenen Eigenwerten der Nullraum. Wäre nun die Summe der Haupträume nicht direkt, so gäbe es nach 6.2.8 eine endliche direkte Summe

$$H = H_1 \oplus \ldots \oplus H_n$$

von Haupträumen, deren Bild in V von einem weiteren Hauptraum $\mathrm{Hau}(f;\mu)$ nichttrivial geschnitten wird. Da aber alle H_i stabil sind unter f, gilt nach 6.3.8

$$\mathrm{Hau}(f;\mu) \cap H = \mathrm{Hau}(f|H;\mu) = \mathrm{Hau}(f|H_1;\mu) \oplus \ldots \oplus \mathrm{Hau}(f|H_n;\mu)$$

und diese Summanden sind alle Null als Schnitte von Haupträumen zu verschiedenen Eigenwerten. Also ist der fragliche Schnitt doch Null und die Summe der Haupträume muß direkt sein. □

Beispiel 6.3.13. Wir zeigen, daß im $\mathbb{R}$-Vektorraum $\mathcal{C}^\infty(\mathbb{R},\mathbb{R})$ aller beliebig oft differenzierbaren Funktionen $\mathbb{R} \to \mathbb{R}$ die Funktionen $t \mapsto t^n \mathrm{e}^{\lambda t}$ eine linear unabhängige Familie $(t^n \mathrm{e}^{\lambda t})_{(n,\lambda)\in\mathbb{N}\times\mathbb{R}}$ bilden. In der Tat, betrachten wir den durch das Ableiten gegebenen Endomorphismus $D : \mathcal{C}^\infty(\mathbb{R},\mathbb{R}) \to \mathcal{C}^\infty(\mathbb{R},\mathbb{R})$, so liegen alle $t^n \mathrm{e}^{\lambda t}$ für festes λ im λ-Hauptraum $\mathrm{Hau}(D;\lambda)$. Wegen 6.3.12 reicht es also, für jedes feste λ die lineare Unabhängigkeit der $t^n \mathrm{e}^{\lambda t}$ zu zeigen. Diese folgt hinwiederum unmittelbar aus unserer Erkenntnis 2.5.19, daß ein reelles Polynom nur dann überall den Wert Null annimmt, wenn es das Nullpolynom ist. In derselben Weise zeigt man auch, daß im $\mathbb{C}$-Vektorraum $\mathcal{C}^\infty(\mathbb{R})$ aller beliebig oft differenzierbaren Funktionen $\mathbb{R} \to \mathbb{C}$ die Funktionen $t \mapsto t^n \mathrm{e}^{\lambda t}$ für komplexe λ eine linear unabhängige Familie $(t^n \mathrm{e}^{\lambda t})_{(n,\lambda)\in\mathbb{N}\times\mathbb{C}}$ bilden, vergleiche **??**.

Satz 6.3.14 (Hauptraumzerlegung). *Ein endlichdimensionaler Vektorraum über einem algebraisch abgeschlossenen Körper zerfällt unter jedem Endomorphismus in die direkte Summe seiner Haupträume.*

6.3.15. Ist $f : V \to V$ unser Endomorphismus und sind $\lambda_1, \ldots, \lambda_n$ seine Eigenwerte, so folgt also in Formeln

$$\mathrm{Hau}(f;\lambda_1) \oplus \ldots \oplus \mathrm{Hau}(f;\lambda_n) = V$$

Alternativ können wir auch schreiben

$$\bigoplus_{\lambda\in k} \mathrm{Hau}(f;\lambda) \xrightarrow{\sim} V$$

wobei zu verstehen ist, daß der Hauptraum $\mathrm{Hau}(f;\lambda)$ im Fall, daß λ kein Eigenwert ist, eben der Nullraum ist.

6.3.16. Der Satz gilt mit dem zweiten Beweis auch, wenn wir statt der algebraischen Abgeschlossenheit des Grundkörpers nur voraussetzen, daß das charakteristische Polynom unseres Endomorphismus über unserem Körper vollständig in Linearfaktoren zerfällt.

Erster Beweis. Wir zeigen zunächst, daß der Hauptraum zum Eigenwert Null stets ein unter unserem Endomorphismus stabiles Komplement besitzt. Bezeichnet $f : V \to V$ unseren Endomorphismus, so behaupten wir genauer sogar, daß für hinreichend großes $n \gg 0$ unser Vektorraum V in die direkte Summe

$$V = (\ker f^n) \oplus (\operatorname{im} f^n)$$

zerfällt. Die Bilder der f^ν bilden in der Tat für wachsendes ν eine monoton fallende Folge von Untervektorräumen. Da V nach Annahme endliche Dimension hat, gibt es eine Stelle n, ab der diese Folge konstant wird. Für dieses n muß die Surjektion $f^n : \operatorname{im} f^n \twoheadrightarrow \operatorname{im} f^{2n}$ aus Dimensionsgründen ein Isomorphismus sein, also haben wir $(\ker f^n) \cap (\operatorname{im} f^n) = 0$ und nochmaliger Dimensionsvergleich mit der Dimensionsformel 1.6.12 zeigt über 1.6.17 die behauptete Zerlegung, die man auch als **Fitting-Zerlegung** bezeichnet. Die Hauptraumzerlegung ergibt sich nun leicht mit vollständiger Induktion über die Dimension: Ist unser Vektorraum Null, so ist eh nichts zu zeigen. Sonst gibt es einen Eigenwert λ. Die Fitting-Zerlegung von V zum Endomorphismus $(f - \lambda\,\mathrm{id})$ liefert dann zum λ-Hauptraum von f ein f-stabiles Komplement, und dieses Komplement können wir nach Induktionsannahme bereits in die Summe seiner Haupträume zerlegen. □

Zweiter Beweis. Der Satz folgt mit der Direktheit der Summe der Haupträume 6.3.12 und Dimensionsvergleich auch unmittelbar aus der anschließenden Proposition 6.3.18, nach der die Dimensionen der Haupträume mit den Vielfachheiten der entsprechenden Eigenwerte als Nullstellen des charakteristischen Polynoms zusammenfallen. Man beachte jedoch, daß der hier gegebene Beweis der Proposition 6.3.18 auch auf der Fitting-Zerlegung beruht. □

Ergänzende Übung 6.3.17. Ein Vektorraum über einem algebraisch abgeschlossenen Körper zerfällt unter einem Endomorphismus in die direkte Summe seiner Haupträume genau dann, wenn unser Endomorphismus **lokal endlich** ist, als da heißt, jeder Vektor liegt in einem endlichdimensionalen unter unserem Endomorphismus stabilen Teilraum.

Proposition 6.3.18. *Gegeben ein Endomorphismus eines endlichdimensionalen Vektorraums stimmt die Dimension jedes Hauptraums überein mit der Vielfachheit des entsprechenden Eigenwerts als Nullstelle des charakteristischen Polynoms.*

6.3.19. Man nennt diese Vielfachheit auch die **algebraische Vielfachheit** des Eigenwerts, im Gegensatz zu seiner **geometrischen Vielfachheit**, unter der man die Dimension des zugehörigen Eigenraums versteht.

Beweis. Sei $f : V \to V$ unser Endomorphismus und λ ein Skalar. Die Fitting-Zerlegung zu $(f - \lambda\,\mathrm{id})$ zerlegt V in die direkte Summe des λ-Hauptraums und eines f-stabilen Komplements

$$V = \mathrm{Hau}(f;\lambda) \oplus W$$

derart, daß λ kein Eigenwert von $f : W \to W$ ist. Auf dem Hauptraum ist $(f - \lambda\,\mathrm{id})$ nilpotent, nach 1.10.12 finden wir also darin eine Basis, bezüglich derer die Matrix von $(f - \lambda\,\mathrm{id})$ obere Dreiecksgestalt hat mit Nullen auf der Diagonalen. Bezüglich derselben Basis hat die Matrix von f obere Dreiecksgestalt mit lauter Einträgen λ auf der Diagonalen. Ergänzen wir diese Basis durch eine Basis von W zu einer Basis von V, so ist die zugehörige Matrix von $f : V \to V$ blockdiagonal und unsere Formel 3.5.11 liefert $\chi_f(T) = (\lambda - T)^d \chi_{f|W}(T)$ für $d = \dim \mathrm{Hau}(f;\lambda)$ die Dimension des λ-Hauptraums und $\chi_{f|W}(T)$ ohne Nullstelle bei λ. □

Ergänzende Übung 6.3.20. Man zeige: Gegeben ein Vektorraum mit einem lokal endlichen Endomorphismus besitzt der Hauptraum zu Null stets genau ein unter besagtem Endomorphismus stabiles Komplement.

Ergänzung 6.3.21. Betrachten wir Vektorräume unendlicher Dimension, so besitzt der Hauptraum zum Eigenwert Null eines Endomorphismus im allgemeinen kein unter besagtem Endomorphismus stabiles Komplement mehr. Betrachten wir zum Beispiel den Vektorraum V aller Abbildungen von der Menge $\{(i,j) \in \mathbb{N}^2 \mid i \geq j\}$ in unseren Grundkörper und den Endomorphismus, der "jede Zeile eins nach unten rückt und die unterste Zeile zu Null mach". Der Hauptraum H zum Eigenwert Null besteht aus allen Funktionen, die nur auf endlich vielen Zeilen von Null verschieden sind. Betrachten wir den Vektor $v \in V$ mit

$$v(i,j) = \begin{cases} 1 & i = 2j; \\ 0 & \text{sonst,} \end{cases}$$

so ist sein Bild im in 9.1.1 diskutierten Quotientenvektorraum $\bar{v} \in V/H$ ein von Null verschiedener Vektor, der im Bild jeder Potenz unseres Endomorphismus liegt. In V selbst gibt es jedoch keinen derartigen von Null verschiedenen Vektor, folglich kann $H \subset V$ kein unter unserem Endomorphismus stabiles Komplement besitzen.

6.4 Jordan-Zerlegung

Satz 6.4.1 (Jordan-Zerlegung). *Sei V ein endlichdimensionaler Vektorraum über einem algebraisch abgeschlossenen Körper und $x \in \operatorname{End} V$ ein Endomorphismus von V. So gibt es genau eine Zerlegung $x = x_\mathrm{s} + x_\mathrm{n}$ mit x_s diagonalisierbar, x_n nilpotent und $x_\mathrm{s}x_\mathrm{n} = x_\mathrm{n}x_\mathrm{s}$.*

6.4.2. Der untere Index s bei x_s steht für "semisimple", die deutsche Übersetzung dafür ist "halbeinfach". Ein Endomorphismus a eines Vektorraums V über einem Körper k heißt ganz allgemein halbeinfach genau dann, wenn er über einem algebraischen Abschluß von k diagonalisierbar ist. In der Situation des Satzes heißen x_s bzw. x_n der **halbeinfache** bzw. der **nilpotente Anteil** von x. Die Zerlegung aus dem Satz bezeichnet man genauer auch als **additive Jordan-Zerlegung**, wenn man Verwechslungen mit der "multiplikativen Jordan-Zerlegung" aus 6.4.16 befürchtet.

Ergänzung 6.4.3. Statt den Grundkörper algebraisch abgeschlossen anzunehmen, reicht für die Gültigkeit unseres Satzes auch die Annahme aus, daß das charakteristische Polynom unseres Endomorphismus über unserem Körper vollständig in Linearfaktoren zerfällt. Der Beweis bleibt derselbe. Ersetzen wir im Satz die Bedingung "diagonalisierbar" durch die Bedingung "halbeinfach", so bleibt er auch ohne alle Forderungen an das charakteristische Polynom gültig für im Sinne von III.3.6.14 "vollkommene" Grundkörper, wie Sie im Rahmen der sogenannten "Galoistheorie" als Übung III.4.1.26 zeigen mögen.

Beweis. Gegeben ein Endomorphismus x eines endlichdimensionalen Vektorraums über einem algebraisch abgeschlossenen Körper erklären wir einen Endomorphismus x_s durch die Vorschrift, daß er auf dem Hauptraum $\operatorname{Hau}(x;\lambda)$ von x zum Eigenwert λ jeweils durch die Multiplikation mit λ operieren soll. Dann ist x_s diagonalisierbar, und setzen wir $x_\mathrm{n} = x - x_\mathrm{s}$, so ist x_n nilpotent und x_s kommutiert mit x und dann auch mit x_n. Das zeigt die Existenz unserer Zerlegung. Ist $x = s+n$ eine weitere Zerlegung mit s diagonalisierbar, n nilpotent und $sn = ns$, so folgt zunächst $sx = xs$ und dann, da s die Haupträume von x stabilisieren muß, auch $sx_\mathrm{s} = x_\mathrm{s}s$. So erkennen wir, daß x, s, n, x_s und x_n paarweise kommutieren. Natürlich ist dann $x_\mathrm{n} - n$ nilpotent. Da s die Haupträume von x stabilisiert und da nach 3.5.17 auch die Restriktion von s auf besagte Haupträume diagonalisierbar ist, folgt aus der Definition von x_s, daß auch $x_\mathrm{s} - s$ diagonalisierbar sein muß. Aus $x_\mathrm{n} - n = s - x_\mathrm{s}$ folgt dann aber sofort, daß beide Seiten Null sind. Das zeigt die Eindeutigkeit unserer Zerlegung. □

Ergänzung 6.4.4. Hier lassen sich x_s und x_n sogar als Polynome in x ohne konstanten Term ausdrücken, d.h. es gibt $P, Q \in T\mathbb{C}[T]$ mit $x_\mathrm{s} = P(x)$ und $x_\mathrm{n} = Q(x)$. In der Tat, falls N so groß ist, daß gilt $\operatorname{Hau}(x;\lambda) = \ker(x-\lambda)^N$ für alle

λ, so erhält man ein mögliches P aus dem chinesischen Restsatz III.2.2.4 als simultane Lösung der Kongruenzen $P \equiv \lambda \pmod{(T-\lambda)^N}$ für alle Eigenwerte λ von x und für $\lambda = 0$, und ein mögliches Q ist dann $T - P(T)$. Ich mag die in der Literatur übliche Argumentation mit diesen Polynomen jedoch nicht, sie sind mir zu willkürlich.

Satz 6.4.5 (Funktorialität der Jordan-Zerlegung). *Sei gegeben ein kommutatives Diagramm endlichdimensionaler Vektorräume über einem algebraisch abgeschlossenen Körper der Gestalt*

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ x\downarrow & & \downarrow y \\ V & \xrightarrow{f} & W \end{array}$$

Sind $x = x_\mathrm{s} + x_\mathrm{n}$ und $y = y_\mathrm{s} + y_\mathrm{n}$ die Jordan-Zerlegungen von x und y, so kommutieren auch die Diagramme

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ x_\mathrm{s}\downarrow & & \downarrow y_\mathrm{s} \\ V & \xrightarrow{f} & W \end{array} \qquad \begin{array}{ccc} V & \xrightarrow{f} & W \\ x_\mathrm{n}\downarrow & & \downarrow y_\mathrm{n} \\ V & \xrightarrow{f} & W \end{array}$$

Beweis. Aus $fx = yf$ folgt wegen $f(\mathrm{Hau}(x;\lambda)) \subset \mathrm{Hau}(y;\lambda)$ nach der im vorhergehenden Beweis von 6.4.1 gegebenen Beschreibung der Jordan-Zerlegung unmittelbar erst $fx_\mathrm{s} = y_\mathrm{s}f$ und dann $fx_\mathrm{n} = y_\mathrm{n}f$. □

6.4.6. Stabilisiert speziell ein Endomorphismus eines endlichdimensionalen Vektorraums einen vorgegebenen Teilraum, so stabilisieren nach 6.4.5 auch sein halbeinfacher und sein nilpotenter Anteil besagten Teilraum.

Ergänzung 6.4.7. Ein Endomorphismus eines Vektorraums heißt **lokal nilpotent** genau dann, wenn jeder Vektor von einer geeigneten Potenz unseres Endomorphismus annulliert wird alias wenn der ganze Vektorraum der Hauptraum zum Eigenwert Null ist. Beide Sätze 6.4.1 und 6.4.5 gelten weiter und mit demselben Beweis auch noch, wenn man statt der Endlichdimensionalität der darin auftauchenden Vektorräume nur fordert, daß die fraglichen Endomorphismen x und y im Sinne von 6.3.17 lokal endlich sein sollen, und von x_n schwächer nur fordert, daß es lokal nilpotent sein soll.

Ergänzende Übung 6.4.8 (**Operatornorm und Spektralradius**). Ist x ein Endomorphismus eines von Null verschiedenen endlichdimensionalen komplexen normierten Vektorraums V im Sinne von **??** und bezeichnet $\| \ \|$ die zugehörige Operatornorm auf $\mathrm{End}\, V$ im Sinne von **??**, so strebt $\sqrt[n]{\|x^n\|}$ für $n \to \infty$ gegen das Maximum der Beträge der Eigenwerte alias den **Spektralradius** von x. Hinweis: Zunächst folgere man aus **??**, daß der fragliche Grenzwert nicht von der auf

unserem Vektorraum gewählten Norm abhängt. Dann behandle man den diagonalisierbaren Fall mithilfe der Maximumsnorm in Bezug auf eine geeignete Basis. Schließlich behandle man den allgemeinen Fall mithilfe der Jordan-Zerlegung und erinnere **??**.

Ergänzende Übung 6.4.9. Gegeben ein endlichdimensionaler komplexer Vektorraum V und ein Endomorphismus $x : V \to V$ haben wir stets

$$\operatorname{im} x \supset \operatorname{im} x_{\mathrm{s}}$$

Hinweis: Das Bild von x_{s} ist genau die Summe der Haupträume zu von Null verschiedenen Eigenwerten und das Bild von x umfaßt offensichtlich diese Summe. Alternativ erkennt man $\operatorname{im} x \supset \operatorname{im}(x_{\mathrm{s}}^N)$ für hinreichend großes N durch Entwicklung von $x_{\mathrm{s}}^N = (x - x_{\mathrm{n}})^N$ nach der binomischen Formel und Ausklammern von x, und die Behauptung folgt wegen $\operatorname{im} x_{\mathrm{s}} = \operatorname{im} x_{\mathrm{s}}^N$.

Ergänzende Übung 6.4.10. Jeder Endomorphismus der Ordnung zwei eines Vektorraums über einem Körper einer von zwei verschiedenen Charakteristik ist diagonalisierbar. Hinweis: Später zeigen wir das als IV.1.1.9. Jeder Endomorphismus der Ordnung vier eines komplexen Vektorraums ist diagonalisierbar. Hinweis: Man zerlege zunächst in Eigenräume unter dem Quadrat unseres Endomorphismus. Allgemeiner werden Sie in 6.4.11 zeigen, daß jeder Endomorphismus endlicher Ordnung eines komplexen Vektorraums diagonalisierbar ist.

Ergänzende Übung 6.4.11. Sei k ein algebraisch abgeschlossener Körper der Charakteristik Null. Sei V ein k-Vektorraum und $\varphi : V \to V$ ein Endomorphismus "endlicher Ordnung", als da heißt, es gebe $n \geq 1$ mit $\varphi^n = \mathrm{id}$. So ist V die direkte Summe der Eigenräume von φ. Hinweis: Man behandle zunächst den endlichdimensionalen Fall mithilfe der Jordan-Zerlegung und beachte dabei, daß nach 2.2.13 höhere Potenzen eines nilpotenten Endomorphismus stets größere Kerne haben müssen, solange nicht beide fraglichen Potenzen bereits Null sind. Fortgeschrittene erkennen einen Spezialfall des Satzes von Maschke IV.2.6.1.

Ergänzende Übung 6.4.12. Gegeben ein Endomorphismus eines endlichdimensionalen Vektorraums über einem algebraisch abgeschlossenen Körper besteht der Hauptraum des transponierten Endomorphismus des Dualraums genau aus den Linearformen, die auf allen Haupträumen zu anderen Eigenwerten des ursprünglichen Endomorphismus verschwinden.

Ergänzung 6.4.13. Ein Endomorphismus f eines Vektorraums heißt **unipotent** genau dann, wenn $(f - \mathrm{id})$ nilpotent ist. Ein Endomorphismus f eines Vektorraums heißt **lokal unipotent** genau dann, wenn $(f - \mathrm{id})$ lokal nilpotent ist. Oft wird aber hier das Wörtchen "lokal" auch weggelassen.

Ergänzende Übung 6.4.14. Ein unipotenter Endomorphismus endlicher Ordnung eines Vektorraums über einem Körper der Charakteristik Null ist bereits die Identität.

Ergänzende Übung 6.4.15. Das Produkt von zwei kommutierenden nilpotenten Endomorphismen ist nilpotent. Das Produkt von zwei kommutierenden unipotenten Endomorphismen ist unipotent. Das Produkt von zwei kommutierenden halbeinfachen Endomorphismen ist halbeinfach.

Ergänzende Übung 6.4.16 (**Multiplikative Jordan-Zerlegung**). Jeder invertierbare Endomorphismus x eines endlichdimensionalen Vektorraums über einem algebraisch abgeschlossenen Körper läßt sich auf genau eine Weise darstellen als Produkt $x = x_{\mathrm{u}}x_{\mathrm{s}}$ mit x_{s} halbeinfach, x_{u} unipotent und $x_{\mathrm{u}}x_{\mathrm{s}} = x_{\mathrm{s}}x_{\mathrm{u}}$. Hinweis: Ist $x = x_{\mathrm{s}} + x_{\mathrm{n}}$ die additive Jordan-Zerlegung, so betrachte man $x = x_{\mathrm{s}}(\mathrm{id} + x_{\mathrm{s}}^{-1}x_{\mathrm{n}})$. Man zeige weiter, daß dieselbe Aussage auch für invertierbare lokal endliche Endomorphismen eines Vektorraums beliebiger Dimension gilt, und zeige die zu 6.4.5 analogen Funktorialitätseigenschaften.

Ergänzende Übung 6.4.17. Gegeben ein Endomorphismus A eines endlichdimensionalen komplexen Vektorraums V liegt $\mathbb{Z}$ im Kern des Gruppenhomomorphismus $\varphi_A : \mathbb{R} \to \mathrm{GL}(V)$ gegeben durch $t \mapsto \exp(tA)$ genau dann, wenn A diagonalisierbar ist mit sämtlichen Eigenwerten aus $2\pi\mathrm{i}\mathbb{Z}$. Weiter ist φ_A genau dann nicht injektiv, wenn A diagonalisierbar ist mit rein imaginären Eigenwerten, und wenn der von seinen Eigenwerten aufgespannte $\mathbb{Q}$-Vektorraum höchstens die Dimension Eins hat.

6.5 Jordan'sche Normalform

Definition 6.5.1. Gegeben $r \geq 1$ definieren wir eine $(r \times r)$-Matrix

$$J(r)$$

genannt der **nilpotente Jordan-Block der Größe** r, durch die Vorschrift $J(r)_{i,j} = 1$ für $j = i+1$ und $J(r)_{i,j} = 0$ sonst. Insbesondere ist also $J(1)$ die (1×1)-Matrix mit dem einzigem Eintrag Null.

Satz 6.5.2 (**Normalform nilpotenter Endomorphismen**). *Gegeben ein nilpotenter Endomorphismus eines endlichdimensionalen Vektorraums gibt es stets eine Basis derart, daß die Matrix unseres Endomorphismus in dieser Basis blockdiagonal ist mit nilpotenten Jordanblöcken auf der Diagonalen, also von der Gestalt*

$$\mathrm{diag}(J(r_1), \ldots, J(r_n))$$

Die positiven natürlichen Zahlen $r_1, \ldots, r_n$ sind hierbei durch unseren nilpotenten Endomorphismus eindeutig bestimmt bis auf Reihenfolge.

Der nilpotente Jordan-Block $J(r)$ der Größe r. Steht auf der Diagonalen statt der Nullen ein Skalar λ, so nennen wir die entsprechende Matrix einen
Jordan-Block der Größe r zum Eigenwert λ und notieren diese Matrix

$$J(r;\lambda) = J(r) + \lambda I_r$$

Ergänzung 6.5.3. Dieser Satz leistet im Sinne von 5.2.1 die Klassifikation aller Paare (V, N) bestehend aus einem endlichdimensionalen Vektorraum V über einem fest vorgegebenen Körper mitsamt einem nilpotenten Endomorphismus N. Zwei Paare (V, A) und (W, B) bestehend aus einem k-Vektorraum mit einem Endomorphismus nennen wir hier "isomorph" und schreiben $(V, A) \cong (W, B)$ genau dann, wenn es einen Isomorphismus $\phi : V \xrightarrow{\sim} W$ gibt mit $B \circ \phi = \phi \circ A$, so daß wir also ein kommutatives Diagramm erhalten der Gestalt

$$\begin{array}{ccc} V & \xrightarrow{A} & V \\ \wr\downarrow{\scriptstyle\phi} & & \wr\downarrow{\scriptstyle\phi} \\ W & \xrightarrow{B} & W \end{array}$$

Für jeden Körper k werden in diesem Sinne also die Paare bestehend aus einem endlichdimensionalen k-Vektorraum und einem nilpotenten Endomorphismus desselben "klassifiziert durch endliche Multimengen von positiven natürlichen Zahlen".

Beweis. Die Eindeutigkeit ist unproblematisch: Ist $N : V \to V$ unser nilpotenter Endomorphismus mit Matrix $\operatorname{diag}(J(r_1), \ldots, J(r_n))$, so finden wir für $n \geq 1$ unmittelbar

$$\dim(\operatorname{im} N^{n-1} / \operatorname{im} N^n) = |\{i \mid r_i \geq n\}|$$

Die Kenntnis aller dieser Zahlen legt aber die Multimenge der r_i bereits fest. Die Existenz folgt unmittelbar aus Lemma 6.5.4, das wir gleich im Anschluß beweisen. □

Lemma 6.5.4. *Ist $N : V \to V$ ein nilpotenter Endomorphismus eines endlichdimensionalen Vektorraums V, so gibt es eine Basis B von V derart, daß $B \cup \{0\}$ stabil ist unter N und daß jedes Element von B unter N höchstens ein Urbild in B hat.*

Beweis. Wir betrachten die Sequenz

$$\ker N \hookrightarrow V \twoheadrightarrow \operatorname{im} N$$

Mit Induktion über die Dimension von V dürfen wir annehmen, daß wir für das Bild von N eine derartige Basis bereits gefunden haben, sagen wir die Basis A. Jetzt ergänzen wir $\{a \in A \mid N(a) = 0\}$ durch irgendwelche $b_1, \ldots, b_s$ zu einer Basis des Kerns von N und wählen Urbilder $c_1, \ldots, c_r \in V$ für die Elemente von $A \backslash N(A)$ und behaupten, daß

$$B = A \cup \{b_1, \ldots, b_s\} \cup \{c_1, \ldots, c_r\}$$

Ich denke mir eine nilpotente Abbildung gerne in der hier gezeigten Weise. Die Kästchen stehen für Basisvektoren, unser Vektorraum hätte also die Dimension 14. Die Abbildung schiebt jedes Kästchen um eins nach links bzw. nach Null, wenn es dabei aus unserem Bild herausfällt. Die Matrix dieser Abbildung hat in der geeignet angeordneten Kästchenbasis offensichtlich Normalform, und die Längen der Zeilen entsprechen hierbei den Größen der Jordanblöcke.

Schraffiert eine Basis des Bildes von N, kreuzweise schraffiert eine Basis des Bildes von N^2. Die Höhe der zweiten Spalte ist also genau $\dim(\operatorname{im} N) - \dim(\operatorname{im} N^2)$.

eine Basis von V ist mit den geforderten Eigenschaften. Nach Konstruktion ist $B \cup \{0\}$ stabil unter N und jedes Element von B hat unter N höchstens ein Urbild in B. Wir müssen also nur noch zeigen, daß B eine Basis von V ist. Dazu schreiben wir B als die Vereinigung der beiden Mengen

$$\begin{array}{lcl} \{a \in A \mid N(a) \neq 0\} & \cup & \{c_1, \ldots, c_r\} \\ \{a \in A \mid N(a) = 0\} & \cup & \{b_1, \ldots, b_s\} \end{array}$$

und bemerken, daß die erste Menge ein System von Urbildern unter N für unsere Basis A von $(\operatorname{im} N)$ ist, wohingegen die zweite eine Basis von $(\ker N)$ ist. Damit ist unsere große Vereinigung eine Basis von V nach 1.6.13. □

Ergänzung 6.5.5. Dieses Lemma gilt sogar ohne die Voraussetzung, daß V endlichdimensional ist. Um das zu zeigen, müssen wir nur die Induktion statt über die Dimension von V über die Nilpotenzordnung von N laufen lassen und 1.4.38 verwenden. Für einen lokal nilpotenten Endomorphismus N findet man jedoch im Allgemeinen keine Jordan-Basis mehr, nebenstehendes Bild zeigt ein Gegenbeispiel. Im Fall abzählbarer Dimension kann man noch zeigen, daß es stets eine Jordan-Basis gibt, wenn der Schnitt der Bilder aller Potenzen Null ist. Das beruht auf dem "Satz von Ulm" aus der Logik. Im Fall beliebiger Dimension gilt auch das nicht mehr: Betrachten wir zum Beispiel den Raum V aller Abbildungen von der Menge $\{(i,j) \in \mathbb{N}^2 \mid i \geq j\}$ nach $\mathbb{R}$, die nur in endlich vielen Zeilen nicht identisch Null sind, und den Endomorphismus $N : V \to V$, der "jede Zeile um eins nach unten drückt und die nullte Zeile annulliert", in Formeln $(N(f))(i,j) = f(i,j+1)$ falls $i > j$ und $(N(f))(i,j) = 0$ falls $i = j$. Sicher hat V/NV eine abzählbare Basis, so daß es nur abzählbar viele "endliche Jordan-Ketten" geben könnte. Da V selbst keine abzählbare Basis besitzt, müßte es also auch mindestens eine, ja sogar überabzählbar viele "unendliche Jordan-Ketten" geben. Die Existenz einer Jordan-Basis stünde also im Widerspruch dazu, daß der Schnitt der Bilder aller Potenzen $\bigcap \operatorname{im} N^n$ der Nullraum ist. Das alles habe ich in Diskussion mit Martin Ziegler gelernt.

Korollar 6.5.6 (Jordan'sche Normalform). *Gegeben ein Endomorphismus eines endlichdimensionalen Vektorraums über einem algebraisch abgeschlossenen Körper gibt es eine Basis unseres Vektorraums derart, daß die Matrix unseres Endomorphismus bezüglich dieser Basis blockdiagonal ist von der Gestalt*

$$\operatorname{diag}(J(r_1;\lambda_1), \ldots, J(r_t;\lambda_t))$$

Die Jordan-Blöcke sind hierbei durch unseren Endomorphismus wohlbestimmt bis auf Reihenfolge.

Eine Basis mit der Eigenschaft aus Lemma 6.5.4 nennen wir auch eine **Jordan-Basis**. Dieses Bild zeigt einen lokal nilpotenten Endomorphismus, für den keine Jordan-Basis existiert. Die fetten Punkte stehen für Basisvektoren, die Pfeile zeigen, wie sie abgebildet werden. Wir erhalten so eine lokal nilpotente Abbildung, bei der der Schnitt der Bilder aller Potenzen nicht Null ist. Dennoch ist kein Element des zugehörigen Vektorraums "unendlich divisibel", folglich kann es in diesem Fall keine Jordan-Basis geben.

Zum Beweis von 6.5.4. Die fetten Punkte stellen die Elemente der Basis A des Bildes $\operatorname{im} N$ dar. Die c_i zusammen mit den $a \in A$ mit $N(a) \neq 0$ bilden ein System von Urbildern unter N der Elemente von A.

Ein Matrix in Jordan'scher Normalform mit drei Jordanblöcken. Genau dann hat eine komplexe (6×6)-Matrix A diese Jordan'sche Normalform, wenn ihr charakteristisches Polynom eine einfache Nullstelle bei 7 und eine fünffache Nullstelle bei 5 hat und $\ker(A - 5I)$ zweidimensional ist sowie $\ker(A - 5I)^2$ vierdimensional.

6.5.7. Dieser Satz leistet im Fall eines algebraisch abgeschlossenen Grundkörpers k im Sinne von 5.2.1 die Klassifikation der endlichdimensionalen k-Vektorräume mit einem ausgezeichneten Endomorphismus in Bezug auf den in 6.5.3 erklärten Isomorphie-Begriff. Genauer werden solche Daten "klassifiziert durch endliche Multimengen von Paaren aus $(k \times \mathbb{N}_{\geq 1})$".

6.5.8. Das Korollar gilt mit demselben Beweis auch, wenn wir statt der algebraischen Abgeschlossenheit des Grundkörpers nur voraussetzen, daß das charakteristische Polynom unseres Endomorphismus über unserem Körper vollständig in Linearfaktoren zerfällt. Gegeben eine quadratische Matrix ist die explizite Berechnung einer "Jordan-Basis" im allgemeinen nicht ganz einfach. Hierzu gibt es auch Algorithmen, mit denen ich Sie jedoch nicht belasten will, da die explizite Berechnung einer Jordan-Basis in der Praxis selten gebraucht wird. Wichtig an diesem Korollar sind vielmehr die darin enthaltenen strukturellen Aussagen über Endomorphismen von Vektorräumen.

Beweis. Sei f unser Endomorphismus. Der Satz über die Hauptraumzerlegung 6.3.14 zeigt, daß wir ohne Beschränkung der Allgemeinheit annehmen dürfen, daß es einen Skalar λ gibt, für den $(f - \lambda\,\mathrm{id})$ nilpotent ist. Der Satz über die Normalform nilpotenter Endomorphismen 6.5.2 beendet dann den Beweis. □

7 Gruppen

7.1 Restklassen

7.1.1. Ist $(G, \perp)$ eine Menge mit Verknüpfung und sind $A, B \subset G$ Teilmengen, so schreiben wir $A \perp B = \{a \perp b \mid a \in A,\ b \in B\} \subset G$ und erhalten auf diese Weise eine Verknüpfung auf der Menge aller Teilmengen von G, der sogenannten Potenzmenge $\mathcal{P}(G)$. Ist unsere ursprüngliche Verknüpfung assoziativ, so auch die induzierte Verknüpfung auf der Potenzmenge. Wir kürzen in diesem Zusammenhang oft die einelementige Menge $\{a\}$ mit a ab, so daß also zum Beispiel $a \perp B$ als $\{a\} \perp B$ zu verstehen ist.

Definition 7.1.2. Ist G eine Gruppe, $H \subset G$ eine Untergruppe und $g \in G$ ein Element, so nennen wir die Menge gH die **Linksnebenklasse von** g **unter** H und die Menge Hg die **Rechtsnebenklasse von** g **unter** H. Diese Nebenklassen sind also Teilmengen von G. Ein Element einer Nebenklasse nennt man einen **Repräsentanten** der besagten Nebenklasse. Weiter betrachten wir in G die beiden Mengensysteme

$$\begin{aligned} G/H &= \{gH \mid g \in G\} \\ H\backslash G &= \{Hg \mid g \in G\} \end{aligned}$$

aller Links- bzw. Rechtsnebenklassen von H in G. Die Elemente von G/H und von $H\backslash G$ sind also Teilmengen von G und G/H sowie $H\backslash G$ selbst sind dementsprechend Teilmengen der Potenzmenge $\mathcal{P}(G)$ von G.

7.1.3. Gegeben $G \supset H$ eine Gruppe mit einer Untergruppe sind die H-Rechtsnebenklassen in G paarweise disjunkt. In der Tat folgt aus $g \in xH$ alias $g = xh$ für $h \in H$ bereits $gH = xhH = xH$. Analoges gilt für die Linksnebenklassen.

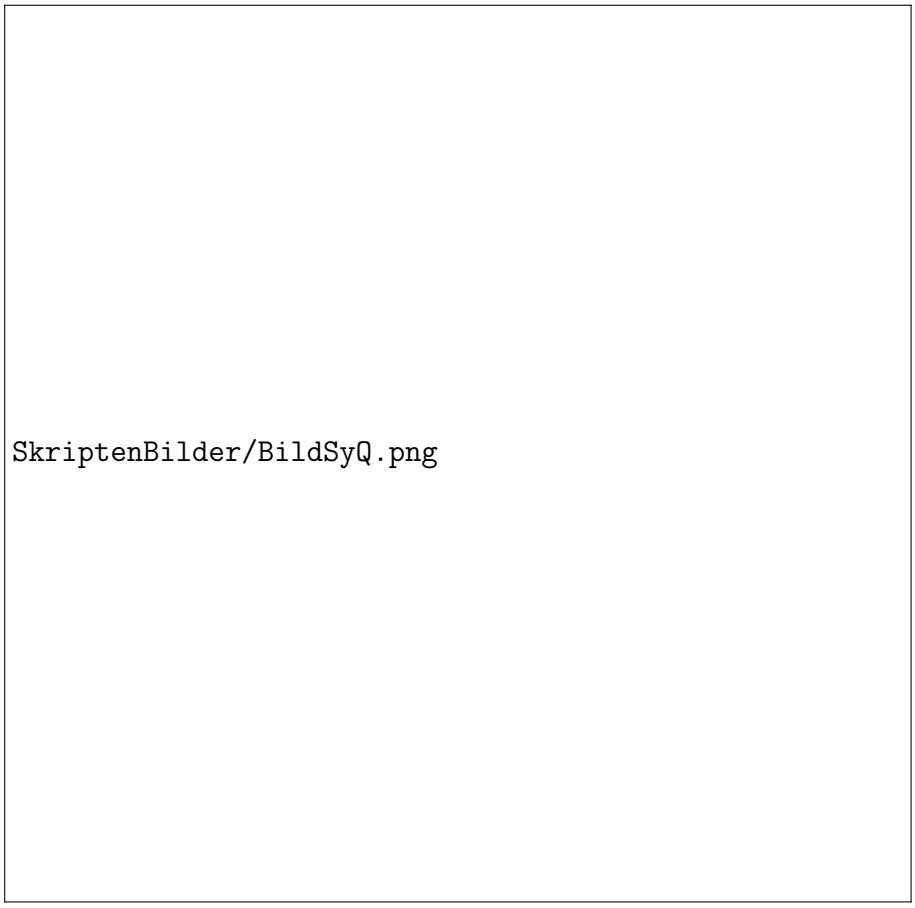
Beispiel 7.1.4. Im Fall $G = \mathbb{Z} \supset H = m\mathbb{Z}$ haben wir die Menge der Nebenklassen $\mathbb{Z}/m\mathbb{Z}$ bereits in 2.4.7 diskutiert und sogar selbst mit der Struktur einer Gruppe, ja sogar mit der Struktur eines Rings versehen. Im allgemeinen trägt G/H nur dann eine natürliche Gruppenstruktur, wenn wir an unsere Untergruppe H zusätzliche Forderungen stellen, vergleiche 7.2.

Satz 7.1.5 (Lagrange). *Gegeben eine endliche Gruppe teilt die Kardinalität jeder Untergruppe die Kardinalität der ganzen Gruppe. Ist G unsere endliche Gruppe und $H \subset G$ eine Untergruppe, so gilt genauer*

$$|G| = |H| \cdot |G/H| = |H| \cdot |H\backslash G|$$

Beweis. Jedes Element von G gehört zu genau einer Links- bzw. Rechtsnebenklasse unter H, und jede dieser Nebenklassen hat genau $|H|$ Elemente. □

Die drei Nebenklassen der Gruppe $\{\pm 1, \pm \mathrm{i}\}$ der vierten Einheitswurzeln in der Gruppe der zwölften Einheitswurzeln. Da diese Gruppe kommutativ ist, fallen hier Rechtsnebenklassen und Linksnebenklassen zusammen.



Die acht Symmetrien des Quadrats. Eine Rechtsnebenklasse der von der Spiegelung an der Nordost-Diagonalen erzeugten Untergruppe besteht aus den beiden Symmetrien des Quadrats, die die obere rechte Ecke in eine vorgegebene weitere Ecke überführen. Eine Linksnebenklasse besteht dahingegen aus den beiden Symmetrien des Quadrats, bei denen die obere rechte Ecke von einer vorgegebenen weiteren Ecke herkommt.

7.1.6. In anderen Worten kann man diesen Beweis auch dahingehend formulieren, daß alle Fasern der offensichtlichen Abbildung $G \to G/H$ genau $|H|$ Elemente haben, denn diese Fasern sind eben gerade die Linksnebenklassen von H in G.

Definition 7.1.7. Gegeben eine Gruppe G mit einer Untergruppe H heißt die Zahl $|G/H|$ der Restklassen auch der **Index** von H in G.

Ergänzende Übung 7.1.8. Haben zwei Untergruppen ein- und derselben Gruppe endlichen Index, so hat auch ihr Schnitt endlichen Index.

Ergänzende Übung 7.1.9. Seien $G \supset H$ eine Gruppe und eine Untergruppe. Man zeige, daß es eine Bijektion zwischen G/H und $H\backslash G$ gibt.

Ergänzende Übung 7.1.10. Haben zwei endliche Untergruppen einer Gruppe teilerfremde Kardinalitäten, so besteht ihr Schnitt nur aus dem neutralen Element.

7.2 Normalteiler und Restklassengruppen

Definition 7.2.1. Eine Untergruppe in einer Gruppe heißt ein **Normalteiler** besagter Gruppe genau dann, wenn die Rechtsnebenklassen unserer Untergruppe mit ihren Linksnebenklassen übereinstimmen. Ist G unsere Gruppe, so heißt also in Formeln eine Untergruppe $N \subset G$ ein Normalteiler genau dann, wenn gilt $gN = Ng \quad \forall g \in G$. Die Aussage "$N \subset G$ ist ein Normalteiler" kürzt man auch mit $N \lhd G$ ab.

Beispiele 7.2.2. In einer kommutativen Gruppe ist jede Untergruppe ein Normalteiler. In der Gruppe $\mathcal{S}_3$ der Permutationen von 3 Elementen ist die Untergruppe $\mathcal{S}_2 \subset \mathcal{S}_3$ aller Permutationen, die die dritte Stelle festhalten, kein Normalteiler.

Übung 7.2.3. Der Kern eines Gruppenhomomorphismus ist stets ein Normalteiler. Allgemeiner ist das Urbild eines Normalteilers unter einem Gruppenhomomorphismus stets ein Normalteiler, und das Bild eines Normalteilers unter einem surjektiven Gruppenhomomorphismus ist wieder ein Normalteiler.

Ergänzende Übung 7.2.4. Jede Untergruppe vom Index zwei ist ein Normalteiler.

Ergänzende Übung 7.2.5. Jede Untergruppe von endlichem Index umfaßt einen Normalteiler von endlichem Index.

Satz 7.2.6 (Konstruktion der Restklassengruppe). *Ist G eine Gruppe und $N \subset G$ ein Normalteiler, so ist die Menge G/N der Restklassen abgeschlossen unter der induzierten Verknüpfung auf der Potenzmenge $\mathcal{P}(G)$ von G und wird damit eine Gruppe, genannt die* **Restklassengruppe** *oder auch der* **Quotient** *von G nach N.*

Beweis. Es gilt $(gN)(g_1N) = gNg_1N = gg_1NN = gg_1N$, also ist unsere Menge stabil unter der Verknüpfung. Das Assoziativgesetz gilt eh, das neutrale Element ist N, und das Inverse zu gN ist $g^{-1}N$. □

Beispiel 7.2.7. Die Restklassengruppe $\mathbb{Z}/m\mathbb{Z}$ kennen wir bereits aus 2.4.7, wo wir darauf sogar noch eine Multiplikation erklärt hatten, die sie zu einem Ring macht. Sie hat genau m Elemente.

Satz 7.2.8 (Universelle Eigenschaft der Restklassengruppe). *Sei G eine Gruppe und $N \subset G$ ein Normalteiler. So gilt:*

1. *Die Abbildung $\mathrm{can} : G \to G/N, g \mapsto gN$ ist ein Gruppenhomomorphismus mit Kern N.*
2. *Ist $\varphi : G \to G'$ ein Gruppenhomomorphismus mit $\varphi(N) = \{1\}$, so gibt es genau einen Gruppenhomomorphismus $\tilde{\varphi} : G/N \to G'$ mit $\varphi = \tilde{\varphi} \circ \mathrm{can}$.*

7.2.9. Man kann die Aussage des zweiten Teils dieses Satzes auch dahingehend zusammenfassen, daß das Vorschalten der kanonischen Abbildung $\mathrm{can} : G \to G/N$ für jede weitere Gruppe G' eine Bijektion

$$\mathrm{Grp}(G/N, G') \xrightarrow{\sim} \{\varphi \in \mathrm{Grp}(G, G') \mid \varphi(N) = \{1\}\}$$

liefert. Der Übersichtlichkeit halber stelle ich die in diesem Satz auftauchenden Gruppen und Morphismen auch noch wieder anders in einem Diagramm dar:

$$\begin{array}{ccc} G & \xrightarrow{\mathrm{can}} & G/N \\ & \searrow^{\varphi} & \downarrow \tilde{\varphi} \\ & & G' \end{array}$$

Man sagt auch, φ **faktorisiert über** die kanonische Abbildung can in den Quotienten.

Beispiel 7.2.10. Wir haben etwa

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\mathrm{can}} & \mathbb{Z}/15\mathbb{Z} \\ & \searrow^{2\,\mathrm{can} = \varphi} & \downarrow \tilde{\varphi} \\ & & \mathbb{Z}/10\mathbb{Z} \end{array}$$

oder in Worten: Die Abbildung $\varphi = 2\,\mathrm{can} : \mathbb{Z} \to \mathbb{Z}/10\mathbb{Z}, n \mapsto (2n+10\mathbb{Z})$ faktorisiert über $\mathbb{Z}/15\mathbb{Z}$ und induziert so einen Gruppenhomomorphismus $\tilde{\varphi} : \mathbb{Z}/15\mathbb{Z} \to \mathbb{Z}/10\mathbb{Z}$.

Beweis. Die erste Aussage ist klar. Für die zweite Aussage beachten wir, daß unter der Annahme $\varphi(N) = \{1\}$ das Bild einer N-Nebenklasse $\varphi(gN) = \varphi(g)\varphi(N) = \{\varphi(g)\}$ nur aus einem einzigen Element besteht. Dies Element nennen wir $\tilde{\varphi}(gN)$, so daß also gilt $\tilde{\varphi}(gN) = \varphi(g)$ und $\varphi(gN) = \{\tilde{\varphi}(gN)\}$. Auf diese Weise erhalten wir die einzig mögliche Abbildung $\tilde{\varphi}$ mit $\tilde{\varphi} \circ \mathrm{can} = \varphi$. Um zu zeigen, daß sie ein Gruppenhomomorphismus ist, rechnen wir $\tilde{\varphi}((xN)(yN)) = \tilde{\varphi}(xyN) = \varphi(xy) = \varphi(x)\varphi(y) = \tilde{\varphi}(xN)\tilde{\varphi}(yN)$. □

Ergänzende Übung 7.2.11. Sei $m \in \mathbb{N}$ eine natürliche Zahl. Man zeige, daß die Vorschrift $\varphi \mapsto \varphi(\bar{1})$ für eine beliebige Gruppe G eine Bijektion liefert

$$\mathrm{Grp}(\mathbb{Z}/m\mathbb{Z}, G) \xrightarrow{\sim} \{g \in G \mid g^m = 1\}$$

Man beachte, daß hierbei $\bar{1}$ nicht das neutrale Element der additiv notierten Gruppe $\mathbb{Z}/m\mathbb{Z}$ bezeichnet, sondern die Nebenklasse der Eins, einen Erzeuger, wohingegen $1 \in G$ das neutrale Element der multiplikativ notierten Gruppe G meint. Wieviele Gruppenhomomorphismen gibt es von $\mathbb{Z}/m\mathbb{Z}$ nach $\mathbb{Z}/n\mathbb{Z}$?

Satz 7.2.12 (Isomorphiesatz). *Jeder Homomorphismus $\varphi : G \to H$ von Gruppen induziert einen Isomorphismus $\tilde{\varphi} : G/\ker\varphi \xrightarrow{\sim} \mathrm{im}\,\varphi$.*

Beispiel 7.2.13. Die Abbildung $\varphi = 2\,\mathrm{can} : \mathbb{Z} \to \mathbb{Z}/10\mathbb{Z}$, $n \mapsto (2n + 10\mathbb{Z})$ hat den Kern $\ker\varphi = 5\mathbb{Z}$ und das Bild $\ker\varphi = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\} \subset \mathbb{Z}/10\mathbb{Z}$. Der Isomorphiesatz liefert in diesem Fall also einen Gruppenisomorphismus

$$\mathbb{Z}/5\mathbb{Z} \xrightarrow{\sim} \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}\}$$

Beweis. Sicher ist unser $\tilde{\varphi}$ surjektiv. Es ist nach 2.2.14 aber auch injektiv, denn sein Kern besteht nur aus dem neutralen Element der Restklassengruppe. □

Korollar 7.2.14 (Noether'scher Isomorphiesatz). *Ist G eine Gruppe und sind $K \subset H \subset G$ zwei Normalteiler von G, so induziert die Komposition von kanonischen Abbildungen $G \twoheadrightarrow (G/K) \twoheadrightarrow (G/K)/(H/K)$ einen Isomorphismus*

$$G/H \xrightarrow{\sim} (G/K)/(H/K)$$

Beweis. Sicher ist unsere Komposition surjektiv. Unsere Aussage folgt also aus dem Isomorphiesatz 7.2.12, sobald wir zeigen, daß H der Kern unserer Komposition ist. Sicher ist H eine Teilmenge dieses Kerns. Liegt umgekehrt $g \in G$ im Kern unserer Komposition $G \twoheadrightarrow (G/K)/(H/K)$, so liegt die Nebenklasse gK im Kern von $(G/K) \twoheadrightarrow (G/K)/(H/K)$, als da heißt, es gibt $h \in H$ mit $gK = hK$, und daraus folgt sofort $g \in H$. □

Ergänzende Übung 7.2.15. Man nennt einen surjektiven Gruppenhomomorphismus $A \twoheadrightarrow A''$ **spaltend** genau dann, wenn er ein Rechtsinverses besitzt, und nennt solch ein Rechtsinverses dann eine **Spaltung**. Man zeige: Ist $\varphi : A \twoheadrightarrow A''$ ein surjektiver Homomorphismus von abelschen Gruppen, $A' \subset A$ sein Kern und $\psi : A'' \to A$ eine Spaltung von φ, so erhalten wir vermittels der Vorschrift $(a', a'') \mapsto a' + \psi(a'')$ einen Isomorphismus $A' \times A'' \xrightarrow{\sim} A$. Verallgemeinerungen auf den Fall nichtabelscher Gruppen besprechen wir in III.1.2.10.

Ergänzende Übung 7.2.16. Jede Surjektion von einer abelschen Gruppe auf $\mathbb{Z}^r$ spaltet. Man gebe ein Beispiel für einen surjektiven Gruppenhomomorphismus, der nicht spaltet.

Übung 7.2.17. Man zeige, daß das Multiplizieren von Matrizen mit Spaltenvektoren eine Bijektion $\mathrm{M}(n \times m; \mathbb{Z}) \xrightarrow{\sim} \mathrm{Grp}(\mathbb{Z}^m, \mathbb{Z}^n)$, $A \mapsto (A\circ)$ zwischen der Menge aller $(n \times m)$-Matrizen mit ganzzahligen Einträgen und der Menge aller Gruppenhomomorphismen $\mathbb{Z}^m \to \mathbb{Z}^n$ liefert.

7.3 Zyklische Gruppen

Definition 7.3.1. Eine Gruppe heißt **zyklisch** genau dann, wenn sie im Sinne von 2.2.7 von einem einzigen Element erzeugt wird.

7.3.2. Zum Beispiel ist eine Gruppe G, deren Kardinalität eine Primzahl ist, notwendig zyklisch, da sie nach 7.1.5 außer $H = G$ und $H = 1$ keine weiteren Untergruppen haben kann. Für jede Gruppe G können wir die von einem Element $g \in G$ erzeugte Untergruppe beschreiben als

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$$

Definition 7.3.3. Sei g ein Element einer Gruppe G. Die **Ordnung**

$$\operatorname{ord} g$$

von g ist die kleinste natürliche Zahl $n \geq 1$ mit $g^n = 1_G$. Gibt es kein solches n, so setzen wir $\operatorname{ord} g = \infty$ und sagen, g habe **unendliche Ordnung**. In jeder Gruppe ist das einzige Element der Ordnung 1 das neutrale Element. Elemente der Ordnung 2 heißen auch **Involutionen**. Elemente, die ihre eigenen Inversen sind, nenne ich **selbstinvers**. In jeder Gruppe ist das neutrale Element das einzige Selbstinverse, das keine Involution ist.

Lemma 7.3.4 (Struktur zyklischer Gruppen). *Ist G eine Gruppe und $g \in G$ ein Element, so stimmt die Ordnung von g überein mit der Kardinalität der von g erzeugten Untergruppe, in Formeln $\operatorname{ord} g = |\langle g \rangle|$. Genauer gilt:*

1. *Hat g unendliche Ordnung, so ist die Abbildung $\nu \mapsto g^\nu$ ein Isomorphismus $\mathbb{Z} \xrightarrow{\sim} \langle g \rangle$.*

2. *Hat g endliche Ordnung $\operatorname{ord} g = n$, so induziert $\nu \mapsto g^\nu$ einen Isomorphismus $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \langle g \rangle$.*

Beweis. Wir betrachten den Gruppenhomomorphismus $\varphi : \mathbb{Z} \to G, \nu \mapsto g^\nu$. Nach dem Isomorphiesatz 7.2.12 haben wir einen Isomorphismus $\mathbb{Z}/\ker\varphi \xrightarrow{\sim} \operatorname{im}\varphi = \langle g \rangle$. Nach der Klassifikation 2.2.16 der Untergruppen von $\mathbb{Z}$ ist $\ker\varphi$ von der Form $\ker\varphi = n\mathbb{Z}$ für ein $n \in \mathbb{Z}$, $n \geq 0$, und dann gilt notwendig $n = \operatorname{ord} g$ für g von endlicher Ordnung bzw. $n = 0$ für g von unendlicher Ordnung. □

7.3.5. Motiviert durch dies Lemma nennt man die Kardinalität einer Gruppe auch oft die **Ordnung der Gruppe**. Wir haben mit unserem Lemma im Übrigen auch bewiesen, daß jede Gruppe mit genau 5 Elementen isomorph ist zu $\mathbb{Z}/5\mathbb{Z}$, denn für jedes vom neutralen Element verschiedene Element unserer Gruppe ist $\langle g \rangle$ eine Untergruppe mit mindestens zwei Elementen, also nach Lagrange bereits die ganze Gruppe. Allgemeiner ist aus demselben Grund jede Gruppe von Primzahlordnung zyklisch.

Ergänzung 7.3.6. Für die endlichen zyklischen Gruppen $\mathbb{Z}/n\mathbb{Z}$ mit $n \geq 1$ sind viele alternative Notationen gebräuchlich. Ich kenne insbesondere die alternativen Notationen C_n, Z_n und $\mathbb{Z}_n$, von denen ich die Letzte am wenigsten mag, da sie im Fall einer Primzahl p auch für die sogenannten p-adischen Zahlen benutzt wird.

Korollar 7.3.7. *Bei einer endlichen Gruppe G teilt die Ordnung jedes Elements $g \in G$ die Ordnung der ganzen Gruppe und es gilt*

$$g^{|G|} = 1$$

Beweis. Man wende den Satz von Lagrange 7.1.5 an auf die von unserem Element erzeugte Untergruppe. Es folgt, daß $r := \operatorname{ord} g = |\langle g \rangle|$ ein Teiler von $|G|$ ist, $|G| = ra$ mit $a \in \mathbb{N}$. Dann folgt aber

$$g^{|G|} = g^{ra} = (g^r)^a = 1^a = 1$$ □

Korollar 7.3.8 (Kleiner Fermat). *Ist p eine Primzahl, so gilt für alle ganzen Zahlen $a \in \mathbb{Z}$ die* **Fermat'sche Kongruenz**

$$a^p \equiv a \pmod{p}$$

Beweis. Die multiplikative Gruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ des Körpers $\mathbb{Z}/p\mathbb{Z}$ hat genau $p-1$ Elemente, nach 7.3.7 gilt also $b^{p-1} = 1$ für alle $b \in (\mathbb{Z}/p\mathbb{Z})^\times$. Es folgt $b^p = b$ für alle $b \neq 0$, und für $b = 0$ gilt diese Gleichung eh. Mit $b = a + p\mathbb{Z}$ ergibt sich dann die Behauptung. □

Ergänzung 7.3.9. Allgemeiner bezeichnet man für $m \geq 1$ mit $\varphi(m)$ die Zahl der zu m teilerfremden Zahlen i mit $1 \leq i \leq m$ und nennt die so definierte Funktion φ die **Euler'sche φ-Funktion**. Wir haben etwa $\varphi(1) = \varphi(2) = 1$, $\varphi(3) = \varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$ und so weiter. Nach 2.4.45 kann $\varphi(m)$ auch interpretiert werden als die Ordnung der Einheitengruppe des Restklassenrings $\mathbb{Z}/m\mathbb{Z}$, in Formeln $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times|$. Wenden wir auf diese Gruppe unsere Erkenntnis 7.3.7 an, daß die Ordnung jedes Elements einer endlichen Gruppe die Gruppenordnung teilt, so erhalten wir für b teilerfremd zu m insbesondere die sogenannte **Euler'sche Kongruenz**

$$b^{\varphi(m)} \equiv 1 \pmod{m}$$

Ergänzende Übung 7.3.10. Sei k ein endlicher Körper mit $|k| = q$ Elementen. Man zeige $a^q = a$ für alle $a \in k$. Man zeige weiter, daß der Kern unserer Surjektion $k[X_1, \ldots, X_n] \to \mathrm{Ens}(k^n, k)$ aus 2.5.37 genau aus denjenigen Polynomen besteht, die sich als Summe $P_1(X_1^q - X_1) + \ldots + P_n(X_n^q - X_n)$ der Produkte von irgendwelchen Polynomen $P_i \in k[X_1, \ldots, X_n]$ mit den Polynomen $(X_i^q - X_i)$ schreiben lassen. Hinweis: Unsere Summen von Produkten bilden einen Untervektorraum, zu dem der Untervektorraum aller Polynome, in denen kein X_i in der Potenz q oder höher vorkommt, komplementär ist.

Übung 7.3.11. Man zeige: Jede Untergruppe einer zyklischen Gruppe ist zyklisch. Genauer haben wir für beliebiges $m \in \mathbb{N}$ eine Bijektion

$$\begin{array}{ccc} \{\text{Teiler } d \in \mathbb{N} \text{ von } m\} & \xrightarrow{\sim} & \{\text{Untergruppen von } \mathbb{Z}/m\mathbb{Z}\} \\ d & \mapsto & d\mathbb{Z}/m\mathbb{Z} \end{array}$$

Man folgere, daß jede von der ganzen Gruppe verschiedene Untergruppe einer zyklischen Gruppe von Primzahlpotenzordnung $\mathbb{Z}/p^r\mathbb{Z}$ in der Untergruppe $p\mathbb{Z}/p^r\mathbb{Z} \subset \mathbb{Z}/p^r\mathbb{Z}$ enthalten sein muß. Hinweis: 2.2.16.

Proposition 7.3.12. *Jede Untergruppe einer endlich erzeugten abelschen Gruppe ist endlich erzeugt, und für die Untergruppe benötigt man höchstens soviele Erzeuger wie für die ganze Gruppe.*

Beweis. Induktion über die Zahl der Erzeuger. Im Fall einer zyklischen Gruppe wissen wir nach 7.3.11 bereits, daß auch jede ihrer Untergruppen zyklisch ist. Sei nun unsere Gruppe G additiv notiert und sei $g_0, \ldots, g_n$ ein Erzeugendensystem. Sei $H \subset G$ eine Untergruppe. Nach 7.3.11 ist $H \cap \langle g_0 \rangle$ zyklisch, etwa erzeugt von h_0. Nach Induktionsannahme ist das Bild von H in $G/\langle g_0 \rangle$ endlich erzeugt, etwa von den Nebenklassen $\bar{h}_1, \ldots, \bar{h}_n$ gewisser Elemente $h_1, \ldots, h_n \in H$. Der Leser wird nun in Anlehnung an den Beweis von 1.6.13 unschwer zeigen können, daß $h_0, h_1, \ldots, h_n$ bereits ganz H erzeugen. □

Ergänzung 7.3.13. Eine Untergruppe einer nicht abelschen endlich erzeugten Gruppe muß im allgemeinen keineswegs endlich erzeugt sein. Ein Beispiel geben wir in **??**.

Ergänzende Übung 7.3.14. Jede endlich erzeugte Untergruppe von $\mathbb{Q}$ ist zyklisch.

Ergänzende Übung 7.3.15. Man zeige, daß die additive Gruppe aller Gruppenhomomorphismen $\mathrm{Grp}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Q}/\mathbb{Z})$ unter punktweiser Addition isomorph ist zu $\mathbb{Z}/n\mathbb{Z}$, für alle $n \geq 1$.

7.3.16. Gibt es natürliche Zahlen $n \in \mathbb{N}$, die

bei Division durch 6 Rest 4 lassen,

bei Division durch 13 Rest 2, und

bei Division durch 11 Rest 9?

Da $\langle 6, 13\rangle = \langle 13, 11\rangle = \langle 6, 11\rangle = \langle 1\rangle$ lautet die Antwort ja, wie man aus dem anschließenden Korollar 7.3.19 folgert.

Satz 7.3.17. *Ist $m = ab$ ein Produkt von zwei zueinander teilerfremden positiven natürlichen Zahlen, so liefert die Abbildung $n \mapsto (n + a\mathbb{Z}, n + b\mathbb{Z})$ einen Isomorphismus*

$$\mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$$

7.3.18. Übung 7.4.15 zeigt, daß die fraglichen Gruppen im Fall nicht teilerfremder Faktoren auch nicht isomorph sind.

Beweis. Der Kern unserer Abbildung

$$\begin{array}{rccc} \varphi: & \mathbb{Z} & \to & \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ & n & \mapsto & (n + a\mathbb{Z}, n + b\mathbb{Z}) \end{array}$$

besteht aus allen $n \in \mathbb{Z}$, die durch a und b teilbar sind, also aus allen Vielfachen von m. Der Isomorphiesatz 7.2.12 liefert mithin einen Isomorphismus $\mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \operatorname{im}\varphi$, und daraus folgt hinwiederum $\operatorname{im}\varphi = \mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z}$, da unsere Untergruppe $\operatorname{im}\varphi$ selbst auch schon $m = ab$ Elemente hat. □

Korollar 7.3.19 (Chinesischer Restsatz). *Ist $m = q_1 \ldots q_s$ ein Produkt von paarweise teilerfremden ganzen Zahlen, so liefert die offensichtliche Abbildung einen Isomorphismus*

$$\mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/q_1\mathbb{Z} \times \ldots \times \mathbb{Z}/q_s\mathbb{Z}$$

Beweis. Das folgt induktiv aus dem in 7.3.17 behandelten Fall $s = 2$. Die Details mag der Leser als Übung selbst ausführen. □

Übung 7.3.20. Man gebe alle Zahlen an, die bei Division durch 6 Rest 4 lassen, bei Division durch 13 Rest 2, und bei Division durch 11 Rest 9. Hinweis: Der euklidische Algorithmus liefert schon mal Lösungen, wenn ein Rest 1 ist und die anderen Null.

Übung 7.3.21. Gibt es ein Vielfaches von 17, dessen letzte Ziffern 39 lauten?

7.3.22. Ich will versuchen, das sogenannte **RSA-Verfahren** nach Rivest, Shamir und Adleman zum öffentlichen Vereinbaren geheimer Schlüssel anhand des folgenden Schemas zu erklären.

Geheimbereich Alice	Öffentlicher Bereich	Geheimbereich Bob
Alice wählt zwei große Primzahlen p, q und berechnet deren Produkt $N = pq$. Sie findet $\varphi(N) = (p-1)(q-1)$ und wählt Zahlen $s, t \in \mathbb{N}$ mit $st \equiv 1 \pmod{\varphi(N)}$. Sie macht N und t öffentlich.		
	N, t	
		Bob wählt eine Zahl $k \in \mathbb{Z}/N\mathbb{Z}$, berechnet k^t, und macht es öffentlich.
	$k^t \in \mathbb{Z}/N\mathbb{Z}$	
Alice berechnet $(k^t)^s = k$.		

Die Restklasse $k \in \mathbb{Z}/N\mathbb{Z}$ ist dann der gemeinsame geheime Schlüssel. Die behauptete Gleichheit von Restklassen $(k^t)^s = k$ prüft man für prime Restklassen $k \in (\mathbb{Z}/N\mathbb{Z})^\times$ leicht durch $(k^t)^s = k^{st} = k^{1+a\varphi(N)} = k$ wo wir beim letzten Schritt die Euler'sche Kongruenz 7.3.9 angewandt haben. Ist unsere Restklasse k nicht prim, bleibt diese Identität aber gültig. Um das zu sehen, beachten wir den Ringisomorphismus

$$\mathbb{Z}/N\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$

In $\mathbb{Z}/p\mathbb{Z}$ haben wir ja $k^x = k$ wann immer gilt $x \equiv 1 \pmod{p-1}$. In $\mathbb{Z}/q\mathbb{Z}$ haben wir ebenso $k^x = k$ wann immer gilt $x \equiv 1 \pmod{q-1}$. Falls also beides gilt, und erst recht falls $x \equiv 1 \pmod{(p-1)(q-1)}$, gilt also $k^x = k$ in $\mathbb{Z}/N\mathbb{Z}$. Der Trick bei diesem Verfahren besteht darin, daß es sehr viel Rechenzeit braucht, eine große Zahl wie N zu faktorisieren. Es ist also möglich, N zu veröffentlichen und dennoch p, q geheim zu halten, die hinwiederum für die Berechnung von s

benötigt werden. Des weiteren braucht es sehr viel Rechenzeit, um aus k^t auf k zurückzuschließen, also eine "t-te Wurzel modulo N" zu finden.

Satz 7.3.23 (Struktur endlicher abelscher Gruppen). *1. Ist G eine endliche abelsche Gruppe und p eine Primzahl, so ist die Teilmenge $G(p)$ aller Elemente, deren Ordnung eine p-Potenz ist, eine Untergruppe von p-Potenzordnung.*

2. Ist G eine endliche abelsche Gruppe und sind $p_1, \ldots, p_r$ die paarweise verschiedenen Primzahlen, die in der Primfaktorzerlegung von $|G|$ mindestens einmal vorkommen, so liefert die Multiplikation einen Gruppenisomorphismus

$$G(p_1) \times \ldots \times G(p_r) \xrightarrow{\sim} G$$

7.3.24. Teilt eine Primzahl p die Ordnung einer endlichen abelschen Gruppe G, so gibt es insbesondere in G ein Element der Ordnung p : In der Tat ist dann $G(p)$ nicht trivial; es gibt darin also ein vom neutralen Element verschiedenes Element a; dessen Ordnung ist etwa p^r mit $r \geq 1$; und dann ist in additiver Notation $p^{r-1}a$ das gesuchte Element der Ordnung p. Dieselbe Aussage gilt auch für beliebige endliche Gruppen und heißt der "Satz von Cauchy" III.1.5.6, aber der Beweis ist dann schwieriger und baut im übrigen auf dieser Bemerkung auf.

Erster Beweis. Unser Satz wird auch unmittelbar aus dem Klassifikationssatz 7.4.3 folgen. Da der Beweis dieses Klassifikationssatzes sich jedoch etwas länger hinzieht, gebe ich noch ein unabhängiges Argument. □

Zweiter Beweis. Wir notieren G additiv. Seien $x_1, \ldots, x_r$ die Elemente von $G(p)$ und $q_1, \ldots, q_r$ ihre Ordnungen. Wir betrachten wir den Gruppenhomomorphismus

$$\varphi : \mathbb{Z}/q_1\mathbb{Z} \times \ldots \times \mathbb{Z}/q_r\mathbb{Z} \quad \to \quad G$$

mit $(a_1, \ldots, a_r) \mapsto a_1x_1 + \ldots a_rx_r$. Sein Bild umfaßt $G(p)$ und enthält nur Elemente, deren Ordnung eine p-Potenz ist. Folglich ist das Bild unseres Gruppenhomomorphismus genau $G(p)$ und damit ist Teil 1 gezeigt. In Teil 2 folgt die Injektivität nun aus 7.1.10 und die Surjektivität aus dem chinesischen Restsatz 7.3.19: Für jedes $g \in G$ ist nämlich sein Erzeugnis eine zyklische Gruppe, die gemäß dem chinesischen Restsatz dargestellt werden kann als ein Produkt zyklischer Gruppen von Primpotenzordnung. □

Ergänzende Übung 7.3.25. Gegeben x, y zwei Elemente endlicher Ordnung in einer abelschen Gruppe G teilt die Ordnung ihres Produkts das kleinste gemeinsame Vielfache ihrer Ordnungen, und sind die Ordnungen von x und y teilerfremd, so gilt sogar $\operatorname{ord}(xy) = (\operatorname{ord} x)(\operatorname{ord} y)$.

Ergänzende Übung 7.3.26. In jeder endlichen kommutativen Gruppe wird die maximal von einem Gruppenelement erreichte Ordnung geteilt von den Ordnungen aller Gruppenelemente. Hinweis: Bezeichnet $M \subset \mathbb{N}$ die Menge aller Ordnungen von Elementen unserer Gruppe, so enthält M mit jeder Zahl auch alle ihre Teiler. Weiter enthält M nach 7.3.25 mit je zwei teilerfremden Zahlen auch ihr Produkt.

Definition 7.3.27. Gegeben eine Gruppe G heißt die kleinste Zahl $e \geq 1$ mit $g^e = 1 \ \ \forall g \in G$ der **Exponent** unserer Gruppe. Gibt es kein solches e, so sagen wir, die Gruppe habe unendlichen Exponenten.

Satz 7.3.28 (Endliche Gruppen von Einheitswurzeln). *Jede endliche Untergruppe der multiplikativen Gruppe eines Körpers ist zyklisch.*

7.3.29. Die Elemente ζ endlicher Ordnung in der multiplikativen Gruppe eines Körpers sind per definitionem genau diejenigen Elemente, die eine Gleichung der Gestalt $\zeta^n = 1$ erfüllen. Man nennt sie deshalb auch die **Einheitswurzeln** des Körpers.

Beispiel 7.3.30. Um uns auf den gleich folgenden Beweis einzustimmen zeigen wir zunächst beispielhaft, daß jede 18-elementige Untergruppe der multiplikativen Gruppe eines Körpers zyklisch ist. Nach 7.4.2 muß unsere Gruppe ja isomorph sein zu genau einer der beiden Gruppen $\mathbb{Z}/18\mathbb{Z}$ oder $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Es gilt also nur, die zweite Möglichkeit auszuschließen. Im zweiten Fall gäbe es jedoch in unserer Gruppe 9 Elemente von durch drei teilbarer Ordnung, und das steht im Widerspruch dazu, daß das Polynom $X^3 - 1$ in unserem Körper höchstens drei Nullstellen haben kann.

Beweis. In jeder endlichen kommutativen Gruppe wird die maximale von einem Gruppenelement erreichte Ordnung n geteilt von den Ordnungen aller Gruppenelemente, zum Beispiel nach dem Klassifikationssatz 7.4.2 oder direkter nach Übung 7.3.26. Wäre eine endliche Untergruppe G der multiplikativen Gruppe eines Körpers nicht zyklisch, so gäbe es also $n < |G|$ mit $\zeta^n = 1 \ \forall \zeta \in G$ im Widerspruch dazu, daß das Polynom $X^n - 1$ in unserem Körper höchstens n Nullstellen haben kann. □

7.4 Endlich erzeugte abelsche Gruppen

7.4.1. Unter einer **Primzahlpotenz** oder kurz **Primpotenz** verstehen wir im folgenden eine natürliche Zahl der Gestalt $q = p^e$ für p prim und $e \geq 1$. Gegeben eine Primzahl p verstehen wir unter einer **p-Potenz** dahingegen eine natürliche Zahl der Gestalt $q = p^e$ für p prim und $e \geq 0$. Man möge mir nachsehen, daß in dieser Terminologie nicht alle p-Potenzen Primzahlpotenzen sind. Die beiden folgenden Sätze geben zwei **Klassifikationen der endlich erzeugten abelschen Gruppen**.

Satz 7.4.2 (Klassifikation durch endliche Teilerfolgen). *Gegeben eine endlich erzeugte abelsche Gruppe G gibt es genau ein $s \geq 0$ und ein s-Tupel von von 1 verschiedenen natürlichen Zahlen $(a_1, \ldots, a_s) \in \{0, 2, 3, \ldots\}^s$ mit $a_i | a_{i+1}$ für $1 \leq i < s$ derart, daß gilt*

$$G \cong \mathbb{Z}/a_1\mathbb{Z} \times \ldots \times \mathbb{Z}/a_s\mathbb{Z}$$

Satz 7.4.3 (Klassifikation durch Multimengen von Primpotenzen). *Gegeben eine endlich erzeugte abelsche Gruppe G gibt es Primzahlpotenzen $q_1, \ldots, q_t$ und eine natürliche Zahl $r \in \mathbb{N}$ mit*

$$G \cong \mathbb{Z}/q_1\mathbb{Z} \times \ldots \times \mathbb{Z}/q_t\mathbb{Z} \times \mathbb{Z}^r$$

Die Zahl r wird durch G eindeutig festgelegt und heißt der **Rang** *von G. Die Primzahlpotenzen q_τ sind eindeutig bis auf Reihenfolge.*

7.4.4. Ich erinnere daran, daß wir in I.2.2.34 eine Multimenge von Elementen einer Menge X erklärt hatten als eine Abbildung $X \to \mathbb{N}$. In diesem Sinne ist dann auch die Bezeichnung des Satzes zu verstehen.

7.4.5. Um von der Darstellung im ersten Klassifikationssatz zu der im Zweiten überzugehen, kann man sich auf den Fall endlicher Gruppen beschränken, indem man die Nullen an der Ende der Folge der a_i abschneidet, die eben für den Faktor $\mathbb{Z}^r$ verantwortlich sind. Die anderen a_i zerlegt man in ein Produkt von Primzahlpotenzen, und die zugehörigen Faktoren $\mathbb{Z}/a_i\mathbb{Z}$ zerfallen dann nach dem chinesischen Restsatz entsprechend in ein Produkt zyklischer Gruppen von Primzahlpotenzordnung. Um von der Darstellung im zweiten Klassifikationssatz zu der im Ersten überzugehen, kann man sich wieder auf den Fall endlicher Gruppen beschränken. Gegeben ein Produkt zyklischer Gruppen von Primzahlpotenzordnung betrachtet man zunächst von jeder dabei auftauchenden Primzahl die höchste jeweils vorkommende Potenz und multipliziert diese zusammen: Das gibt a_s. Dann streicht man alle "verbrauchten" Potenzen und macht genauso weiter.

Korollar 7.4.6. *Jede endliche abelsche Gruppe ist ein Produkt von zyklischen Gruppen von Primzahlpotenzordnung, und die dabei auftretenden Primzahlpotenzen und ihre Vielfachheiten sind wohlbestimmt bis auf Reihenfolge. In Formeln erhalten wir so eine Bijektion*

$$\begin{array}{ccc} \left\{ \begin{array}{c} \textit{Endliche Multimengen} \\ \textit{von Primzahlpotenzen} \end{array} \right\} & \xrightarrow{\sim} & \left\{ \begin{array}{c} \textit{Endliche abelsche Gruppen} \\ \textit{bis auf Isomorphismus} \end{array} \right\} \\ \{q_1, q_2, \ldots, q_t\} & \mapsto & \mathbb{Z}/q_1\mathbb{Z} \times \mathbb{Z}/q_2\mathbb{Z} \times \ldots \times \mathbb{Z}/q_t\mathbb{Z} \end{array}$$

7.4.7. Man beachte bei den vorhergehenden Sätzen, daß die Faktoren keineswegs eindeutig sind "als Untergruppen unserer abelschen Gruppe". Die Beweise werden uns bis zum Ende des Abschnitts beschäftigen. Eine erste wesentliche Zutat ist der gleich folgende Elementarteilersatz 7.4.11.

Beispiel 7.4.8. Die Gruppen $(\mathbb{Z}/9\mathbb{Z})^2 \times \mathbb{Z}/4\mathbb{Z}$ und $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ sind nicht isomorph, denn sie entsprechen den beiden unterschiedlichen Multimengen von Primzahlpotenzen $\{9, 9, 4\}$ und $\{3,\ 27, 4\}$ oder alternativ den unterschiedlichen "Teilerfolgen" $9|36$ und $3|108$. Man kann das aber auch ohne alle Theorie unschwer einsehen: Die zweite Gruppe enthält Elemente der Ordnung 27, die erste nicht. Der Beweis, daß die Gruppen in unseren Klassifikationen paarweise nicht isomorph sind, verfeinert diese Grundidee.

Ergänzung 7.4.9. Ein Element endlicher Ordnung in einer Gruppe heißt ein **Torsionselement**. Eine Gruppe, in der alle Elemente außer dem neutralen Element unendliche Ordnung haben, heißt **torsionsfrei**. Zum Beispiel sind die abelschen Gruppen $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ torsionsfrei. Jede endlich erzeugte torsionsfreie abelsche Gruppe ist nach unserer Klassifikation isomorph zu $\mathbb{Z}^r$ für geeignetes $r \in \mathbb{N}$.

Ergänzung 7.4.10. Die Menge aller Torsionselemente ist in jeder abelschen Gruppe eine Untergruppe. Das Produkt aller endlichen Faktoren in jeder unserer beiden Darstellungen ist also eine wohldefinierte Untergruppe. Genauer ist sogar das Produkt aller Faktoren in der zweiten Zerlegung, deren Ordnungen Potenzen einer festen Primzahl p sind, eine wohlbestimmte Untergruppe unserer endlich erzeugten abelschen Gruppe, nämlich die Untergruppe aller Elemente von p-Potenzordnung, vergleiche auch 7.3.23.

Satz 7.4.11 (**Elementarteilersatz**). *1. Gegeben eine nicht notwendig quadratische Matrix A mit ganzzahligen Einträgen gibt es stets quadratische ganzzahlig invertierbare Matrizen mit ganzzahligen Einträgen P und Q derart, daß $B = PAQ$ eine Matrix mit Nullen außerhalb der Diagonalen ist, in der die Diagonaleinträge weiter vorn jeweils die Diagonaleinträge weiter hinten teilen, in Formeln $i \neq j \Rightarrow B_{i,j} = 0$ und $B_{i,i}|B_{i+1,i+1}\ \forall i$.*

2. Wir können durch geeignete Wahl von P und Q sogar zusätzlich erreichen, daß alle Diagonaleinträge nichtnegativ sind, und unter dieser Zusatzannahme werden besagte Diagonaleinträge durch die Matrix A bereits eindeutig festgelegt.

7.4.12. Ich nenne die Multimenge der Diagonaleinträge von B die Multimenge der **Elementarteiler der Matrix** A. Den Beweis der analogen Aussage für Polynomringe dürfen Sie selbst als Übung 7.4.22 ausarbeiten. Eine gemeinsame Verallgemeinerung für sogenannte "Hauptidealringe" wird in IV.1.8.1 dargestellt.

SkriptenBilder/BildElT.png

Berechnung der Elementarteiler einer ganzzahligen Matrix durch ganzzahlige ganzzahlig invertierbare Zeilen- und Spaltenoperationen. Wir finden die Elementarteiler $2, 10, 0$ jeweils mit der Vielfachheit Eins.

Beweis. Wir beginnen mit dem Nachweis der Existenz. Ist A die Nullmatrix, so ist nichts mehr zu zeigen. Sonst finden wir P, Q invertierbar derart, daß PAQ oben links einen positiven Eintrag hat, und zwar den kleinstmöglichen unter allen PAQ mit positivem Eintrag dort. Dann teilt dieser Eintrag notwendig alle anderen Einträge der ersten Spalte, da wir sonst durch Zeilenoperationen, genauer durch Subtraktion eines Vielfachen der ersten Zeile von einer anderen Zeile, Multiplikation einer Zeile mit -1 und Vertauschung zweier Zeilen, einen noch kleineren positiven Eintrag oben links erzeugen könnten. Ebenso teilt unser Eintrag auch alle anderen Einträge in der ersten Zeile. Durch entsprechende Zeilen- und Spaltenoperationen können wir also zusätzlich die erste Zeile und Spalte bis auf den ersten Eintrag als genullt annehmen. Teilt nun unser positiver Eintrag oben links nicht alle anderen Einträge unserer Matrix, sagen wir nicht den Eintrag $a_{i,j}$ mit $i \neq 1 \neq j$, so könnten wir durch Addieren der ersten Zeile zur i-ten Zeile gefolgt von einer Subtraktion eines Vielfachen der ersten Spalte von von der j-ten Spalte einen noch kleineren positiven Eintrag an der Stelle (i, j) erzeugen, und ihn durch Zeilen- und Spaltenvertauschung in die linke obere Ecke bringen im Widerspruch zu unserer Annahme. Also teilt unser positiver Eintrag oben links alle anderen Einträge unserer Matrix und eine offensichtliche Induktion beendet den Beweis der Existenz. Um die Eindeutigkeit zu zeigen, betrachten wir für jedes r die sogenannten $(r\times r)$**-Minoren** unserer Matrix. Man versteht darunter die Determinanten aller derjenigen $(r \times r)$-Matrizen, die wir aus unserer Matrix durch das Streichen von Zeilen und Spalten erhalten können. Dann bemerken wir, daß sich für gegebenes $r \geq 1$ der größte gemeinsame Teiler G_r aller $(r \times r)$-Minoren unter Zeilen- und Spaltenoperationen nicht ändert. Folglich sind die $G_r = d_1 \ldots d_r$ wohlbestimmt durch A, und dasselbe gilt dann auch für die d_i. □

Beweis von 7.4.2. Wir notieren in diesem Beweis unsere abelsche Gruppe G additiv. Gegeben ein Erzeugendensystem $g_1, \ldots, g_n$ von G erklären wir durch die Vorschrift $(a_1, \ldots, a_n) \mapsto a_1 g_1 + \ldots + a_n g_n$ einen surjektiven Gruppenhomomorphismus

$$\mathbb{Z}^n \twoheadrightarrow G$$

Dessen Kern ist nach 7.3.12 eine endlich erzeugte abelsche Gruppe K, für die wir wieder einen surjektiven Gruppenhomomorphismus $\mathbb{Z}^m \twoheadrightarrow K$ finden können. Mit der Notation ψ für die Komposition $\mathbb{Z}^m \twoheadrightarrow K \hookrightarrow \mathbb{Z}^n$ erhalten wir also einen Isomorphismus abelschen Gruppen

$$\mathbb{Z}^n / \operatorname{im} \psi \cong G$$

Genau wie bei Vektorräumen überlegt man sich, daß die Gruppenhomomorphismen $\mathbb{Z}^m \to \mathbb{Z}^n$ genau die Multiplikationen von links mit ganzzahligen $(n \times m)$-Matrizen sind, falls Elemente aus $\mathbb{Z}^m$ bzw. $\mathbb{Z}^n$ als Spaltenvektoren aufgefaßt werden, vergleiche 7.2.17. Weiter überlegt man sich, daß auch in dieser Situation die

Verknüpfung von Homomorphismen der Multiplikation von Matrizen entspricht. Bezeichnet nun A die Matrix unserer Abbildung $\mathbb{Z}^m \to \mathbb{Z}^n$, und wählen wir P und Q wie im Elementarteilersatz, so ergibt sich ein kommutatives Diagramm von abelschen Gruppen

$$\begin{array}{ccc} \mathbb{Z}^m & \xrightarrow{A} & \mathbb{Z}^n \\ {\scriptstyle Q}\uparrow\wr & & \wr\downarrow{\scriptstyle P} \\ \mathbb{Z}^m & \xrightarrow{D} & \mathbb{Z}^n \end{array}$$

für eine nicht notwendig quadratische Diagonalmatrix D mit nichtnegativen Einträgen $d_1|d_2|\ldots|d_r$ für $r = \min(m,n)$. In anderen Worten bildet der Gruppenisomorphismus $P : \mathbb{Z}^n \xrightarrow{\sim} \mathbb{Z}^n$ in dieser Situation $\operatorname{im}\psi = \operatorname{im} A$ bijektiv auf $\operatorname{im} D$ ab und wir erhalten Isomorphismen

$$G \cong \mathbb{Z}^n/\operatorname{im}\psi = \mathbb{Z}^n/\operatorname{im} A \cong \mathbb{Z}^n/\operatorname{im} D$$

Für die Diagonalmatrix D mit Diagonaleinträgen d_i scheint mir aber nun klar zu sein, daß $\mathbb{Z}^n/(\operatorname{im} D)$ isomorph ist zu einem Produkt der Gruppen $\mathbb{Z}/d_i\mathbb{Z}$ mit soviel Kopien von $\mathbb{Z}$, wie es in unserer Matrix D mehr Spalten als Zeilen gibt, also mit $(n-r)$ Kopien von $\mathbb{Z}$. Formaler kann das auch mit 7.5.6 aus dem folgenden Abschnitt begründet werden. Lassen wir von unserer Folge $d_1|d_2|\ldots|d_r$ nun alle Einsen vorne weg und ergänzen am Ende $(n-r)$ Nullen, so erhalten wir eine Folge $a_1|\ldots|a_s$ wie im Satz 7.4.2 gefordert, und die Existenz dort ist gezeigt. Um die Eindeutigkeit zu zeigen bemerken wir, daß für jede endlich erzeugte abelsche Gruppe G und jede Primzahl p und alle $n \geq 1$ der Quotient $p^{n-1}G/p^nG$ nach 2.4.40 in eindeutiger Weise ein endlichdimensionaler Vektorraum über $\mathbb{F}_p$ ist. Wir notieren seine Dimension

$$D_p^n(G) := \dim_{\mathbb{F}_p}(p^{n-1}G/p^nG)$$

Alternativ mag man $D_p^n(G)$ auch als die eindeutig bestimmte natürliche Zahl $D \in \mathbb{N}$ mit $|p^{n-1}G/p^nG| = p^D$ charakterisieren. Man sieht nun leicht oder folgert formal mit 7.5.6 die Formel $D_p^n(G \times H) = D_p^n(G) + D_p^n(H)$ für je zwei endlich erzeugte abelsche Gruppen G und H. Für zyklische Gruppen $G \cong \mathbb{Z}/a\mathbb{Z}$ behaupten wir nun

$$D_p^n(\mathbb{Z}/a\mathbb{Z}) \quad = \quad \begin{cases} 1 & p^n \text{ teilt } a; \\ 0 & \text{sonst.} \end{cases}$$

In der Tat ist das klar für $a = p^m$, für a teilerfremd zu p ist es eh klar, und mit dem chinesischen Restsatz 7.3.17 folgt es im allgemeinen. Für eine Zerlegung $G \cong \mathbb{Z}/a_1\mathbb{Z} \times \ldots \times \mathbb{Z}/a_s\mathbb{Z}$ wie in 7.4.2 finden wir also

$$D_p^n(G) = |\{i \mid p^n \text{ teilt } a_i\}|$$

Die Zahl der Nullen unter unseren a_i wird damit für jedes p gegeben durch die Formel $|\{i \mid a_i = 0\}| = \lim_{n\to\infty} D_p^n(G)$, und welche Potenz von jeder Primzahl in jedem von Null verschiedenen a_i stecken muß, kann man offensichtlich auch an den Zahlen $D_p^n(G)$ ablesen. Folglich hängen die a_i nur von der Gruppe G und nicht von der gewählten Zerlegung ab. □

Beweis von 7.4.3. Die Existenz folgt aus 7.4.2 mit dem Chinesischen Restsatz 7.3.19. Die Eindeutigkeit erkennt man, indem man sich überlegt, daß verschiedene Folgen $a_1|a_2|\ldots|a_s$ auch zu verschiedenen Produkten wie in 7.4.3 führen. Genauer kann man a_1 beschreiben als das Produkt der jeweils höchsten Primzahlpotenzen für alle vorkommenden Primzahlen, a_2 als das Produkt der jeweils zweithöchsten und so weiter, bis am Ende die Zahl der Nullen gerade die Zahl der Faktoren $\mathbb{Z}$ in der Zerlegung 7.4.3 sein muß. Alternativ kann man die Eindeutigkeit auch mit den Methoden des vorhergehenden Beweises der Eindeutigkeit in 7.4.2 direkt zeigen: Für $G \cong \mathbb{Z}^r \times \mathbb{Z}/q_1\mathbb{Z} \times \ldots \times \mathbb{Z}/q_t\mathbb{Z}$ wie in 7.4.3 finden wir nämlich mit den Notationen von dort

$$D_p^n(G) = r + |\{i \mid p^n \text{ teilt } q_i\}|$$

Wenden wir diese Erkenntnis an auf alle Primzahlen p, so folgt die im Satz behauptete Eindeutigkeit ohne weitere Schwierigkeiten: Wir erhalten genauer für jede Primzahl p und jedes $n \geq 1$ die nur von unserer Gruppe abhängenden Darstellungen $|\{i \mid q_i = p^n\}| = D_p^n(G) - D_p^{n+1}(G)$ und $r = \lim_{n\to\infty} D_p^n(G)$ für die Zahl der zyklischen Faktoren von vorgegebener Primpotenzordnung und den Rang r des freien Anteils. □

Ergänzende Übung 7.4.13. Der Rang einer endlich erzeugten abelschen Gruppe kann beschrieben werden als die Dimension des $\mathbb{Q}$-Vektorraums $\mathrm{Grp}(G,\mathbb{Q})$ aller Gruppenhomomorphismen von G nach $\mathbb{Q}$, mit seiner Vektorraumstruktur als Teilraum des $\mathbb{Q}$-Vektorraums $\mathrm{Ens}(G,\mathbb{Q})$.

Ergänzende Übung 7.4.14. Man gebe ein dreielementiges bezüglich Inklusion minimales Erzeugendensystem der Gruppe $\mathbb{Z}$ an.

Ergänzende Übung 7.4.15. Gegeben $a, b \in \mathbb{N}_{\geq 1}$ gibt es einen Gruppenisomorphismus $\mathbb{Z}/ab\mathbb{Z} \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ genau dann, wenn a und b teilerfremd sind.

Ergänzende Übung 7.4.16. Man zeige, daß es für jede zyklische Gruppe G gerader Ordnung genau ein Element der Ordnung zwei und genau einen surjektiven Gruppenhomomorphismus in die zweielementige Gruppe gibt.

Ergänzende Übung 7.4.17. Man berechne die Elementarteiler der Matrix

$$\begin{pmatrix} 2 & 3 & 4 & 5 \\ 6 & 7 & 8 & 9 \\ 5 & 5 & 5 & 5 \end{pmatrix}$$

Ergänzende Übung 7.4.18. Man zeige, daß jede von Null verschiedene Zeilenmatrix als einzigen Elementarteiler den größten gemeinsamen Teiler der Matrixeinträge hat.

Ergänzung 7.4.19. Gegeben eine abelsche Gruppe M bilden die Elemente endlicher Ordnung stets eine Untergruppe $M_{\text{tor}} \subset M$ und der Quotient M/M_{tor} ist torsionsfrei. Allerdings gibt es im Gegensatz zum Fall endlich erzeugter abelscher Gruppen im allgemeinen keinen Gruppenisomorphismus zwischen M und $M_{\text{tor}} \times (M/M_{\text{tor}})$. Betrachten wir etwa in der Gruppe $M = \prod_{n=0}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$ das Element $v = (\overline{p^0}, 0, \overline{p^1}, 0, \overline{p^2}, 0, \ldots)$, so ist $\overline{v} \in M/M_{\text{tor}}$ nicht Null und für alle $i \geq 0$ gibt es $w = w_i \in M/M_{\text{tor}}$ mit $p^i w = v$. Das einzige Element von M, das in dieser Weise "durch alle p-Potenzen teilbar ist", ist jedoch die Null, folglich existiert kein Gruppenisomorphismus zwischen M und $M_{\text{tor}} \times (M/M_{\text{tor}})$. Dies Beispiel ist im übrigen eine Variation von 6.3.21.

Ergänzende Übung 7.4.20. Man finde ein Repräsentantensystem für die Bahnen unter der offensichtlichen Wirkung von $\mathrm{GL}(n;\mathbb{Z}) \times \mathrm{GL}(m;\mathbb{Z})$ auf dem Matrizenraum $\mathrm{M}(n \times m;\mathbb{Q})$. Hinweis: 7.4.11.

Ergänzende Übung 7.4.21. Sind $a, b \in \mathbb{Z}$ teilerfremd, in Formeln $\langle a, b\rangle = \langle 1\rangle$, so läßt sich das Element $(a, b) \in \mathbb{Z}^2$ ergänzen zu einem Erzeugendensystem von $\mathbb{Z}^2$. Man formuliere und zeige auch die analoge Aussage für $\mathbb{Z}^n$.

Ergänzende Übung 7.4.22 (**Smith-Zerlegung**). Gegeben eine nicht notwendig quadratische Matrix A mit Einträgen im Polynomring $k[X]$ mit Koeffizienten in einem Körper k zeige man: (1) Es gibt quadratische im Matrizenring über $k[X]$ invertierbare Matrizen mit polynomialen Einträgen P und Q derart, daß $B = PAQ$ eine Matrix mit Nullen außerhalb der Diagonalen ist, in der die Diagonaleinträge weiter vorn jeweils die Diagonaleinträge weiter hinten teilen, in Formeln $i \neq j \Rightarrow B_{i,j} = 0$ und $B_{i,i} | B_{i+1,i+1}\ \forall i$; (2) Wir können durch geeignete Wahl von P und Q sogar zusätzlich erreichen, daß alle von Null verschiedenen Diagonaleinträge normiert sind, und unter dieser Zusatzannahme werden besagte Diagonaleinträge durch die Matrix A bereits eindeutig festgelegt.

Ergänzung 7.4.23. Die Smith-Zerlegung aus der vorhergehenden Übung wird sich später als ein Spezialfall des Elementarteilersatzes für Hauptidealringe IV.1.8.1 erweisen. Dieser Satz wird sich als der Schlüssel zum vertieften Verständnis der Jordan'schen Normalform erweisen und liefert auch Verallgemeinerungen über nicht notwendig algebraisch abgeschlossenen Körpern.

Übung 7.4.24 (**Einheitengruppen von Restklassenringen**). Nach dem chinesischen Restsatz kennen wir die Einheitengruppen $(\mathbb{Z}/m\mathbb{Z})^\times$, sobald wir sie für jede Primzahlpotenz m kennen. In dieser Übung sollen sie zeigen:

$$(\mathbb{Z}/p^r\mathbb{Z})^\times \cong \begin{cases} \mathbb{Z}/p^{r-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} & p \text{ ist eine ungerade Primzahl, } r \geq 1; \\ \mathbb{Z}/2^{r-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & p = 2,\ r \geq 2. \end{cases}$$

Ein Erzeugendensystem von $\mathbb{Z}^2$

Man beachte, daß hier links die Multiplikation als Verknüpfung zu verstehen ist, rechts dahingegen die Addition. Hinweis: Nach 7.3.28 ist die Gruppe $(\mathbb{Z}/p\mathbb{Z})^\times$ stets zyklisch. Bei ungeradem p gehe man von der Abbildung $(\mathbb{Z}/p^r\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ aus und zeige, daß die Restklasse von $1+p$ den Kern erzeugt. Dazu beachte man, daß für alle $b \in \mathbb{Z}$ und $n \geq 1$ gilt $(1+p^n+bp^{n+1})^p \in 1+p^{n+1}+p^{n+2}\mathbb{Z}$. Dann beachte man, daß diese Formel unter der stärkeren Annahme $n \geq 2$ auch für $p=2$ gilt, und folgere, daß der Kern der Abbildung $(\mathbb{Z}/2^r\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/4\mathbb{Z})^\times$ für $r \geq 2$ von der Restklasse von 5 erzeugt wird.

Übung 7.4.25. Gibt es eine Potenz von 17, deren Dezimaldarstellung mit den Ziffern 37 endet?

Übung 7.4.26 (**Primitivwurzeln in Restklassenringen**). Man zeige, daß für $m \geq 2$ die Einheitengruppe $(\mathbb{Z}/m\mathbb{Z})^\times$ des Restklassenrings $\mathbb{Z}/m\mathbb{Z}$ zyklisch ist genau dann, wenn m eine Potenz einer ungeraden Primzahl oder das Doppelte einer Potenz einer ungeraden Primzahl oder Zwei oder Vier ist. Hinweis: Man beachte 7.4.24, den chinesischen Restsatz 7.3.17, und die Tatsache, daß eine zyklische Gruppe nie $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ als Quotienten haben kann. Ein Erzeuger der Einheitengruppe $(\mathbb{Z}/m\mathbb{Z})^\times$ heißt im übrigen auch eine **Primitivwurzel modulo** m und die vorhergehende Aussage darüber, modulo welcher natürlichen Zahlen m Primitivwurzeln existieren, wird als der **Satz von Euler** zitiert. Bis heute (2011) ungelöst ist die **Vermutung von Artin**, nach der die 2 modulo unendlich vieler Primzahlen eine Primitivwurzel sein sollte.

Ergänzende Übung 7.4.27. Eine Untergruppe eines endlichdimensionalen $\mathbb{Q}$-Vektorraums heißt ein $\mathbb{Z}$**-Gitter** genau dann, wenn sie von einer Basis unseres $\mathbb{Q}$-Vektorraums erzeugt wird. Man zeige: Eine endlich erzeugte Untergruppe eines endlichdimensionalen $\mathbb{Q}$-Vektorraums ist ein $\mathbb{Z}$-Gitter genau dann, wenn sie besagten Vektorraum als $\mathbb{Q}$-Vektorraum erzeugt. Ist $\Gamma \subset V$ ein $\mathbb{Z}$-Gitter eines endlichdimensionalen $\mathbb{Q}$-Vektorraums und $\varphi : V \twoheadrightarrow W$ eine surjektive lineare Abbildung, so ist $\varphi(\Gamma)$ ein $\mathbb{Z}$-Gitter in W. Ist $U \subset V$ ein Untervektorraum, so ist $U \cap \Gamma$ ein $\mathbb{Z}$-Gitter in U.

7.5 Exakte Sequenzen

7.5.1. Beim Arbeiten mit Restklassengruppen ermöglicht der Formalismus der "exakten Sequenzen" oft besonders transparente Formulierungen. Wir führen deshalb im folgenden auch diese Sprache ein und verwenden sie im folgenden Abschnitt bei der Klassifikation endlich erzeugter abelscher Gruppen. Mehr zu exakten Sequenzen wird in 9.2 erklärt.

Definition 7.5.2. 1. Eine Sequenz von Gruppen und Gruppenhomomorphismen $A' \xrightarrow{x} A \xrightarrow{y} A''$ heißt **exakt bei** A genau dann, wenn das Bild der

ersten Abbildung zusammenfällt mit dem Kern der zweiten Abbildung, in Formeln $\operatorname{im} x = \ker y$.

2. Eine Sequenz von Gruppen $\ldots \to A_{i+1} \to A_i \to A_{i-1} \to \ldots$ heißt **exakt** genau dann, wenn sie exakt ist an jeder Stelle A_i.

Beispiele 7.5.3. Eine Sequenz der Gestalt $A \xrightarrow{r} B \xrightarrow{s} 1$ ist exakt genau dann, wenn r surjektiv ist. Eine Sequenz der Gestalt $1 \xrightarrow{r} B \xrightarrow{s} C$ ist exakt genau dann, wenn s injektiv ist.

Beispiele 7.5.4. Für jeden Homomorphismus $x : M \to N$ von abelschen Gruppen ist die Sequenz

$$1 \to (\ker x) \to M \to N \to (N/\operatorname{im} x) \to 1$$

exakt. Man nennt wegen dieser Symmetrie den Quotienten nach dem Bild auch den **Kokern** unseres Morphismus von abelschen Gruppen und notiert ihn $\operatorname{cok} x := (N/\operatorname{im} x)$.

Proposition 7.5.5. *1. Gegeben ein kommutatives Diagramm von Gruppen mit exakten Zeilen*

$$\begin{array}{ccccccc} M' & \xrightarrow{x} & M & \xrightarrow{y} & M'' & \longrightarrow & 1 \\ \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \vdots{\scriptstyle f''} & & \| \\ N' & \xrightarrow{p} & N & \xrightarrow{q} & N'' & \longrightarrow & 1 \end{array}$$

ohne den gestrichelten Pfeil, in Formeln mit $pf' = fx$, existiert genau ein Gruppenhomomorphismus f'' wie durch den gestrichelten Pfeil angedeutet, der das mittlere Quadrat unseres Diagramms zum Kommutieren bringt in dem Sinne, daß gilt $qf = f''y$.

2. Sind f' und f Isomorphismen, so auch f''.

Beweis. Wir zeigen zunächst den zweiten Teil zusammen mit der Eindeutigkeit von f''. Wegen der Exaktheit der unteren Horizontale ist $q : N \to N''$ surjektiv. Ist f surjektiv, so ist $q \circ f = f'' \circ y$ surjektiv und folglich ist auch f'' surjektiv, und wegen der Surjektivität von y ist f'' auch eindeutig bestimmt. Die Injektivität von f'' ist etwas mühsamer zu zeigen. Sei $m'' \in M$ gegeben mit $f''(m'') = 1$. Wegen der Exaktheit der oberen Horizontale existiert $m \in M$ mit $y(m) = m''$. Für dies m gilt wegen der Kommutativität des zweiten Quadrats $qf(m) = f''y(m) = f''(m'') = 1$, also $f(m) \in \ker q$. Wegen der Exaktheit der unteren Horizontale gibt es also $n' \in N'$ mit $p(n') = f(m)$. Da nun nach Annahme f' surjektiv ist, gibt es $m' \in M'$ mit $f'(m') = n'$. Dann haben wir wegen der Kommutativität des linken Quadrats $fx(m') = pf'(m') = p(n') = f(m)$ und die Injektivität

von f liefert $x(m') = m$. Wegen der Exaktheit der oberen Horizontale liefert das jedoch hinwiederum $1 = yx(m') = y(m) = m''$ wie gewünscht. Um nun noch die Existenz im ersten Teil zu zeigen, betrachten wir das erweiterte Diagramm

$$\begin{array}{ccccccc}
M' & \xrightarrow{x} & M & \xrightarrow{y} & M'' & \longrightarrow & 1 \\
\| & & \| & & \uparrow{\scriptstyle g} & & \| \\
M' & \xrightarrow{x} & M & \xrightarrow{\mathrm{can}} & \operatorname{cok} x & \longrightarrow & 1 \\
\downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle h} & & \| \\
N' & \xrightarrow{p} & N & \xrightarrow{q} & N'' & \longrightarrow & 1
\end{array}$$

Wegen $yx = 1$ existiert nach der universellen Eigenschaft des Kokerns ein g mit $g \circ \mathrm{can} = y$, das also das obere mittlere Quadrat zum Kommutieren bringt. Wegen $qfx = f'pq = 1$ existiert nach der universellen Eigenschaft des Kokerns auch ein h mit $h \circ \mathrm{can} = q \circ f$, das also das untere mittlere Quadrat zum Kommutieren bringt. Nach dem bereits bewiesenen Teil ist g ein Isomorphismus. Mit $f'' = h \circ g^{-1}$ haben wir dann ein mögliches f'' gefunden. □

Übung 7.5.6. Gegeben zwei Sequenzen von Gruppen $A \xrightarrow{r} B \xrightarrow{s} C$ und $A' \xrightarrow{r'} B' \xrightarrow{s'} C'$ ist ihr **Produkt**

$$(A \times A') \xrightarrow{r \times r'} (B \times B') \xrightarrow{s \times s'} (C \times C')$$

exakt genau dann, wenn die beiden Ausgangssequenzen exakt sind. Analoges gilt sowohl für das Produkt als auch für die direkte Summe einer beliebigen Familie von Sequenzen von Gruppen. Diese Aussage bedeutet im Lichte von 7.5.5 insbesondere, daß das "Bilden von Produkten mit dem Bilden von Quotienten kommutiert".

8 Symmetrie

8.1 Gruppenwirkungen

Definition 8.1.1. Eine **Operation** oder **Wirkung** einer Gruppe G auf einer Menge X ist eine Abbildung

$$\begin{array}{ccc} G \times X & \to & X \\ (g,x) & \mapsto & gx \end{array}$$

derart, daß gilt $g(hx) = (gh)x$ für alle $g, h \in G$, $x \in X$ und $ex = x$ für das neutrale Element $e \in G$ und alle $x \in X$. Die erste Eigenschaft werde ich manchmal auch als die **Assoziativität** der Gruppenoperation ansprechen. Ich ziehe die Bezeichnung als Operation vor, da das Wort "Wirkung" in der Physik in einer anderen Bedeutung verwendet wird. Eine Menge mit einer Operation einer Gruppe G nennt man eine G-**Menge**. Die Aussage "X ist eine G-Menge" schreiben wir in Formeln

$$G \curvearrowright X$$

8.1.2. In derselben Weise erklärt man allgemeiner auch den Begriff der Operation eines Monoids auf einer Menge. Allerdings ist der Begriff in dieser Allgemeinheit wesentlich weniger nützlich, da viele der im folgenden bewiesenen Aussagen wie die Zerlegung in Bahnen 8.1.14 oder die Darstellung von Bahnen als Quotienten 8.2.1 in dieser Allgemeinheit nicht mehr gelten.

Beispiele 8.1.3.

1. Das Anwenden eines Isomorphismus definiert für jeden Vektorraum V eine Operation $\mathrm{GL}(V) \times V \to V$ von $\mathrm{GL}(V)$ auf V.

2. Jede Gruppe operiert vermittels ihrer Verknüpfung $G \times G \to G$ auf sich selbst.

3. Die symmetrische Gruppe $\mathcal{S}_n$ operiert in offensichtlicher Weise auf der Menge $\{1, 2, \ldots, n\}$.

4. Jede Gruppe G operiert auf jeder Menge X vermittels der **trivialen Operation** $gx = x \; \forall g \in G, x \in X$.

5. Ist G eine Gruppe und X eine G-Menge und $H \subset G$ eine Untergruppe, so ist X auch eine H-Menge in offensichtlicher Weise. Ist allgemeiner X eine G-Menge und $H \to G$ ein Gruppenhomomorphismus, so kann X in offensichtlicher Weise mit einer Operation von H versehen werden.

6. Ist X ein G-Menge, so ist auch die Potenzmenge $\mathcal{P}(X)$ eine G-Menge in natürlicher Weise.

Ergänzende Übung 8.1.4. Gegeben ein Monoid G und eine Menge X induziert unsere Bijektion $\mathrm{Ens}(G \times X, X) \xrightarrow{\sim} \mathrm{Ens}(G, \mathrm{Ens}(X, X))$ aus I.2.2.26 eine Bijektion

$$\left\{ \begin{array}{c} \text{Operationen des Monoids } G \\ \text{auf der Menge } X \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{c} \text{Monoidhomomorphismen} \\ G \to \mathrm{Ens}(X) \end{array} \right\}$$

Ist G eine Gruppe, so erhalten wir insbesondere eine Bijektion

$$\left\{ \begin{array}{c} \text{Operationen der Gruppe } G \\ \text{auf der Menge } X \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{c} \text{Gruppenhomomorphismen} \\ G \to \mathrm{Ens}^\times(X) \end{array} \right\}$$

In gewisser Weise ist also eine Operation einer Gruppe G auf einer Menge X "dasselbe" wie ein Gruppenhomomorphismus $G \to \mathrm{Ens}^\times(X)$.

8.1.5. Ist ganz allgemein $X \times Y \to Z$ eine Abbildung, etwa $(x, y) \mapsto x \top y$, und sind $A \subset X$ und $B \subset Y$ Teilmengen, so notieren wir $(A \top B) \subset Z$ die Teilmenge

$$(A \top B) = \{x \top y \mid x \in A,\ y \in B\}$$

Wir haben derartige Notationen auch bereits oft verwendet, zum Beispiel, wenn wir das Erzeugnis eines Vektors in einem reellen Vektorraum als $\langle v \rangle = \mathbb{R}v$ schreiben, oder wenn wir das Erzeugnis von zwei Teilräumen U, W eines Vektorraums V als $U + W$ schreiben.

Definition 8.1.6. Sei X eine Menge mit einer Operation einer Gruppe G, also eine G-Menge.

1. Die Menge aller **Fixpunkte von** G **in** X notiert man

   $$X^G = \{x \in X \mid gx = x\ \forall g \in G\}$$

   In vielen Situationen nennt man die Fixpunkte auch **Invarianten**.

2. Die **Standgruppe** oder **Isotropiegruppe** oder auch der **Fixator** oder **Stabilisator** eines Punktes $x \in X$ ist die Menge

   $$G_x = \{g \in G \mid gx = x\}$$

   Sie ist eine Untergruppe von G. Ist allgemeiner $A \subset X$ eine Teilmenge, so unterscheiden wir zwischen dem **Stabilisator** $\{g \in G \mid gA = A\}$ und dem **Fixator** $\{g \in G \mid gx = x\ \forall x \in A\}$. Beide sind Untergruppen von G. Den Stabilisator nennen wir insbeondere im Fall, daß A mehr als nur ein Element besitzt, auch die **Symmetriegruppe** von A. Natürlich kann der Stabilisator von $A \subset X$ auch beschrieben werden als die Isotropiegruppe des Punktes $A \in \mathcal{P}(X)$ für die auf $\mathcal{P}(X)$ induzierte Operation.

3. Eine G-Menge X heißt **frei** genau dann, wenn die Standgruppen aller ihrer Punkte trivial sind, in Formeln $(gx = x \text{ für ein } x \in X) \Rightarrow (g = e)$.

4. Für $A \subset X$, $H \subset G$ schreiben wir kurz HA für die Menge $HA = \{ha \mid h \in H, a \in A\}$. Für jede Teilmenge $A \subset X$ ist GA eine G-Menge in offensichtlicher Weise. Eine Teilmenge $Y \subset X$ heißt G**-stabil** genau dann, wenn gilt $GY = Y$, wenn also G der Stabilisator der Teilmenge Y ist.

5. Sei $x \in X$. Die Menge

$$Gx = \{gx \mid g \in G\} \subset X$$

heißt die **Bahn** (englisch und französisch **orbit**) von x.

6. Eine Operation heißt **transitiv** und X heißt ein **homogener Raum** für G genau dann, wenn es ein $x \in X$ gibt mit $X = Gx$.

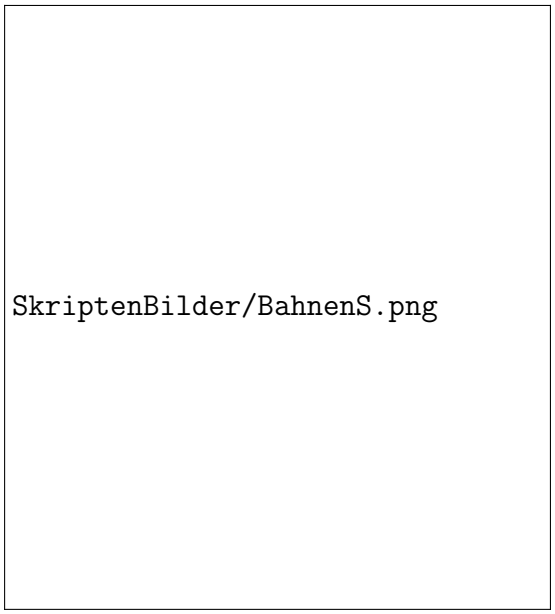
7. Eine Menge X mit einer freien transitiven Operation einer Gruppe G heißt ein **prinzipaler homogener Raum** für die Gruppe G oder auch kürzer ein G**-Torsor**.

8.1.7. Per definitionem sind die Rechtsnebenklassen von H in G genau die Bahnen der durch Multiplikation gegebenen Operation von H auf G. Insbesondere bilden sie also eine Partition von G. Analoges gilt für die Linksnebenklassen.

8.1.8. Ist G eine Gruppe und $H \subset G$ eine Untergruppe, so ist die Menge der Linksnebenklassen $X = G/H$ eine G-Menge in offensichtlicher Weise.

Ergänzende Übung 8.1.9. Genau dann stimmen für einen gegebenen homogenen Raum alle Isotropiegruppen überein, wenn er isomorph ist zum Quotienten der Gruppe nach einem Normalteiler. Wir sagen dann auch, der homogene Raum sei **normal**. Hinweis: 8.2.2. Ich finde diese Begriffsbildung ungeschickt: Normal zu sein ist für homogene Räume etwas ganz Besonderes, ebenso wie es leider für eine Untergruppe auch etwas ganz Besonderes ist, ein Normalteiler zu sein. Aber gut, vielleicht ist es ja bei Menschen auch so, daß normal zu sein etwas ganz Besonderes ist.

Beispiele 8.1.10. In jedem eindimensionalen Vektorraum über einem Körper k bilden die von Null verschiedenen Vektoren einen Torsor über der multiplikativen Gruppe $k^\times$ unseres Körpers. Jeder affine Raum ist ein Torsor über seinem Richtungsraum. Jede Menge mit genau zwei Elementen ist in natürlicher Weise ein $(\mathbb{Z}/2\mathbb{Z})$-Torsor. Jede Gruppe G kann in offensichtlicher Weise aufgefaßt werden als ein G-Torsor.



Einige Bahnen von S^1 auf $\mathbb{C}$

Einige Bahnen der Symmetriegruppe eines Quadrats

Bemerkung 8.1.11. Die Wirkung einer Gruppe auf der leeren Menge ist in unseren Konventionen nicht transitiv. Hier sind jedoch auch andere Konventionen gebräuchlich, zum Beispiel nennt Bourbaki die Wirkung einer Gruppe auf der leeren Menge durchaus transitiv. Noch mehr Terminologie zu Mengen mit Gruppenwirkung führen wir in **??** ein.

Übung 8.1.12. Ist E ein affiner Raum über einem Körper der Charakteristik Null und $G \subset \mathrm{Aff}^\times E$ eine endliche Untergruppe seiner Automorphismengruppe, so besitzt G stets einen Fixpunkt in E. Hinweis: Man betrachte den Schwerpunkt einer Bahn.

Ergänzung 8.1.13. Es gibt auch eine Variante des Torsor-Begriffs, bei der man nicht auf eine vorgegebene Gruppe Bezug nimmt: In dieser Variante definiert man einen **Torsor** als eine Menge X mitsamt einer ausgezeichneten Untergruppe $G \subset \mathrm{Ens}^\times(X)$, die frei und transitiv auf X wirkt. Ordnet man jedem Paar $(x, y) \in X \times X$ das Element $g \in G$ zu mit $gx = y$, so erhält man daraus erst eine Abbildung $X \times X \to \mathrm{Ens}^\times(X)$ und dann mit I.2.2.26 weiter auch eine Abbildung $\varphi_G : X \times X \times X \to X$. Verschiedene frei und transitiv operierende Untergruppen $G \subset \mathrm{Ens}^\times(X)$ liefern nun offensichtlich verschiedene Abbildungen φ_G, so daß man zusammenfassend einen Torsor in diesem Sinne auch definieren kann als eine Menge X nebst einer Abbildung $\varphi : X \times X \times X \to X$ mit gewissen Eigenschaften, die ich hier nicht ausschreibe.

Lemma 8.1.14 (Zerlegung in Bahnen). *Gegeben eine Menge mit Gruppenoperation sind je zwei Bahnen entweder gleich oder disjunkt.*

8.1.15. Unter einer **Partition einer Menge** X versteht man ein System $\mathcal{U} \subset \mathcal{P}(X)$ von paarweise disjunkten nichtleeren Teilmengen, deren Vereinigung ganz X ist. In dieser Terminologie besagt unser Lemma also, daß die Bahnen unter der Operation einer Gruppe auf einer Menge eine Partition besagter Menge bilden.

8.1.16. Im Fall der Operation eines Monoids ist die analoge Aussage im allgemeinen nicht mehr richtig: Man betrachte für ein Gegenbeispiel etwa die Operation durch Addition des additiven Monoids $\mathbb{N}$ auf $\mathbb{Z}$.

Beweis. Sei $G \curvearrowright X$ unsere Menge mit Gruppenoperation. Wegen unserer Forderung $ex = x$ an eine Gruppenoperation liegt jedes $x \in X$ in einer G-Bahn, nämlich in der G-Bahn Gx. Andererseits folgt aus $Gx \cap Gy \neq \emptyset$ schon $Gx = Gy$: In der Tat liefert $gx = hy$ wegen $Gg = G$ unter Verwendung der Assoziativitätsbedingung an eine Gruppenoperation ja $Gx = Ggx = Ghy = Gy$. Die Bahnen sind also auch paarweise disjunkt. □

Definition 8.1.17. Gegeben eine Menge mit Gruppenoperation bezeichnet man das Mengensystem der Bahnen auch als den **Bahnenraum**. Ist $G \curvearrowright X$ unsere

Eine Partition einer Menge mit dreizehn Elementen durch vier Teilmengen.

Menge mit Gruppenoperation, so ist der Bahnenraum also die Teilmenge $\{Gx \mid x \in X\} \subset \mathcal{P}(X)$ der Potenzmenge von X. Man notiert den Bahnenraum meist $G\backslash X$ oder auch X/G. Wir haben eine kanonische Surjektion $\mathrm{can} : X \twoheadrightarrow G\backslash X$, $x \mapsto Gx$, die jedem Element von X seine Bahn zuordnet.

8.1.18. Beide Notationen für den Bahnenraum haben ihre Tücken: Die Notation $G\backslash X$ könnte auch die in I.2.1.11 eingeführte Differenzmenge bedeuten, die Notation X/G hinwiederum könnte auch für den Bahnenraum einer Rechtsoperation stehen, wie wir ihn gleich einführen werden. Was im Einzelfall gemeint ist, muß aus dem Kontext erschlossen werden.

Beispiel 8.1.19. Wir betrachten die Menge $X = \mathbb{C}$ der komplexen Zahlen mit der Operation von $G = S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ durch Multiplikation. Die Standgruppen sind $G_x = 1$ falls $x \neq 0$ und $G_0 = S^1$. Die Bahnen sind genau alle Kreise um den Nullpunkt mit Radius $r \geq 0$. Die Einbettung $\mathbb{R}_{\geq 0} \hookrightarrow \mathbb{C}$ induziert eine Bijektion mit dem Bahnenraum $\mathbb{R}_{\geq 0} \xrightarrow{\sim} (S^1\backslash\mathbb{C})$.

8.1.20 (**Universelle Eigenschaft des Bahnenraums**). Gegeben eine Menge mit Gruppenoperation $G \curvearrowright X$ und eine Abbildung in eine weitere Menge $\varphi : X \to Y$ mit der Eigenschaft $\varphi(gx) = \varphi(x)$ für alle $g \in G, x \in X$ existiert genau eine Abbildung $\tilde{\varphi} : G\backslash X \to Y$ mit $\tilde{\varphi} \circ \mathrm{can} = \varphi$, im Diagramm

$$\begin{array}{ccc} X & \xrightarrow{\mathrm{can}} & G\backslash X \\ & \searrow^{\varphi} & \downarrow{\scriptstyle \tilde{\varphi}} \\ & & Y \end{array}$$

In der Tat können und müssen wir $\tilde{\varphi}(Gx)$ als das einzige Element der Menge $\varphi(Gx)$ definieren. Man mag diese universelle Eigenschaft des Bahnenraums auch als einen Spezialfall der universellen Eigenschaft des Raums der Äquivalenzklassen einer Äquivalenzrelation im Sinne von 2.6.4 verstehen.

Definition 8.1.21. Sei X eine Menge und G eine Gruppe. Eine **Rechtsoperation** von G auf X ist eine Abbildung

$$\begin{array}{ccc} X \times G & \to & X \\ (x, g) & \mapsto & xg \end{array}$$

derart, daß $x(gh) = (xg)h$ für alle $g, h \in G$, $x \in X$, und daß gilt $xe = x$ für das neutrale Element $e \in G$ und alle $x \in X$. Eine Menge mit einer Rechtsoperation einer Gruppe G nennt man auch eine G-**Rechtsmenge**.

8.1.22. Jede G-Rechtsmenge X wird zu einer G-Menge durch die Operation $gx = xg^{-1}$, die Begriffsbildung einer G-Rechtsmenge ist also in gewisser Weise obsolet. Sie dient im wesentlichen dem Zweck, in manchen Situationen suggestivere Notationen zu ermöglichen. Unsere Begriffe für Linksoperationen wie

Bahn, Isotropiegruppe etc. verwenden wir analog auf für Rechtsoperationen. Den Bahnenraum notieren wir in diesem Fall stets X/G. Die kanonische Abbildung $X \twoheadrightarrow X/G$ hat dann offensichtlich eine zu 8.1.20 analoge universelle Eigenschaft.

8.1.23. Unter unserer Identifikation $\mathrm{Ens}(X \times G, X) \xrightarrow{\sim} \mathrm{Ens}(G, \mathrm{Ens}(X, X))$ aus I.2.2.26 entsprechen die Rechtsoperationen einer Gruppe G auf einer Menge X gerade den Gruppenhomomorphismen $G^{\mathrm{opp}} \to \mathrm{Ens}^{\times}(X)$. Hierbei meint G^{opp} die **opponierte Gruppe**, die entsteht, indem wir die Menge G mit der **opponierten Verknüpfung** $g * h = hg$ versehen. Im übrigen liefert das Bilden des Inversen stets einen Gruppenisomorphismus $G \xrightarrow{\sim} G^{\mathrm{opp}}$.

Ergänzung 8.1.24. Sei G eine Gruppe. Eine freie transitive G-Rechtsmenge nennen wir einen G-**Rechtstorsor** oder auch kurz einen G-**Torsor** in der Hoffnung, daß der Leser aus dem Kontext erschließen kann, ob im jeweils vorliegenden Fall eine Menge mit freier und transitiver Rechts- oder mit freier und transitiver Linksoperation gemeint ist.

Ergänzende Übung 8.1.25. Sei k ein Körper. Man zeige, daß wir eine Operation der Gruppe $\mathrm{GL}(n;k) \times \mathrm{GL}(m;k)$ auf der Menge $\mathrm{M}(n \times m; k)$ erhalten durch die Vorschrift $(A, B)M = AMB^{-1}$. Man zeige weiter, daß die Bahnen unserer Operation genau die nichtleeren Fasern der durch den Rang gegebenen Abbildung $\mathrm{rk} : \mathrm{M}(n \times m; k) \to \mathbb{N}$ sind. Hinweis: Smith-Normalform 1.10.11.

Ergänzende Übung 8.1.26. Sei k ein Körper. Man zeige, daß wir eine Operation der Gruppe $\mathrm{GL}(n;k)$ auf der Menge $\mathrm{M}(n \times n; k)$ erhalten durch die Vorschrift $A.M = AMA^{-1}$. Man zeige, wie für einen algebraisch abgeschlossenen Körper k die Theorie der Jordan'schen Normalform eine Bijektion liefert zwischen dem Bahnenraum zu dieser "Operation durch Konjugation" und der Menge aller endlichen Multimengen von Paaren aus $\mathbb{N}_{\geq 1} \times k$, deren erste Komponenten sich zu n aufaddieren.

Ergänzende Übung 8.1.27. Man gebe für jedes ungerade n einen Gruppenisomorphismus $\mathrm{SO}(n) \times \mathbb{Z}/2\mathbb{Z} \xrightarrow{\sim} \mathrm{O}(n)$ an; Man zeige, daß es für gerades n keinen derartigen Isomorphismus gibt.

8.2 Bahnformel

Lemma 8.2.1 (Bahnen als Quotienten). *Sei G eine Gruppe, X eine G-Menge und $x \in X$ ein Punkt. So induziert die Abbildung $G \to X$, $g \mapsto gx$ eine Bijektion*

$$G/G_x \xrightarrow{\sim} Gx$$

Beweis. Für jede G_x-Linksnebenklasse $L \subset G$ im Sinne von 7.1.2 besteht die Menge Lx nur aus einem Punkt, für $L = gG_x$ haben wir genauer $Lx = gG_xx = \{gx\}$. Die Abbildung im Lemma wird nun definiert durch die Bedingung, daß

sie jeder Nebenklasse $L \in G/G_x$ das einzige Element von Lx zuordnet. Diese Abbildung ist offensichtlich surjektiv. Sie ist aber auch injektiv, denn aus $gG_xx = hG_xx$ folgt $gx = hx$, also $h^{-1}g \in G_x$, also $gG_x = hG_x$. □

8.2.2. Ist G eine endliche Gruppe und X eine G-Menge, so folgt mit dem vorhergehenden Lemma 8.2.1 aus dem Satz von Lagrange 7.1.5 für alle $x \in X$ insbesondere die sogenannte **Bahnformel**

$$|G| = |G_x| \cdot |Gx|$$

Die Kardinalität jeder Bahn teilt also die Kardinalität der ganzen Gruppe, und die Kardinalität der Isotropiegruppen ist konstant auf den Bahnen. Genauer prüft man für beliebiges G die Formel $G_{gx} = gG_xg^{-1}$ für $g \in G$, $x \in X$. Ist weiter X endlich und $X = X_1 \sqcup \ldots \sqcup X_n$ seine Zerlegung in Bahnen und $x(i) \in X_i$ jeweils ein Element, so folgt

$$|X| = |X_1| + \ldots + |X_n| = |G|/|G_{x(1)}| + \ldots + |G|/|G_{x(n)}|$$

Beispiel 8.2.3. Seien $k \leq n$ natürliche Zahlen. Auf der Menge X aller k-elementigen Teilmengen der Menge $\{1, 2, \ldots, n\}$ operiert die symmetrische Gruppe $\mathcal{S}_n$ transitiv. Die Isotropiegruppe des Punktes $x \in X$, der durch die k-elementige Teilmenge $\{1, 2, \ldots, k\}$ gegeben wird, ist isomorph zu $\mathcal{S}_k \times \mathcal{S}_{n-k}$. Die Bahnformel liefert folglich $|X| = n!/(k!(n-k)!)$ in Übereinstimmung mit unseren Erkenntnissen aus I.1.1.18. Ähnlich kann man auch die in I.2.2.29 diskutierten Formeln für die Multinomialkoeffizienten herleiten.

Beispiel 8.2.4. Wir können unsere Bahnformel auch umgekehrt anwenden, wenn wir zum Beispiel die Drehungen zählen wollen, die einen Würfel in sich überführen. Die Gruppe G dieser Drehungen operiert sicher transitiv auf der Menge E der acht Ecken des Würfels und die Isotropiegruppe jeder Ecke p hat drei Elemente. Wir folgern $|G| = |G_p| \cdot |E| = 3 \cdot 8 = 24$.

Ergänzende Übung 8.2.5. Sind Q, H Untergruppen einer Gruppe G, so induziert die Einbettung $Q \hookrightarrow G$ eine Bijektion $Q/(Q \cap H) \xrightarrow{\sim} QH/H$. Gemeint ist auf der rechten Seite der Bahnenraum der Operation von rechts durch Multiplikation der Gruppe H auf der Teilmenge $QH \subset G$.

8.3 Konjugationsklassen

Definition 8.3.1. Ist G eine Gruppe und $x \in G$ ein Element, so ist die Abbildung

$$\begin{array}{rccc} (\operatorname{int} x): & G & \to & G \\ & g & \mapsto & xgx^{-1} \end{array}$$

ein Isomorphismus der Gruppe G mit sich selber. Er heißt die **Konjugation mit** x. Ganz allgemein nennt man einen Isomorphismus einer Gruppe mit sich selber auch einen **Automorphismus** der Gruppe. Die Automorphismen einer Gruppe G bilden selber eine Gruppe mit der Verknüpfung von Abbildungen als Verknüpfung. Sie heißt die **Automorphismengruppe** von G und wir notieren sie $\mathrm{Grp}^\times(G)$. Diejenigen Automorphismen einer Gruppe, die sich als Konjugation mit einem geeigneten Gruppenelement schreiben lassen, heißen **innere Automorphismen** und auf englisch **interior automorphisms**, daher die Notation int. Sicher gilt $(\mathrm{int}\, x) \circ (\mathrm{int}\, y) = \mathrm{int}(xy)$, folglich ist $x \mapsto \mathrm{int}\, x$ ein Gruppenhomomorphismus $\mathrm{int} : G \to \mathrm{Grp}^\times(G)$ und insbesondere eine Operation der Gruppe G auf der Menge G, die **Operation durch Konjugation**

$$\begin{array}{ccc} G \times G & \to & G \\ (x, y) & \mapsto & (\mathrm{int}\, x)(y) = xyx^{-1} \end{array}$$

Die Bahnen unter dieser Operation heißen die **Konjugationsklassen** unserer Gruppe.

Beispiele 8.3.2. Die Konjugationsklassen in einer kommutativen Gruppe sind einelementig. Die Theorie der Jordan'schen Normalform beschreibt die Konjugationsklassen in $\mathrm{GL}(n;\mathbb{C})$, vergleiche 8.1.26.

Ergänzende Übung 8.3.3. Sei A eine zyklische Gruppe der Ordnung $n \in \mathbb{N}$. So gibt es genau einen Ringisomorphismus $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathrm{End}\, A$, und dieser Ringisomorphismus induziert einen Isomorphismus zwischen der Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^\times$ und der Automorphismengruppe von A.

Ergänzende Übung 8.3.4. Man gebe jeweils ein Repräsentantensystem an für die Konjugationsklassen der Gruppe der Isometrien der affinen euklidischen Ebene $\mathbb{R}^2$ und der Untergruppe ihrer orientierungserhaltenden Isometrien. Hinweis: 4.4.13.

8.4 Endliche Untergruppen der Drehgruppe

Satz 8.4.1 (Klassifikation der endlichen Bewegungsgruppen). *Jede endliche Untergruppe der Bewegungsgruppe des Anschauungsraums ist genau eine der folgenden Gruppen:*

1. *Eine* **zyklische Gruppe** C_k *mit* $k \geq 1$ *Elementen, bestehend aus allen Drehungen zu einer festen Drehachse um Winkel der Gestalt* $2\pi n/k$. *Der Fall* $k = 1$ *deckt hier den Fall der trivialen Gruppe ab, die nur aus der Identität besteht.*

2. *Eine* **Diedergruppe** D_k *mit* $2k$ *Elementen für* $k \geq 2$. *Im Fall* $k > 2$ *ist das die Gruppe aller Drehsymmetrien eines ebenen gleichseitigen* k*-Ecks, aufgefaßt als räumliche Figur. Im Fall* $k = 2$ *ist es die Gruppe aller derjenigen Drehungen, die von einem Paar orthogonaler Geraden jede in sich überführen.*

3. *Eine* **Tetraedergruppe** T *aller 12 Drehsymmetrien eines Tetraeders.*

4. *Eine* **Würfelgruppe** W *aller 24 Drehsymmetrien eines Würfels.*

5. *Eine* **Ikosaedergruppe** I *aller 60 Drehsymmetrien eines Ikosaeders.*

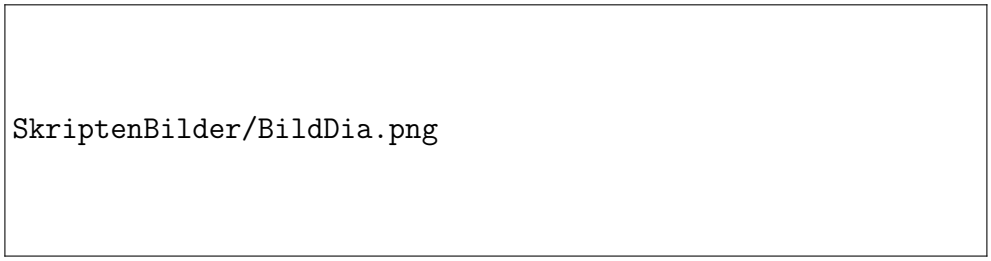
Bemerkung 8.4.2. Will man diesen Satz einem Laien erklären, der mit dem Gruppenbegriff nicht vertraut ist, so mag man nach 2.2.4 auch einfacher von endlichen Mengen von Drehungen reden, die mit je zwei Drehungen stets auch deren Hintereinanderausführung enthalten. Vom mathematischen Standpunkt aus mag man das Resultat als eine Klassifikation aller Konjugationsklassen von endlichen Untergruppen der Drehgruppe ansehen.

Bemerkung 8.4.3. Das Evozieren der platonischen Körper stellt insofern einen Stilbruch dar, als wir uns zumindest implizit darauf verständigt hatten, alle unsere Überlegungen ausschließlich im Rahmen der Mengenlehre durchzuführen. Ein möglicher **Würfel** ist schnell beschrieben, man mag als Ecken für irgendeine Orthonormalbasis $(\vec{v}_1, \vec{v}_2, \vec{v}_3)$ die acht Vektoren $\pm\vec{v}_1 \pm \vec{v}_2 \pm \vec{v}_3$ nehmen, im $\mathbb{R}^3$ also etwa $(\pm 1, \pm 1, \pm 1)$. Die Ecken eines **Tetraeders** erhält man, wenn man nur die vier Ecken dieses Würfels nimmt, bei denen das Produkt der Koordinaten Eins ist. Den **Ikosaeder** besprechen wir in 8.4.13 noch ausführlich. Zu den fünf sogenannten "platonischen Körpern" rechnet man außer diesen dreien noch den **Oktaeder** und den **Dodekaeder**. Die Eckenmenge eines Oktaeders bilden etwa die drei Vektoren der Standardbasis des $\mathbb{R}^3$ mitsamt ihren Negativen. Die Eckenmenge eines Dodekaeders mag man anschaulich als die Menge der "Flächenmitten eines Ikosaeders" beschreiben und formal als die Menge der "Pole der Polordnung drei" im Sinne des gleich folgenden Beweises im Fall der Symmetriegruppe eines Ikosaeders. Die Bezeichnungen Tetraeder, Oktaeder, Dodekaeder und Ikosaeder für die platonischen Körper außer dem Würfel kommen von den griechischen Worten für die Anzahlen 4, 8, 12 und 20 ihrer Flächen her. Man findet für den Würfel wegen seiner 6 Flächen manchmal auch die Bezeichnung "Hexaeder".

Ergänzung 8.4.4. Unser Satz 8.4.1 ist ein möglicher Ausgangspunkt der Kristallographie: Unter einem **n-dimensionalen Kristall** verstehen wir hier eine Teilmenge K eines n-dimensionalen affinen reellen euklidischen Raums E, etwa die Menge der Orte der Atome eines Kristallgitters, mit der Eigenschaft, daß (1) die Translationen aus ihrer Symmetriegruppe den Richtungsraum aufspannen und

daß es (2) eine positive untere Schranke gibt für die Längen aller von Null verschiedenen Translationen aus besagter Symmetriegruppe. Die zweite Eigenschaft schließt etwa den Fall aus, daß unsere Teilmenge einfach der ganze besagte euklidische Raum ist. Unter der **Punktgruppe** P eines Kristalls verstehen wir die Untergruppe $P \subset \mathrm{O}(\vec{E})$ aller linearen Anteile von Symmetrien unseres Kristalls, unter seiner **Drehgruppe** $D \subset \mathrm{SO}(\vec{E})$ die Menge aller orientierungserhaltenden Elemente der Punktgruppe. Man zeigt, daß die Punktgruppe eines Kristalls stets endlich sein muß, und daß als Drehgruppen von räumlichen, als da heißt dreidimensionalen Kristallen nur die Gruppen C_k und D_k mit $k \in \{1, 2, 3, 4, 6\}$ sowie die Tetraedergruppe und die Würfelgruppe auftreten können. Die Einteilung nach Drehgruppen entspricht in etwa, aber leider nicht ganz, der in der Kristallographie gebräuchlichen Einteilung in die sieben **Kristallsysteme**. Genauer entsprechen dem "kubischen System" die Würfelgruppe und die Tetraedergruppe, dem "tetragonalen System" die Drehgruppen C_4 und D_4, dem "hexagonalen System" die Drehgruppen C_6 und D_6, dem "trigonalen System" die Drehgruppen C_3 und D_3, aber das "orthorhombische", "monokline" und "trikline System" lassen sich erst anhand ihrer Punktgruppen unterscheiden. Auch in den übrigen Fällen liefert die Punktgruppe eine feinere Klassifikation, für sie gibt es 32 Möglichkeiten, nach denen die Kristalle in die sogenannten **Kristallklassen** eingeteilt werden. Die eigentliche Klassifikation beschreibt alle als Symmetriegruppen von räumlichen Kristallen möglichen Bewegungsgruppen des Anschauungsraums bis auf Konjugation mit affinen, nicht notwendig euklidischen Automorphismen. Es gibt hierfür 230 Möglichkeiten. Das **achtzehnte Hilbert'sche Problem** fragte unter anderem danach, ob es analog in jeder Dimension nur endlich viele Möglichkeiten für wesentlich verschiedene Kristalle gibt. Bieberbach konnte dafür einen Beweis geben.

Ergänzende Übung 8.4.5 (**Kristallgitter des Diamants**). Seien $v_1, \ldots, v_4$ Richtungsvektoren des dreidimensionalen Anschauungsraums, die vom Schwerpunkt eines Tetraeders zu seinen vier Ecken zeigen. Wir betrachten alle Linearkombinationen $\sum_{i=1}^{4} n_i v_i$ mit $\sum_{i=1}^{4} n_i \in \{0, 1\}$ und behaupten, daß diese Linearkombinationen gerade die Punkte beschreiben, an denen in einem Diamant die Kohlenstoffatome sitzen. In der Tat sind unsere Linearkombinationen paarweise verschieden, die "einzige" Relation $v_1 + v_2 + v_3 + v_4 = 0$ unserer Vektoren führt aufgrund unserer Einschränkungen nicht zu Mehrdeutigkeiten, und unsere Linearkombinationen lassen sich auch beschreiben als die Elemente des von den Richtungsvektoren $v_1 - v_2, v_1 - v_3$ und $v_1 - v_4$ erzeugten Gitters mitsamt dem um v_1 verschobenen Gitter. Jeder Punkt hat vier nächste Nachbarn, der Nullpunkt etwa $v_1, \ldots, v_4$, und zu diesen ist er gebunden im Diamantkristall. Anschaulich mag man sich eine Lage von parallelen horizontalen Zick-Zack-Linien denken, die Zick-Zacks darin nach oben und unten, dann eine weitere horizontale Lage senkrecht dazu, bei denen



Versuch einer graphischen Darstellung der räumlichen Struktur des Diamantkristalls. Die durchgezogenen und gestrichelten Linien sind nur der Transparenz halber verschiedenartig gezeichnet und bedeuten die Bindungen zwischen den Kohlenstoffatomen, die jeweils an den Ecken der Zick-Zack-Linien sitzen. Die hier gezeichnete Struktur gilt es nun übereinanderzuschichten, so daß sich jeweils die Ecken treffen.

die Tiefpunkte immer gerade die Hochpunkte der Lage darunter berühren, und so weiter, und schließlich an jedem dieser Berührungspunkte ein Kohlenstoffatom.

Ergänzung 8.4.6. Eine Würfelgruppe kann auch als die Gruppe aller Drehsymmetrien desjenigen Oktaeders aufgefaßt werden, dessen Ecken die Mittelpunkte der Flächen des Würfels sind. Ähnlich kann eine Ikosaedergruppe auch als Gruppe aller Drehsymmetrien eines Dodekaeders aufgefaßt werden. Die Kantenmitten eines Tetraeders bilden die Ecken eines Oktaeders, so erhält man eine Einbettung der Tetraedergruppe in die Würfelgruppe.

Ergänzung 8.4.7. Die Diedergruppe D_2 ist isomorph zur Klein'schen Vierergruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Sie kann vielleicht übersichtlicher auch beschrieben werden als die Gruppe aller Drehungen, die von einem Tripel paarweise orthogonaler Geraden jede in sich überführen. Neben der Identität liegen darin also die Drehungen um $180°$ um jede dieser drei Geraden. Die Tetraedergruppe kann man in die symmetrische Gruppe $\mathcal{S}_4$ einbetten vermittels ihrer Operation auf den Ecken des Tetraeders. Wir erhalten so einen Isomorphismus der Tetraedergruppe mit der alternierenden Gruppe A_4 aller geraden Permutationen von vier Elementen. Die Würfelgruppe operiert auf der Menge der vier räumlichen Diagonalen des Würfels und wir erhalten so einen Isomorphismus $W \cong \mathcal{S}_4$. Die Ikosaedergruppe operiert auf der Menge der fünf eingeschriebenen Würfel eines Dodekaeders, von denen einer in nebenstehendem Bild schematisch dargestellt ist. Mit etwas Geduld kann man direkt einsehen, daß diese Operation einen Isomorphismus der Ikosaedergruppe I mit der alternierenden Gruppe A_5 aller geraden Permutationen von 5 Elementen liefert. In III.1.2.5 werden wir erklären, wie man das auch mit weniger Geduld aber mehr Gruppentheorie einsehen kann, und in III.1.6.9 werden wir zusätzlich einen Isomorphismus dieser Gruppe mit der Gruppe $\mathrm{SL}(2;\mathbb{F}_5)/\{\pm \mathrm{id}\}$ herleiten.

Ergänzende Übung 8.4.8. Man konstruiere einen surjektiven Gruppenhomomorphismus $\mathcal{S}_4 \twoheadrightarrow \mathcal{S}_3$. Hinweis: Geometrisch mag man sich die $\mathcal{S}_4$ nach 8.4.7 als die Gruppe der Drehsymmetrien eines Würfels denken und den fraglichen Gruppenhomomorphismus konstruieren vermittels der Operation dieser Gruppe auf der Menge der drei Mittelsenkrechten auf den Flächen des Würfels.

Beweis von Satz 8.4.1. Sei $G \subset \mathrm{SO}(3)$ eine endliche Untergruppe. Für jedes vom neutralen Element verschiedene Element $g \in G\backslash 1$ unserer Gruppe definieren wir seine "Pole" als die beiden Schnittpunkte seiner Drehachse mit der Einheitssphäre. Sei P die Menge aller Pole von Elementen aus $G\backslash 1$. Natürlich ist P eine endliche Menge und G operiert auf P. Wir zählen nun die Menge M aller Paare (g, p) mit $g \in G\backslash 1$ und p einem Pol von g auf zwei Weisen: Einmal gehört jedes von 1 verschiedene Gruppenelement $g \in G\backslash 1$ zu genau zwei Polen, also haben wir $|M| = 2(|G| - 1)$. Andererseits gehört jeder Pol $p \in P$ mit Isotropiegruppe

Einer der fünf eingeschriebenen Würfel eines Dodekaeders, mit gestrichelt eingezeichneten Kanten.

G_p zu genau $|G_p| - 1$ von 1 verschiedenen Gruppenelementen, also haben wir $|M| = \sum_{p \in P}(|G_p| - 1)$. Zusammen erhalten wir

$$2(|G| - 1) = \sum_{p \in P}(|G_p| - 1)$$

Sei nun $P = P_1 \cup \ldots \cup P_r$ die Bahnzerlegung von P und seien $p_i \in P_i$ fest gewählt. Die Isotropiegruppe von p_i habe sagen wir $n_i \geq 2$ Elemente. Die zugehörige Bahn hat dann $|P_i| = |G|/n_i$ Elemente und alle Isotropiegruppen zu Polen aus P_i haben n_i Elemente. Die Kardinalität der Isotropiegruppe eines Pols nennen wir auch kürzer die **Polordnung**. In dieser Terminologie ist also n_i die Polordnung des Pols p_i. Fassen wir dann die Pole jeder Bahn in unserer Summe zu einem Summanden zusammen, so können wir in unserer Gleichung die rechte Seite umformen zu $\sum_{i=1}^{r}(|G|/n_i)(n_i - 1)$ und es ergibt sich die Gleichung

$$2 - \frac{2}{|G|} = \sum_{i=1}^{r}\left(1 - \frac{1}{n_i}\right)$$

Jeder Summand auf der rechten Seite ist mindestens 1/2, der Ausdruck links ist aber kleiner als 2. Es kommen also nur bis zu drei Bahnen von Polen in Betracht. Wir machen nun eine Fallunterscheidung nach der Zahl r der Bahnen von Polen.

Fall 0: Es gibt überhaupt keine Pole. In diesem Fall besteht G nur aus dem neutralen Element, und wir haben die Gruppe C_1 vor uns.

Fall 1: Ganz P ist eine Bahn. Das ist unmöglich, denn es muß gelten $|G| \geq 2$ wenn es überhaupt Pole geben soll, und damit hätten wir $2 - \frac{2}{|G|} \geq 1 > 1 - \frac{1}{n_1}$ im Widerspruch zu unserer Gleichung.

Fall 2: Es gibt genau zwei Bahnen P_1 und P_2 in P. Wir haben dann

$$\frac{2}{|G|} = \frac{1}{n_1} + \frac{1}{n_2}$$

Da n_1 und n_2 Teiler sind von $|G|$, haben wir $n_i \leq |G|$ und damit notwendig $n_1 = n_2 = |G|$. Alle Pole werden also von der Gruppe festgehalten, es gibt folglich nur zwei Pole, die sich notwendig gegenüberliegen müssen. Damit sind wir im Fall der zyklischen Gruppen C_k mit $k > 1$.

Fall 3: Es gibt genau drei Bahnen P_1, P_2 und P_3 in P, wir haben also

$$\frac{2}{|G|} = \frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} - 1$$

Wir dürfen annehmen $n_1 \leq n_2 \leq n_3$. Sicher gilt dann $n_1 = 2$, sonst wäre die rechte Seite ≤ 0. Haben wir auch $n_2 = 2$, so kann n_3 beliebige Werte annehmen und

Die “von vorne sichtbaren” Pole der Würfelgruppe mit den Kardinalitäten der jeweiligen Isotropiegruppen

wir haben $|G| = 2n_3$. Die Bahn P_3 besteht dann aus zwei Polen, die sich notwendig gegenüberliegen, und die von den Gruppenelementen zu den anderen Polen vertauscht werden. Die Gruppe wird damit eine Diedergruppe. Sicher sind $(2,4,4)$ und $(2,3,6)$ unmöglich für (n_1,n_2,n_3), da ja gilt $\frac{1}{2}+\frac{1}{4}+\frac{1}{4}-1 = 0 = \frac{1}{2}+\frac{1}{3}+\frac{1}{6}$, also bleiben nur die Fälle $(2,3,3)$, $(2,3,4)$ und $(2,3,5)$, und man berechnet leicht die zugehörigen Gruppenordnungen zu $12, 24,$ und 60.

Den Stand unseres Beweises bis hierher können wir wie folgt zusammenfassen: Wir haben eine Abbildung konstruiert—man mag sie die **Bahnpolordnungsabbildung** nennen—die jeder endlichen Untergruppe der Drehgruppe eine endliche Multimenge natürlicher Zahlen zuordnet, und haben gezeigt, daß in ihrem Bild höchstens die folgenden Multimengen liegen:

$$\emptyset, \{k,k\}_{k\geq 2}, \{2,2,k\}_{k\geq 2}, \{2,3,3\}, \{2,3,4\} \text{ und } \{2,3,5\}.$$

Wir müssen nun noch zeigen, daß (1) die angegebenen Multimengen genau das Bild unserer Bahnpolordnungsabbildung sind, und daß (2) je zwei Drehgruppen mit denselben Bahnpolordnungen zueinander konjugiert sind. Wenn wir das alles gezeigt haben, so folgt, daß die Bahnpolordungsabbildung eine Bijektion

$$\left\{ \begin{array}{c} \text{endliche Untergruppen} \\ \text{der Drehgruppe } \mathrm{SO}(3), \\ \text{bis auf Konjugation} \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{c} \emptyset, \{k,k\}_{k\geq 2}, \{2,2,k\}_{k\geq 2}, \\ \{2,3,3\}, \{2,3,4\}, \{2,3,5\} \end{array} \right\}$$

liefert, und zusammen mit der beim Beweis erzeugten Anschauung zeigt das unseren Satz. Die Existenz endlicher Untergruppen der Drehgruppe mit derartigen Polbahnen und Polordnungen scheint mir anschaulich klar. Zum Beispiel hat die Würfelgruppe drei Polbahnen, als da sind: Eine Bahn aus den 8 Ecken zur Polordnung 3; eine Bahn aus den auf Länge Eins normierten 12 Mittelpunkten der Kanten, zur Polordnung 2; und eine Bahn aus den auf Länge Eins normierten 6 Mittelpunkten der Flächen, zur Polordnung 4. Diese Anschauung läßt sich auch leicht zu einem formalen Beweis präzisieren in allen Fällen mit Ausnahme des Ikosaeder-Falls $(2,3,5)$. In diesem Fall folgt die Existenz formal erst aus 8.4.13. Daß je zwei zyklische Gruppen derselben endlichen Ordnung und je zwei Diedergruppen derselben endlichen Ordnung in der Drehgruppe zueinander konjugiert sind, scheint mir offensichtlich. Die folgenden beiden Lemmata 8.4.9 und 8.4.10 zeigen, daß auch je zwei Gruppen mit gegebenen Bahnpolordnungen oder, wie wir von jetzt an abkürzend sagen werden, zu gegebenem "Typ" $(2,3,n)$ in der Drehgruppe zueinander konjugiert sind. Damit vervollständigen sie den Beweis unseres Satzes. □

Lemma 8.4.9. *1. Jede endliche Untergruppe einer Drehgruppe von einem der beiden Typen $(2,3,4)$ oder $(2,3,5)$ ist maximal unter allen endlichen Untergruppen der Drehgruppe.*

2. *Eine endliche Drehgruppe von einem der Typen $(2,3,n)$ mit $n \geq 3$ kann beschrieben werden als die Symmetriegruppe jeder ihrer beiden kleineren Bahnen von Polen.*

Beweis. Nach unseren bisherigen Erkenntnissen kommen bei endlichen Drehgruppen für die Paare (Ordnung eines Pols, Kardinalität seiner Bahn) nur die Paare $(n,1)$, $(n,2)$, $(2,n)$, $(3,4)$, $(3,8)$, $(3,20)$, $(4,6)$ und $(5,12)$ in Frage. Für jeden Pol müssen sich bei Übergang zu einer echt größeren Gruppe nach der Bahnformel entweder seine Polordnung oder die Kardinalität seiner Bahn oder beide vervielfachen. Das ist aber bei $(4,6)$ und $(5,12)$ unmöglich und wir erhalten die erste Behauptung. In den drei Fällen der zweiten Behauptung enthält weiter jede Bahn von Polen mindestens drei Punkte, also auch zwei verschiedene nicht gegenüberliegende Punkte. Folglich operiert sogar die Symmetriegruppe der Bahn P_i treu auf P_i und ist insbesondere endlich. Nun muss P_i auch unter der fraglichen Symmetriegruppe eine Bahn von Polen sein. Wenn diese Symmetriegruppe größer sein will, muss sie also an diesen Polen größere Polordnungen haben. Wieder ist das unmöglich bei $(3,4)$, $(3,8)$, $(3,20)$, $(4,6)$ und $(5,12)$. □

Lemma 8.4.10. *Sind zwei endliche Drehgruppen vom selben Typ $(2,3,n)$ mit $n \geq 3$ gegeben und sind P_3 und $\tilde{P}_3$ jeweils zugehörige Polbahnen kleinstmöglicher Kardinalität, so gibt es eine Drehung, die P_3 in $\tilde{P}_3$ überführt.*

Beweis. Gegeben eine Bahn von Polen P_i betrachten wir ganz allgemein die Operation von G auf $P_i \times P_i$ und beachten, daß aus geometrischen Gründen die Isotropiegruppe eines Paars (p,q) mit $p \neq \pm q$ trivial sein muß. Nach dieser Vorüberlegung betrachten wir die drei Fälle der Reihe nach.

Im Fall $(2,3,3)$ haben wir $|P_3| = 4$ und $|P_3 \times P_3| = 16$. Folglich gibt es in $P_3 \times P_3$ ein Paar mit trivialer Isotropiegruppe, das also eine 12-elementige Bahn hat, die notwendig aus allen (p,q) mit $p \neq q$ bestehen muß. Je zwei verschiedene Punkte aus P_3 haben also denselben Abstand. Ich hoffe, daß damit sowohl die Aussage des Lemmas im Fall $n = 3$ klar wird als auch, daß die Punkte aus P_3 die Ecken eines Tetraeders bilden.

Im Fall $(2,3,4)$ haben wir $|P_3| = 6$ und $|P_3 \times P_3| = 36$. Folglich gibt es in $P_3 \times P_3$ ein Paar mit trivialer Isotropiegruppe, das also eine 24-elementige Bahn hat, die notwendig aus allen (p,q) mit $p \neq \pm q$ bestehen muß. Die anderen Bahnen müssen aus Paaren mit nichttrivialer Isotropiegruppe bestehen, und da die Bahn der sechs Paare der Gestalt (p,p) noch nicht genug Elemente liefert, muß auch noch eine Bahn von der Gestalt $(p,-p)$ vorkommen. Wir sehen so einerseits, daß P_3 stabil ist unter Punktspiegelung am Ursprung, und andererseits, daß je zwei voneinander verschiedene Pole aus P_3, die sich nicht gegenüberliegen, denselben Abstand haben. So erkennen wir hoffentlich sowohl die Aussage des Lemmas im

Fall $n = 4$ als auch, daß die Elemente von P_3 die Ecken eines Oktaeders bilden müssen.

Im Fall $(2, 3, 5)$ haben wir $|P_3| = 12$ und $|P_3 \times P_3| = 144$. Wieder haben wir an Bahnen in $|P_3 \times P_3|$ die zwölfelementige Bahn aller Paare (p, p), möglicherweise eine eine zwölfelementige Bahn aller Paare $(p, -p)$, und daneben nur Bahnen mit 60 Elementen. Es folgt, daß $P_3 \times P_3$ in vier Bahnen zerfällt, und zwar die Bahn der Paare gleicher Pole, die Bahn der Paare von sich gegenüberliegenden Polen, und zwei weitere Bahnen von Polpaaren. Nehmen wir irgendeinen Pol $p \in P_3$, so bilden die Bilder von jedem Pol $q \in P_3$ mit $q \neq \pm p$ unter den Drehungen aus unserer Gruppe mit Fixpunkt p ein regelmäßiges Fünfeck, und für zwei verschiedene Ecken eines Fünfecks gibt es zwei Möglichkeiten für ihren Abstand, deren Verhältnis übrigends nach **??** oder elementargeometrischen Überlegungen gerade der goldene Schnitt ist. Unsere beiden 60-elementigen Bahnen müssen sich also im Abstand zwischen den Polen eines Paars unterscheiden. Zu jedem Pol aus P_3 gibt es damit außer dem Pol selbst und dem gegenüberliegenden Pol noch 5 "nahe" Pole und 5 "weite" Pole. Nun bilden zwei sich gegenüberliegende Pole aus P_3 mit jedem weiteren Pol ein Dreieck, das nach dem Satz des Thales bei diesem weiteren Pol einen rechten Winkel hat, wobei dieser Pol notwendig zu einem von unseren beiden sich gegenüberliegenden Polen nah sein muß und zum anderen weit, da ja zu jedem unserer sich gegenüberliegenden Pole von den zehn verbleibenden Polen fünf nah und fünf weit sein müssen. Da unser Dreieck eine Hypotenuse der Länge 2 hat, wird dadurch der Abstand zwischen nahen Polen und der zwischen weiten Polen bereits vollständig beschrieben und hängt insbesondere nicht von unserer Gruppe ab. Damit erkennen wir, daß im Fall $(2, 3, 5)$ die Bahn P_3 bestehen muß aus (1) zwei gegenüberliegenden Punkten N und $S = -N$ sowie (2) zwei regelmäßigen Fünfecken der fünf zu N nahen Pole und der fünf zu S nahen Pole mit jeweils von der speziellen Gruppe unabhängigem Abstand der Ecken dieser Fünfecke zu den jeweiligen Polen. Jede Ecke des "nördlichen" Fünfecks muß aber auch einer Ecke des "südlichen" Fünfecks gegenüberliegen. Unser Lemma folgt unmittelbar. □

Ergänzende Übung 8.4.11. Die Multiplikation definiert einen Isomorphismus zwischen der Gruppe aller Symmetrien aus $\mathrm{O}(3)$ eines Ikosaeders und dem Produkt der Gruppe seiner Drehsymmetrien mit der zweielementigen Gruppe, die von der Punktspiegelung am Ursprung erzeugt wird. Insbesondere ist die "nichtorientierte Ikosaedergruppe" keineswegs isomorph zur symmetrischen Gruppe $\mathcal{S}_5$.

Übung 8.4.12. Unter einem **Graphen** (ungerichtet, ohne mehrfache Kanten, ohne Schleifen) verstehen wir ein Paar (E, K) bestehend aus einer Menge E und einem System $K \subset \mathcal{P}(E)$ von zweielementigen Teilmengen von E. Die Elemene von E heißen die **Ecken** unseres Graphen, die Elemente von K seine **Kanten**. Zwei

verschiedene Ecken, die zu einer gemeinsamen Kante gehören, heißen **benachbart**. Ein **Isomorphismus** zwischen zwei Graphen ist eine Bijektion zwischen ihren Eckenmengen, die eine Bijektion zwischen ihren Kantenmengen induziert. Zwei Graphen heißen **isomorph** genau dann, wenn es zwischen ihnen einen Isomorphismus gibt. Die Äquivalenzklassen der kleinsten Äquivalenrelation auf der Eckenmenge eines Graphen, unter der benachbarte Elemente äquivalent sind, heißen die **Zusammenhangskomponenten** unseres Graphen. Ein Graph heißt **zusammenhängend** genau dann, wenn er aus einer einzigen Zusammenhangskomponente besteht. Man zeige: Ein zusammenhängender Graph, in dem jede Ecke genau fünf Nachbarn besitzt und je zwei benachbarte Ecken genau zwei gemeinsame Nachbarn, ist isomorph zu jedem weiteren Graphen mit diesen beiden Eigenschaften. Den so charakterisierten Graphen mag man den den "Kantengraphen des Ikosaeders" nennen. Hinweis: Ausprobieren.

Lemma 8.4.13 (Existenz der Ikosaedergruppe). *Es gibt eine endliche Untergruppe der Drehgruppe* $\mathrm{SO}(3)$ *mit Elementen der Ordnungen drei und fünf.*

Beweis. Wir betrachten die Menge $\mathcal{D} \subset \mathcal{P}(S^2)$ aller gleichseitigen Dreiecke mit Ecken auf der Einheitssphäre, die nicht in einer Ebene mit dem Ursprung liegen, formal also

$$\mathcal{D} = \left\{ \{a,b,c\} \;\middle|\; \begin{array}{c} a,b,c \in \mathbb{R}^3,\ \|a\| = \|b\| = \|c\| = 1, \\ \|a-b\| = \|b-c\| = \|c-a\|, \\ \langle a,b,c\rangle_{\mathbb{R}} = \mathbb{R}^3. \end{array} \right\}$$

Gegeben ein Dreieck $\Delta \in \mathcal{D}$ und eine Ecke $a \in \Delta$ definieren wir das **umgeklappte Dreieck** $\Delta^a \in \mathcal{D}$ als das eindeutig bestimmte gleichseitige Dreieck $\Delta^a \in \mathcal{D}$ mit $\Delta \cap \Delta^a = \{b,c\}$. Definieren wir zu einem Dreieck $\Delta \in \mathcal{D}$ die Menge

$$\mathcal{D}(\Delta)$$

als die kleinste Teilmenge $\mathcal{D}(\Delta) \subset \mathcal{D}$, die Δ enthält und stabil ist unter dem Umklappen von Dreiecken, so gilt offensichtlich $\mathcal{D}(\Delta) = \mathcal{D}(\Delta')$ für alle $\Delta' \in \mathcal{D}(\Delta)$. Ist $r \in \mathrm{O}(3)$ orthogonal, so gilt sicher $\{ra, rb, rc\}^{ra} = r(\{a,b,c\}^a)$ für jedes Dreieck $\{a,b,c\} \in \mathcal{D}$ und insbesondere $r(\mathcal{D}(\Delta)) = \mathcal{D}(r\Delta)$. Haben wir nun zusätzlich $|(r\Delta) \cap \Delta| \geq 2$, so folgt $r\Delta \in \mathcal{D}(\Delta)$ und damit $\mathcal{D}(r\Delta) = \mathcal{D}(\Delta)$. Nach diesen Vorüberlegungen gehen wir nun aus von einem regelmäßigen Fünfeck, bilden darauf die Pyramide mit Spitze N und aufsteigenden Kanten von derselben Länge wie die Kanten des Fünfecks, und schrumpfen oder strecken diese Pyramide so, daß wir sie als "Polkappe" in die Einheitssphäre legen können. Dann gehen offensichtlich die fünf gleichseitigen Dreiecke dieser Polkappe durch Umklappen auseinander hervor. Bezeichne $\mathcal{D}^* \subset \mathcal{D}$ die kleinste unter Umklappen

stabile Menge von Dreiecken, die diese fünf Dreiecke umfaßt. Wir zeigen im folgenden, daß $\mathcal{D}^*$ endlich ist: Dann bilden alle Drehungen, die $\mathcal{D}^*$ in sich überführen, offensichtlich eine endliche Untergruppe der Drehgruppe mit Elementen der Ordnungen drei und fünf, und wir sind fertig. Um zu zeigen, daß $\mathcal{D}^*$ endlich ist, bilden wir zu $\mathcal{D}^*$ einen Graphen im Sinne von 8.4.12 wie folgt: Als Graphenecken nehmen wir alle fünfelementigen Teilmengen von $\mathcal{D}^*$ vom Typ "Polkappe", die also aus einem festen Dreieck mit ausgezeichneter Ecke durch wiederholtes Umklappen unter Festhalten dieser einen ausgezeichneten Ecke gewonnen werden können. Nun verbinden wir zwei verschiedene derartige Graphenecken durch eine Graphenkante genau dann, wenn sie mindestens ein Dreieck gemeinsam haben. So erhält man aus $\mathcal{D}^*$ einen zusammenhängenden Graphen mit den Eigenschaften aus 8.4.12: Jede Graphenecke hat genau fünf Nachbarn, und je zwei benachbarte Graphenecken haben genau zwei gemeinsame Nachbarn. Nach Übung 8.4.12 ist ein zusammenhängender Graph mit diesen Eigenschaften jedoch endlich, und damit muß auch unsere Menge von Dreiecken $\mathcal{D}^*$ endlich gewesen sein. □

Ergänzung 8.4.14. Die obigen Überlegungen kann man dahingehend zusammenfassen, daß gegeben ein gleichseitiges Dreieck $\Delta = \{a, b, c\}$, für das es eine Drehung r um die Ursprungsgerade durch a gibt mit $r^5 = \mathrm{id}$ und $r : b \mapsto c$, die Menge $\mathcal{D}(\Delta)$ der daraus durch Umklappen entstehenden Dreiecke endlich ist. Die hier geforderte Eigenschaft hat sicher jedes Dreieck, das anschaulich gesprochen "Fläche eines Ikosaeders" ist. Es gibt aber auch noch andere gleichseitige Dreiecke mit dieser Eigenschaft, nämlich diejenigen gleichseitigen Dreiecke, die anschaulich gesprochen die "Diagonale unseres Ausgangsfünfecks" als Seitenlänge haben.

Übung 8.4.15. Es gibt in der Einheitssphäre zwölfelementige Teilmengen, die stabil sind unter der Drehung mit den Winkeln $\pm 2\pi/5$ um die Ursprungsgeraden durch jeden ihrer Punkte, und je zwei derartige Teilmengen lassen sich durch eine Drehung ineinander überführen.

Ergänzung 8.4.16. Mit welchen platonischen Körpern kann man den Raum füllen? Ich vermute, das geht nur mit Würfeln: Die anderen sollten als Winkel zwischen an einer Kante angrenzenden Flächen nie einen Winkel der Gestalt $2\pi/n$ haben.

Ergänzung 8.4.17. Vielleicht ist es vernünftig, platonische Körper zu definieren über die Mengen ihrer Ecken, die man wohl wie folgt charakterisieren kann: Man definiere für eine endliche Teilmenge E des Raums ihre **Abständezahl** $A(E)$ als die Zahl der möglichen von Null verschiedenen verschiedenen Abstände zwischen ihren Elementen. Eine endliche Teilmenge E einer Sphäre heißt nun Tetraeder bei $|E| = 4$, $A(E) = 1$, Würfel bei $|E| = 8$, $A(E) = 3$, Oktaeder bei $|E| = 6$, $A(E) = 2$, Ikosaeder bei $|E| = 12$, $A(E) = 3$, Dodekaeder bei $|E| = 20$,

$A(E) = 4$. Stimmt das eigentlich? Möglicherweise sollte man bei allen außer dem Tetraeder noch fordern, daß E stabil ist unter Punktspiegelung am Ursprung.

8.5 Skalarprodukte zu Drehgruppen*

8.5.1. In diesem Abschnitt holen wir den Rest des Beweises von Satz 4.1.8 über den Zusammenhang zwischen Bewegungsgruppen und Skalarprodukten nach. Ich erinnere daran, daß wir in 4.1.2 eine Bewegungsgruppe eines dreidimensionalen reellen affinen Raums E definiert hatten als eine alle Translationen umfassende Untergruppe $B \subset \mathrm{Aff}^\times E$ seiner Automorphismengruppe derart, daß es für je zwei Paare (H, L) von Teilmengen von E bestehend aus einer Halbebene und einer Halbgerade auf ihrem Rand genau einen Automorphismus aus B gibt, der sie ineinander überführt. Die Elemente der Isotropiegruppe $B_p \subset B$ eines Punktes $p \in E$ nennen wir **Drehungen um den Punkt** p. Da unsere Bewegungsgruppe nach Annahme alle Translationen enthält, liefert das Bilden des linearen Anteils einen Isomorphismus der Isotropiegruppe B_p jedes Punktes $p \in E$ mit derselben Gruppe $D \subset \mathrm{GL}(\vec{E})$ von Automorphismen des Richtungsraums. Die Elemente von D nennen wir **Drehungen im Richtungsraum**. Nach unserer Definition einer Bewegungsgruppe 4.1.2 bilden die linearen Anteile der Elemente einer Bewegungsgruppe eine Drehgruppe im Sinne der gleich folgenden Definition.

Definition 8.5.2. Unter einem **Strahl** L in einem reellen Vektorraum V verstehen wir eine Teilmenge $L \subset V$ mit der Eigenschaft, daß es in V einen Vektor $v \neq 0$ gibt mit $L = \mathbb{R}_{\geq 0} v$. Unter einer **Drehgruppe** in einem dreidimensionalen reellen Vektorraum verstehen wir eine Untergruppe seiner Automorphismengruppe mit der Eigenschaft, daß es für je zwei Paare von Teilmengen unseres Vektorraums bestehend aus einer linearen Halbebene und einem Strahl auf ihrem Rand genau ein Element unserer Untergruppe gibt, die das eine Paar in das andere überführt. Die Elemente einer solchen Drehgruppe bezeichnen wir dann auch als **Drehungen**.

Satz 8.5.3 (Drehgruppen und Skalarprodukte). *Gegeben ein dreidimensionaler reeller Vektorraum V und ein ausgezeichneter Vektor $m \in V \backslash 0$ liefert die Abbildung $b \mapsto \mathrm{SO}(V; b)$ eine Bijektion*

$$\{\textit{Skalarprodukte } b \textit{ auf } V \textit{ mit } b(m,m) = 1\} \quad \xrightarrow{\sim} \quad \{\textit{Drehgruppen } D \subset \mathrm{GL}(V)\}$$

8.5.4. Aus diesem Satz folgen unmittelbar die noch unbewiesenen Behauptungen von Satz 4.1.8 über den Zusammenhang zwischen Bewegungsgruppen und Skalarprodukten. Der Satz und sein Beweis bleiben richtig, wenn wir statt den reellen Zahlen einen beliebigen angeordneten Körper zugrundelegen, in dem zu jedem positiven Element eine Quadratwurzel existiert.

Zwei Paare von Teilmengen eines dreidimensionalen reellen Vektorraums bestehend aus je einer linearen Halbebene und einem Strahl auf ihrem Rand. Unsere Bedingung an eine Drehgruppe besagt, daß je zwei derartige Paare durch genau eine Drehung unserer Drehgruppe ineinander überführt werden.

Beweis. Den Nachweis, daß für jedes Skalarprodukt b auf V die Gruppe $\mathrm{SO}(V;b) = \{d \in \mathrm{GL}(V) \mid b(dv,dw) = b(v,w)\ \forall v,w \in V \text{ und } \det d = 1\}$ in der Tat eine Drehgruppe ist, überlasse ich dem Leser und beginne gleich mit der Konstruktion der Umkehrabbildung. Sei also V ein dreidimensionaler reeller Vektorraum und $D \subset \mathrm{GL}(V)$ eine Drehgruppe im Sinne unserer Definition 8.5.2. Gegeben $v,w \in V$ vereinbaren wir die Sprechweise, w **stehe drehsenkrecht auf** v und schreiben

$$w \vdash v$$

genau dann, wenn es eine Drehung $r \in D$ gibt mit $r(w) = -w$ und $r(v) = v$. Aus $w \vdash v$ folgt leicht $dw \vdash dv$ für jede Drehung d und $\lambda w \vdash \mu v$ für alle $\mu,\lambda \in \mathbb{R}$. Des weiteren steht nur der Nullvektor drehsenkrecht auf sich selbst. Gegeben linear unabhängige Vektoren $v,w \in V$ vereinbaren wir nun für das dadurch bestimmt Paar aus einer Halbebene nebst einem Strahl auf ihrem Rand speziell für diesen Beweis die Notation

$$[v,w] = (\mathbb{R}v + \mathbb{R}_{\geq 0}w, \mathbb{R}_{\geq 0}v)$$

Unsere Definition einer Drehgruppe besagt in dieser Notation, daß es für je zwei Paare (v,w) und (v',w') von linear unabhängigen Vektoren genau ein Element r unserer Drehgruppe gibt mit $r : [v,w] \mapsto [v',w']$. Als nächstes zeigen wir die Symmetrie der Relation des Drehsenkrechtstehens.

Lemma 8.5.5. *Es gilt* $w \vdash v \ \Rightarrow\ v \vdash w$.

Beweis. Zunächst zeigen wir das für v,w linear unabhängig. Gilt $w \vdash v$, so gibt es ja per definitionem eine Drehung r mit $rw = -w$ und $rv = v$. Das muß natürlich die Drehung r sein mit $r : [v,w] \mapsto [v,-w]$. Betrachten wir zusätzlich die Drehung s mit $s : [v,w] \mapsto [-v,w]$, so folgt $s^2 = \mathrm{id}$ und weiter $sr = rs$, da beide Abbildungen die Eigenschaft $[v,w] \mapsto [-v,-w]$ haben. Daraus folgt erst $sv = -v$ und dann $sw = w$ durch explizite Rechnung oder konzeptioneller, da s die Eigenräume von r im Erzeugnis $\mathbb{R}v + \mathbb{R}w$ stabilisiert. Das liefert dann $v \vdash w$ wie behauptet. Gilt $w \vdash v$ für linear abhängige Vektoren, so muß mindestens einer der Nullvektor sein. Im Fall $v = 0$ ist $0 \vdash w$ offensichtlich, bereits die Identität hält dann w fest und bildet v auf sein Negatives ab. Es reicht also, wenn wir $v \vdash 0$ zeigen für alle $v \neq 0$. Unter dieser Annahme gibt es jedoch für $u \notin \mathbb{R}v$ eine Drehung s mit $s : [v,u] \mapsto [-v,u]$. Wegen $s^2 : [v,u] \mapsto [v,u]$ gilt $s^2 = \mathrm{id}$ und daraus folgt $s(v) = -v$ und damit haben wir in der Tat $v \vdash 0$. □

Lemma 8.5.6. *1. Die auf allen Vektoren einer Ebene drehsenkrecht stehenden Vektoren bilden eine Gerade.*

2. Die auf allen Vektoren einer Gerade drehsenkrecht stehenden Vektoren bilden eine Ebene.

3. *Für jeden von Null verschiedenen Vektor $n \neq 0$ gibt es genau eine Drehung r_n mit $r_n n = n$ und $u \vdash n \Leftrightarrow r_n u = -u$.*

Beweis. Gegeben $G \subset P \subset V$ eine Gerade in einer Ebene gibt es genau eine Drehung, die die Gerade G punktweise festhält und die beiden zugehörigen Halbebenen von P vertauscht: Schreiben wir etwa $G = \mathbb{R}v$ und $P = \mathbb{R}v + \mathbb{R}w$, so kann unsere Drehung charakterisiert werden durch $[v, w] \mapsto [v, -w]$. Es folgt, daß die Menge der auf allen Vektoren aus G drehsenkrecht stehenden Vektoren von P eine Gerade G' ist, eben der (-1)-Eigenraum dieser Drehung in P, und nach 8.5.5 ist die Menge der auf allen Vektoren aus G drehsenkrecht stehenden Vektoren von P dann wieder unsere ursprüngliche Gerade G. Gegeben linear unabhängige Vektoren v, w mit $v \vdash w$ hat die Drehung d mit $d : [v, w] \mapsto [w, -v]$ folglich die Eigenschaft $d(w) \in \mathbb{R}v$ und es ergibt sich sofort $d : [w, -v] \mapsto [-v, -w]$, also $d^4 = \mathrm{id}$. Wir erkennen $d^2 v = -v$, $d^2 w = -w$ und folglich $d^2 u = -u$ für alle $u \in P$. Andererseits haben wir $d^2 \neq -\mathrm{id}$, etwa da die Determinante eines Quadrats nie negativ sein kann, folglich hat d^2 einen von Null verschiedenen Fixvektor n und es folgt $P = \{u \in V \mid n \vdash u\}$. Wir erkennen so, daß die auf einer vorgegebenen Ebene drehsenkrechten Vektoren stets eine Gerade bilden, und daß es zu einem von Null verschiedenen Vektor $n \neq 0$ stets genau eine Drehung r_n gibt mit $r_n(n) = n$ und $u \vdash n \Rightarrow r_n(u) = -u$. Daß die auf allen Vektoren einer Gerade drehsenkrecht stehenden Vektoren eine Ebene bilden, folgt daraus dann unmittelbar. □

Übung 8.5.7. Gegeben ein Vektor $n \neq 0$ gilt für jede Drehung d die Identität $r_{dn} = d \circ r_n \circ d^{-1}$ und für jeden von Null verschiedenen Skalar $\lambda \in \mathbb{R}^\times$ haben wir $r_{\lambda n} = r_n$.

Lemma 8.5.8. *Gegeben zwei linear unabhängige Vektoren v, w gilt für die Drehung r mit $r : [v, w] \mapsto [w, v]$ die Identität $r^2 = \mathrm{id}$ und es gibt $\lambda > 0$ mit $rv = \lambda w$ und $r\lambda w = v$.*

Beweis. Die Restriktion von r auf die Ebene $\mathbb{R}v + \mathbb{R}w$ hat negative Determinante, da ihre Matrix in der Basis v, w oben links eine Null hat und in der Nebendiagonalen positive Einträge. Damit hat unsere Matrix zwei verschiedene reelle Eigenwerte und r^2 hat zwei positive reelle Eigenwerte, etwa mit Eigenvektoren n und m, und wegen $r^2 : [n, m] \mapsto [n, m]$ folgt $r^2 = \mathrm{id}$. Der Rest des Lemmas folgt leicht. □

Lemma 8.5.9. *Bildet eine Drehung einen Strahl bijektiv auf sich selber ab, so hält sie ihn bereits punktweise fest.*

Bemerkung 8.5.10. Dies Lemma formalisiert die Erfahrungstatsache, daß eine Achse beim Drehen ihre Länge nicht ändert, und es mag lächerlich wirken, das

beweisen zu wollen. In der Tat hätten wir diese Aussage auch als zusätzliche Bedingung zu unserer Definition des Anschauungsraums und zur Definition des Begriffs einer Drehgruppe hinzunehmen können. Daß ich das nicht getan habe, hat rein ästhetische Gründe: Wir können so eine größere Wegstrecke mit reiner Logik zurücklegen.

Beweis. Es gilt für $u \neq 0$ und jede Drehung $d \in D$ zu zeigen

$$d(\mathbb{R}_{\geq 0}u) = \mathbb{R}_{\geq 0}u \;\Rightarrow\; du = u$$

Dazu wählen wir $v \neq 0$ mit $v \vdash u$. Gilt $dv \in \mathbb{R}v$, so folgt $d^2v \in \mathbb{R}_{>0}v$ und damit $d^2 : [u, v] \mapsto [u, v]$ und so $d^2 = \mathrm{id}$ und dann $du = u$. Sonst spannen v und dv die zu u drehsenkrechte Ebene auf. Nach 8.5.8 gibt es $\lambda > 0$ und eine Drehung r, die λv mit dv vertauscht. Deren Quadrat ist die Identität, woraus leicht folgt $ru = -u$. Für die Verknüpfung rr_v gilt dann $\lambda v \mapsto dv$ und $u \mapsto u$, woraus folgt $rr_v : [u, v] \mapsto [u, dv]$, also $rr_v = d$ und damit dann $du = u$ wie gewünscht. □

Lemma 8.5.11. *Jede Bahn einer Drehgruppe trifft jeden Strahl in genau einem Punkt.*

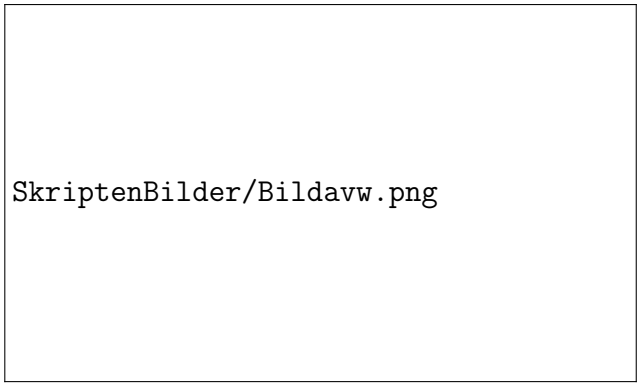
Beweis. Daß jede Bahn jeden Strahl in höchstens einem Punkt trifft, folgt sofort aus 8.5.9. Daß jede Bahn jeden Strahl in mindestens einem Punkt trifft, folgt unmittelbar aus unserer Definition einer Drehgruppe. □

8.5.12. Wie in 4.1.11 erklären wir die Drehnorm eines Vektors v als diejenige nichtnegative reelle Zahl $\|v\| = \lambda$, für die es eine Drehung d gibt mit $d(v) = \lambda m$. Das vorhergehende Lemma 8.5.11 zeigt, daß es genau ein $\lambda \geq 0$ mit dieser Eigenschaft gibt.

Nach diesen Vorbereitungen konstruieren wir nun unser Skalarprodukt. Gegeben $v \neq 0$ und $w \notin \mathbb{R}v$ gilt für unser r_v aus 8.5.6.1 sicher $r_v w = \alpha v - \gamma w$ mit $\gamma \geq 0$. Wegen $r_v^2 w = \alpha v - \alpha\gamma v + \gamma^2 w = w$ folgt $\gamma = 1$. Es gibt folglich für alle $w \in V$ genau eine reelle Zahl $\alpha_v(w)$ mit der Eigenschaft

$$r_v w + w = \alpha_v(w)v$$

Man erkennt unschwer, daß α_v eine Linearform auf V ist. Wir können α_v auch charakterisieren als die eindeutig bestimmte Linearform, die auf v den Wert Zwei annimmt und auf allen zu v drehsenkrechten Vektoren den Wert Null. Unsere Definitionen liefern für jede weitere Drehung d die Identität $\alpha_{dv} \circ d = \alpha_v$ alias $\alpha_{dv} = \alpha_v \circ d^{-1}$ und für jeden von Null verschiedenen Skalar $\lambda \in \mathbb{R}^\times$ die Identität $\alpha_{\lambda v} = \lambda^{-1}\alpha_v$. Werden zwei von Null verschiedene Vektoren v, w durch eine Drehung untereinander vertauscht, so gilt für unsere Ausdrücke weiter die Identität



Diese Abbildung illustriert die Definition von $\alpha_v(w)$. Im hier dargestellten Fall hätten wir etwa $\alpha_v(w) = 3$ und für das Skalarprodukt b_l mit $v \in l$ hätten wir $b_l(v, w) = 3/2$.

Illustration der Identität $\alpha_v(w) = \alpha_w(v)$ unter der Annahme, daß es eine Drehung r gibt, die v und w vertauscht.

$\alpha_v(w) = \alpha_w(v)$. In der Tat, aus $rv = w$ und $rw = v$ folgt $rr_v = r_w r$ und aus der von der Mitte ausgehend zu entwickelnden Gleichungskette

$$\alpha_w(v)w - v = r_w(v) = r_w rw = rr_v w = r(\alpha_v(w)v - w) = \alpha_v(w)w - v$$

ergibt sich die Behauptung. Nun wählen wir die durch unseren ausgezeichneten Vektor m gegebene Drehnorm und erklären die Abbildung $b = b_m : V \times V \to \mathbb{R}$ durch die Vorschrift

$$b(v,w) = \begin{cases} \|v\|^2 \alpha_v(w)/2 & v \neq 0; \\ 0 & v = 0. \end{cases}$$

Offensichtlich gilt $\|v\|^2 = b(v,v)$ und $w \mapsto b(v,w)$ ist linear für alle v. Schließlich beachten wir, daß für je zwei von Null verschiedene Vektoren $v, w \in V$ die Vektoren $\|v\|^{-1}v$ und $\|w\|^{-1}w$ durch eine Drehung untereinander vertauscht werden. Nach dem Vorhergehenden folgt $\|v\|\|w\|^{-1}\alpha_v(w) = \|w\|\|v\|^{-1}\alpha_w(v)$ alias $\|v\|^2\alpha_v(w) = \|w\|^2\alpha_w(v)$ und damit $b(v,w) = b(w,v)$ erst für je zwei von Null verschiedene Vektoren, aber dann auch sofort für alle $v, w \in V$. In der Terminologie aus 4.1.6 ist also b ein Skalarprodukt auf V und wir haben wie versprochen eine Abbildung in die Gegenrichtung konstruiert. Daß unsere beiden Abbildungen in der Tat zueinander invers sind, mag der Leser selbst prüfen. □

8.6 Das kanonische Skalarprodukt*

8.6.1. Ich erinnere an unser Tensorprodukt mit eindimensionalen Räumen aus 2.7.2. Das Tensorprodukt in voller Allgemeinheit werden wir erst in 9.3.2 besprechen.

Definition 8.6.2. Sei V ein reeller Vektorraum und L ein eindimensionaler orientierter reeller Vektorraum. Unter einem **Skalarprodukt auf V mit Einheiten in L** oder kürzer einem **L-wertigen Skalarprodukt** verstehen wir eine symmetrische bilineare Abbildung

$$s : V \times V \to L^{\otimes 2}$$

mit $v \neq 0 \Rightarrow s(v,v) > 0$ für diejenige Orientierung auf $L^{\otimes 2}$, die charakterisiert wird durch die Eigenschaft $a^{\otimes 2} \in L^{\otimes 2}_{>0}$ für alle $a \in L\backslash 0$. Die Orientierung auf L setzen wir hier voraus, damit wir eine Wurzelabbildung $\sqrt{} : L^{\otimes 2}_{\geq 0} \to L_{\geq 0}$ erklären können als das Inverse des Quadrierens $L_{\geq 0} \xrightarrow{\sim} L^{\otimes 2}_{\geq 0}$, $a \mapsto a^{\otimes 2}$, so daß sich die **Länge** eines Vektors erklären läßt als

$$\|v\|_s = \sqrt{s(v,v)} \in L_{\geq 0}$$

8.6.3. Gegeben ein dreidimensionaler reeller Vektorraum mit ausgezeichneter Drehgruppe im Sinne von 8.5.2 soll nun in vollständig kanonischer Weise ein Skalarprodukt mit Einheiten konstruiert werden. Dazu müssen wir aus diesen Daten zuerst einmal einen orientierten eindimensionalen Vektorraum konstruieren, die "Längengerade". Das braucht bereits einige Vorbereitungen.

Definition 8.6.4. Gegeben eine Gruppe G, eine G-Menge X und eine G-Rechtsmenge Y definieren wir ihr **balanciertes Produkt**

$$Y \times_G X$$

als den Quotienten des kartesischen Produkts $Y \times X$ nach der Äquivalenzrelation $(yg, x) \sim (y, gx) \quad \forall y \in Y, x \in X$ und $g \in G$, alias den Bahnenraum von $Y \times X$ unter der durch die Vorschrift $g.(y, x) = (yg^{-1}, gx)$ gegebenen G-Operation. Die Äquivalenzklasse alias Bahn von $(y, x) \in Y \times X$ notieren wir $[y, x] \in Y \times_G X$.

8.6.5. Seien k ein Körper, V ein k-Vektorraum und G eine Gruppe. Seien weiter $\rho : G \to \mathrm{GL}(V)$ ein Gruppenhomomorphismus und Y ein G-Torsor. So gibt es auf dem balancierten Produkt

$$Y \times_G V = Y \times_G^{\rho} V$$

genau eine Struktur als k-Vektorraum derart, daß für alle $y \in Y$ die Abbildung $v \mapsto [y, v]$ einen Vektorraumisomorphismus $V \xrightarrow{\sim} Y \times_G V$ liefert. Des weiteren liefert jede G-äquivariante Abbildung von Torsoren $Y \to Z$ offensichtlich einen Isomorphismus von k-Vektorräumen $Y \times_G V \xrightarrow{\sim} Z \times_G V$.

Definition 8.6.6. Sei V ein dreidimensionaler reeller Vektorraum V mit einer ausgezeichneten Drehgruppe $D \subset \mathrm{GL}(V)$ im Sinne von 8.5.2. Eine Bahn $l \subset V \backslash 0$ unserer Drehgruppe D nennen wir eine **positive Länge**. Diese positiven Längen bilden in natürlicher Weise einen $\mathbb{R}_{>0}$-Torsor im Sinne von 8.1.6.7. Den zugehörigen orientierten eindimensionalen **Vektorraum der Längen** alias die zugehörige **Längengerade** erklären wir als das balancierte Produkt

$$L_D = L = L_{>0} \times_{\mathbb{R}_{>0}} \mathbb{R}$$

versehen mit derjenigen Orientierung, für die alle Vektoren $[l, \alpha]$ mit $l \in L_{>0}$ und $\alpha > 0$ positiv orientierte Basen sind. Die Injektion $L_{>0} \hookrightarrow L$, $l \mapsto [l, 1]$ notieren wir nicht extra, sondern fassen sie im weiteren als die Einbettung einer Teilmenge auf. Das Bild dieser Einbettung sind im übrigen genau die positiven Vektoren unseres orientierten eindimensionalen Vektorraums, so daß wir mit unserer Notation keine Zweideutigkeiten erzeugen.

8.6.7. Gegeben ein dreidimensionaler reeller Vektorraum V mit ausgezeichneter Drehgruppe $D \subset \mathrm{GL}(V)$ gibt es genau ein Skalarprodukt auf V mit Einheiten in der zugehörigen Längengerade L, als da heißt genau eine positiv definite symmetrische bilineare Abbildung

$$s : V \times V \to L^{\otimes 2}$$

derart, daß gilt $s(v,v) = Dv \otimes Dv$ für alle $v \neq 0$. Hier meint $Dv \in L_{>0} \subset L$ die Bahn von v unter der Drehgruppe D. Die Eindeutigkeit von s folgt aus der Polarisierungsidentität und die Existenz erhält man, indem man das Ende des Beweises von 8.5.3 geeignet variiert. Ich schlage vor, diese Abbildung $s : V \times V \to L^{\otimes 2}$ das **kanonische Skalarprodukt** unserer Drehgruppe zu nennen, da es sich dabei um ein Skalarprodukt mit Einheiten im Sinne unserer Definition 8.6.2 handelt, das nur von der ausgezeichneten Drehgruppe und sonst von keinerlei Wahlen abhängt. Die Abbildung $V \to L_{\geq 0}$, die jedem von Null verschiedenen Vektor v seine D-Bahn zuordnet und dem Nullvektor die Null, notieren wir

$$\begin{array}{ccc} V & \to & L_{\geq 0} \\ v & \mapsto & \|v\| \end{array}$$

und nennen $\|v\|$ die **Länge von** v.

Ergänzung 8.6.8. Ist V' ein weiterer dreidimensionaler reeller Vektorraum mit ausgezeichneter Drehgruppe $D' \subset \mathrm{GL}(V')$ und $a : V \xrightarrow{\sim} V'$ ein Vektorraumisomorphismus mit $aDa^{-1} = D'$, so gibt es genau einen Isomorphismus $\hat{a} : L \xrightarrow{\sim} L'$ der zugehörigen Längengeraden mit $\|av\| = \hat{a}\|v\|$ für alle $v \in V$. Für die kanonischen Skalarprodukte s, s' gilt dann auch $s'(av, aw) = \hat{a}^{\otimes 2} s(v,w)$.

8.6.9. Ich fasse nun nocheinmal unser mathematisches Modell des Anschauungsraums zusammen: Wir modellieren ihn, wie in 1.7.7 erklärt, als einen dreidimensionalen reellen affinen Raum

$$\mathbb{E}$$

zusammen mit einer ausgezeichneten Bewegungsgruppe im Sinne von 4.1.2 und einer ausgezeichneten Orientierung. Die Geraden entsprechen unseren Sichtlinien, die ausgezeichneten Bewegungen den anschaulichen Bewegungen, wie in 4.1.4 ausgeführt wird, und die ausgezeichnete Orientierung der "rechte-Hand-Orientierung" aus 4.1.15. Im Richtungsraum des Anschaungsraums erhalten wir dann als Gruppe der linearen Anteile unserer ausgezeichneten Bewegungen eine ausgezeichnete Drehgruppe im Sinne von 8.5.2. Diese ausgezeichnete Drehgruppe liefert hinwiederum, wie in 8.6.6 und 8.6.7 erklärt, eine ausgezeichnete Längengerade, die wir in diesem Fall mit

$$\mathbb{L}$$

bezeichnen. Außerdem erhalten wir nach 8.6.7 ein kanonisches Skalarprodukt $\langle\ ,\ \rangle$ mit Einheiten in dieser Längengerade, als da heißt mit Werten in ihrem Tensorquadrat $\mathbb{L}^{\otimes 2}$. Zumindest in Europa wird besagte Längengerade meist vermittels des in der französischen Revolution gewählten **Meters**

$$\mathrm{m} \in \mathbb{L}_{>0}$$

mit der Zahlengerade $\mathbb{R}$ identifiziert. Das kanonische Skalarprodukt auf dem Richtungsraum des Anschauungsraums nimmt also Werte in einem eindimensionalen reellen Vektorraum an, für den das "Quadratmeter" eine Basis ist. Man notiert das Quadratmeter meist abkürzend m^2 statt $\mathrm{m}^{\otimes 2}$, wie in 2.7.6 erklärt. Natürlich haben wir auch in diesem Fall eine Abbildung

$$\| \ \| : \vec{\mathbb{E}} \to \mathbb{L}_{\geq 0}$$

die eben jedem Vektor seine Länge zuordnet.

8.6.10. Sei nun V ein dreidimensionaler reeller Vektorraum mit einem L-wertigen Skalarprodukt. Sei $\mathrm{or}_{\mathbb{R}}(V)$ seine Orientierungsgerade aus 4.5.25. So können wir im nach Übung 3.3.9 eindimensionalen Raum aller alternierenden multilinearen Abbildungen

$$V \times V \times V \ \to \ L^{\otimes 3} \otimes \mathrm{or}_{\mathbb{R}}(V)$$

eine Abbildung auszeichnen durch die Eigenschaft, daß sie eine angeordnete Orthogonalbasis auf das Produkt der Längen ihrer Vektoren mit ihrer Orientiertierung abbildet. Daß sie das dann sogar für jede Orthogonalbasis tut, folgt ohne große Schwierigkeiten aus unserer Erkenntnis, daß jede orthogonale Matrix Determinante ± 1 hat. Diese Abbildung heißt dann das **Spatprodukt**. Es verallgemeinert unser Spatprodukt aus 4.5.20 und hat auch dieselbe anschauliche Bedeutung als das Volumen des von unseren drei Vektoren gebildeten Spats mit einem von der Orientierung abhängigen Faktor. Insbesondere erhalten wir so durch die Wahl der der Rechte-Hand-Orientierung auf dem Anschauungsraum das Spatprodukt

$$\begin{array}{ccc} \vec{\mathbb{E}} \times \vec{\mathbb{E}} \times \vec{\mathbb{E}} & \to & \mathbb{L}^{\otimes 3} \\ (u,v,w) & \mapsto & \langle u,v,w\rangle \end{array}$$

8.6.11. Sei weiter V ein dreidimensionaler reeller Vektorraum mit einem L-wertigen Skalarprodukt. Wir können eine bilineare Abbildung, das **Kreuzprodukt**

$$\begin{array}{ccc} V \times V & \to & V \otimes L \otimes \mathrm{or}_{\mathbb{R}}(V) \\ (v,w) & \mapsto & v \times w \end{array}$$

definieren durch die Vorschrift $\langle u, v \times w\rangle = \langle u,v,w\rangle \ \forall u \in V$. Es verallgemeinert unsere Kreuzprodukte aus 4.5.18 und 4.5.25 und hat auch dieselbe anschauliche

Bedeutung, wie sie in 4.5.22 erklärt wird. Ist insbesondere $\mathrm{e}_1, \mathrm{e}_2, \mathrm{e}_3$ eine Orthogonalbasis aus drei Vektoren gleicher Länge $l \in L$, so gilt $\mathrm{e}_1 \times \mathrm{e}_2 = \mathrm{e}_3 \otimes l \otimes \varepsilon$ mit ε der durch unsere Basis gegebenen Orientierung. Als Spezialfall ergibt sich durch Auszeichnung der Rechte-Hand-Orientierung das **Kreuzprodukt auf dem Anschauungsraum**

$$\begin{array}{ccc} \vec{\mathbb{E}} \times \vec{\mathbb{E}} & \to & \vec{\mathbb{E}} \otimes \mathbb{L} \\ (v, w) & \mapsto & v \times w \end{array}$$

8.7 Projektive Räume

Definition 8.7.1. Gegeben ein Körper k und ein k-Vektorraum W bezeichnen wir die Menge aller Geraden in W durch den Ursprung mit

$$\mathbb{P}W = \mathbb{P}_k W := \{V \subset W \mid V \text{ ist ein eindimensionaler Untervektorraum}\}$$

und nennen diese Menge den **projektiven Raum** zu W.

8.7.2. Jeder Punkt unseres Raums hat also die Gestalt $\langle w \rangle$ für $w \in W \backslash 0$. Ist W der Nullvektorraum, so ist $\mathbb{P}W$ leer. Ist W eindimensional, so besteht $\mathbb{P}W$ aus einem einzigen Punkt. Für $n \geq 0$ heißt der projektive Raum zu k^{n+1} der **n-dimensionale projektive Raum über dem Körper** k und wir notieren ihn

$$\mathbb{P}(k^{n+1}) = \mathbb{P}^n k$$

Gegeben $x_0, x_1, \ldots, x_n \in k$ nicht alle Null bezeichnen wir die Gerade durch den Ursprung und den Punkt mit den Koordinaten $x_0, x_1, \ldots, x_n$, aufgefaßt als Punkt des n-dimensionalen projektiven Raums, mit

$$\langle x_0, x_1, \ldots, x_n \rangle := \langle (x_0, x_1, \ldots, x_n) \rangle$$

Üblich sind auch die Schreibweisen $[x_0, x_1, \ldots, x_n]$ und $(x_0; x_1; \ldots; x_n)$ für diesen Punkt des projektiven Raums $\mathbb{P}^n k$. Wir erhalten eine Einbettung $k^n \hookrightarrow \mathbb{P}^n k$ vermittels der Abbildungsvorschrift $(x_1, \ldots, x_n) \mapsto \langle 1, x_1, \ldots, x_n \rangle$. Das Komplement des Bildes dieser Einbettung ist genau die Menge $\mathbb{P}^{n-1} k$ aller Geraden durch den Ursprung im Teilraum $0 \times k^n \subset k^{n+1}$, so daß wir mit einigen impliziten Identifikationen für alle $n \geq 1$ eine Zerlegung

$$\mathbb{P}^n k = k^n \sqcup \mathbb{P}^{n-1} k$$

erhalten. Im Fall $n = 1$ notieren wir diese Zerlegung meist $\mathbb{P}^1 k = k \sqcup \{\infty\}$ oder reden von der **kanonischen Bijektion** $k \sqcup \{\infty\} \xrightarrow{\sim} \mathbb{P}^1 k$.

Ergänzung 8.7.3. Die projektiven Räume $\mathbb{P}V$ zu endlichdimensionalen reellen oder komplexen Vektorräumen V können mit einer Topologie versehen werden durch die Vorschrift, daß eine Teilmenge offen sein soll genau dann, wenn ihr Urbild in $V\backslash 0$ offen ist. Mehr zu dieser sogenannten "natürlichen Topologie" diskutieren wir in **??**. Bereits hier sei erwähnt, daß es für diese Topologien stetige Bijektionen mit stetiger Umkehrung gibt, die $\mathbb{P}^1\mathbb{R}$ mit der Kreislinie S^1 und $\mathbb{P}^1\mathbb{C}$ mit der Kugelschale S^2 identifizieren. Deshalb heißt $\mathbb{P}^1\mathbb{C}$ auch die **Riemann'sche Zahlenkugel**. Genauer erhalten wir eine derartige Identifikation für $\mathbb{P}^1\mathbb{C}$, indem wir eine Kugelschale auf die komplexe Zahlenebene legen, eine Lampe an den höchsten Punkt P stellen und jeden Punkt der Kugelschale, der nicht gerade der höchste Punkt ist, auf seinen Schatten in der Ebene $\mathbb{C}$ abbilden, den höchsten Punkt P jedoch auf ∞. Im reellen Fall verfährt man analog.

8.7.4. Sicher operiert die Gruppe $\mathrm{GL}(n+1;k)$ auf $\mathbb{P}^n k$. Die offensichtliche Operation von $\mathrm{GL}(2;k)$ auf $\mathbb{P}^1 k$ entspricht unter unserer Identifikation von $\mathbb{P}^1 k$ mit $k \sqcup \{\infty\}$ der Operation von $\mathrm{GL}(2;k)$ auf $k \sqcup \{\infty\}$, unter der eine Matrix durch die Transformation

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : x \mapsto \frac{c+dx}{a+bx}$$

wirkt. Der Punkt ∞ muß hier mit etwas Sorgfalt ins Spiel gebracht werden und ich schreibe nicht alle Fälle aus. Man sie jedoch leicht erschließen, wenn man weiß, daß diese Operation im Fall $k = \mathbb{R}$ stetig ist für die natürliche Topologie aus 8.7.3. Zum Beispiel geht ∞ im Fall $b \neq 0$ nach d/b.

Übung 8.7.5. Unter der Operation von $\mathrm{GL}(n+1;\mathbb{Q})$ auf dem projektiven Raum $\mathbb{P}^n\mathbb{Q}$ operiert bereits die Gruppe $\mathrm{SL}(n;\mathbb{Z})$ aller $(n\times n)$-Matrizen mit ganzzahligen Einträgen und Determinante Eins transitiv. Hinweis: 7.4.21.

Übung 8.7.6. Gegeben zwei Tripel von paarweise verschiedenen Geraden in der Ebene k^2 gibt es stets eine lineare Abbildung, die das eine Tripel in das andere überführt, und diese lineare Abbildung ist eindeutig bestimmt bis auf einen Skalar. Betrachten wir die offensichtliche Operation von $\mathrm{GL}(2;k)$ auf $(\mathbb{P}^1 k)^3$, so erhalten demnach durch die Vorschrift $g \mapsto g(0,1,\infty)$ eine Bijektion

$$\mathrm{GL}(2;k)/(k^\times \,\mathrm{id}) \;\xrightarrow{\sim}\; (\mathbb{P}^1 k)^3\backslash\Delta$$

für Δ die "dicke Diagonale" alias die Menge aller Tripel mit mindestens zwei gleichen Einträgen. Man definiert das **Doppelverhältnis**

$$b : (\mathbb{P}^1 k)^4\backslash\Delta \;\xrightarrow{\sim}\; k\backslash\{0,1\}$$

auf der Menge aller Quadrupel mit vier paarweise verschiedenen Einträgen durch die Vorschrift, daß jedem derartigen Quadrupel (x_1,x_2,x_3,x_4) derjenige eindeutig

Der gestrichelte Kreis wird durch die “stereographische Projektion” mit der gestrichelten Geraden identifiziert. Demnächst werden Sie diese Abbildung auch als “Inversion am durchgezogenen Kreis” verstehen lernen.

bestimmte Punkt $x \in k$ zugeordnet werden soll, für den es ein $g \in \mathrm{GL}(2;k)$ gibt mit $g : (x_1, x_2, x_3, x_4) \mapsto (x, 0, 1, \infty)$. Man zeige für dies Doppelverhältnis die Formel

$$b(x_1, x_2, x_3, x_4) = \frac{x_1 - x_2}{x_1 - x_4} \Big/ \frac{x_3 - x_2}{x_3 - x_4}$$

Diese Formel erklärt auch die Herkunft der Bezeichnung als Doppelverhältnis.

Ergänzende Übung 8.7.7. Eine Teilmenge von $\mathbb{C} \sqcup \{\infty\}$ heißt ein **verallgemeinerter Kreis** genau dann, wenn sie entweder einen Kreis in der komplexen Zahlenebene darstellt oder aber aus allen Punkten einer affinen reellen Gerade besteht, die also nicht notwendig durch den Ursprung geht, ergänzt um den Punkt ∞. Eine **reelle Form** eines $\mathbb{C}$-Vektorraums ist ein $\mathbb{R}$-Untervektorraum mit der Eigenschaft, daß jede $\mathbb{R}$-Basis dieses Teilraums eine $\mathbb{C}$-Basis unseres ursprünglichen Raums ist. Man zeige, daß unter der zuvor erklärten Identifikation $\mathbb{C} \sqcup \{\infty\} \xrightarrow{\sim} \mathbb{P}^1\mathbb{C}$ die verallgemeinerten Kreise gerade die Bilder in $\mathbb{P}^1\mathbb{C}$ der Mengen $E \backslash 0$ für die reellen Formen $E \subset \mathbb{C}^2$ von $\mathbb{C}^2$ sind. Man zeige weiter, daß so die Menge aller verallgemeinerten Kreise aus $\mathbb{C} \sqcup \{\infty\}$ identifiziert werden kann mit der Menge der reellen Formen auf dem $\mathbb{C}^2$, und daß die Operation von $\mathrm{GL}(2;\mathbb{C})$ auf $\mathbb{C} \sqcup \{\infty\}$ aus 8.7.4 verallgemeinerte Kreise in verallgemeinerte Kreise überführt. Im übrigen stabilisiert die induzierte Operation von $\mathrm{GL}(2;\mathbb{R})$ auf $\mathbb{C} \sqcup \{\infty\}$ den verallgemeinerten Kreis $\mathbb{R} \sqcup \{\infty\}$ und die induzierte Operation der zusammenhängenden Untergruppe $\mathrm{GL}(2;\mathbb{R})^+$ aller Matrizen mit positiver Determinante stabilisiert auch die offene obere und untere Halbebene in der komplexen Zahlenebene.

Ergänzende Übung 8.7.8 (**Möbius-Geometrie**). Sei $n \geq 1$ gegeben. Eine Teilmenge $K \subset \mathbb{R}^n \sqcup \{\infty\}$ heiße eine **verallgemeinerte Sphäre** genau dann, wenn sie entweder eine Sphäre in $\mathbb{R}^n$ ist, also $K = K(c,r) = \{x \in \mathbb{R}^n \mid \|x - c\| = r\}$ für ein $c \in \mathbb{R}^n$ und $r \in \mathbb{R}_{>0}$, oder eine affine Hyperebene vermehrt um den Punkt ∞. Jeder verallgemeinerten Sphäre K ordnen wir eine Abbildung

$$s_K : \mathbb{R}^n \sqcup \{\infty\} \to \mathbb{R}^n \sqcup \{\infty\}$$

zu, die wir die **Spiegelung an unserer verallgemeinerten Sphäre** nennen, und zwar die übliche Spiegelung $\mathbb{R}^n \to \mathbb{R}^n$ mit der Zusatzregel $\infty \mapsto \infty$ im Fall, daß unsere verallgemeinerte Sphäre eine Hyperebene ist, die Abbildung $y \mapsto y/\|y\|^2$ mit der Zusatzregel $c \mapsto \infty$ und $\infty \mapsto c$ im Fall der in Null zentrierten Einheitssphäre $K(0,1)$ und allgemeiner die **Inversion**

$$y \mapsto c + \frac{r^2}{\|y - c\|^2}(y - c)$$

mit der Zusatzregel $c \mapsto \infty$ und $\infty \mapsto c$ im Fall $K = K(c,r)$. Man zeige, daß Inversionen verallgemeinerte Sphären in verallgemeinerte Sphären überführen. Hinweis: Man verwende 8.7.7. Man zeige, daß Inversionen Winkel erhalten in

dem Sinne, daß ihr Differential an jedem vom Zentrum der Inversion verschiedenen Punkt Winkel erhält. Hinweis: Es reicht zu zeigen, daß *eine* Orthonormalbasis unter dem Differential an jedem festen Punkt eine mit einem festen Faktor skalierte Orthonormalbasis wird. Man betrachte hierzu Orthonormalbasen, bei denen ein Vektor die Richtung vom Zentrum der Inversion zu unserem festen Punkt angibt.

Ergänzung 8.7.9. Die von allen Spiegelungen an verallgemeinerten Sphären erzeugte Untergruppe von $\mathrm{Ens}^\times(\mathbb{R}^n \sqcup \{\infty\})$ heißt die **Möbiusgruppe** und ihre Elemente heißen **Möbiustransformationen**. Zum Beispiel identifiziert die Spiegelung an der Sphäre mit Zentrum im Punkt e_{n+1} und Radius Zwei die Einheitssphäre $S^n \subset \mathbb{R}^{n+1} \sqcup \{\infty\}$ mit der Hyperebene $\{x_{n+1} = -1\} \sqcup \{\infty\}$, wie nebenstehendes Bild im Fall $n = 1$ illustriert. Halten wir noch eine Verschiebung um e_{n+1} dahinter, so erhalten wir eine Identifikation $S^n \xrightarrow{\sim} \mathbb{R}^n \sqcup \{\infty\}$, die wir verwenden, um die rechte Seite und insbesondere auch $\mathbb{P}^1\mathbb{C} = \mathbb{C} \sqcup \{\infty\}$ mit einer Topologie zu versehen. Die von allen Verknüpfungen von zwei solchen Spiegelungen erzeugte Untergruppe heißt die Gruppe der **orientierungserhaltenden Möbiustransformationen**. Sie besteht genau aus denjenigen Möbiustransformationen, die in einer Terminologie, die erst später eingeführt wird, die "Orientierung auf der Mannigfaltigkeit $\mathbb{R}^n \sqcup \{\infty\} \cong S^n$ erhalten". Unter den üblichen Identifikationen

$$\mathbb{R}^2 \sqcup \{\infty\} \xrightarrow{\sim} \mathbb{C} \sqcup \{\infty\} \xrightarrow{\sim} \mathbb{P}^1\mathbb{C}$$

entsprechen die orientierungserhaltenden Möbiustransformationen gerade den von der Operation von $\mathrm{GL}(2;\mathbb{C})$ herkommenden Transformationen, bei denen wir ja bereits in 8.7.7 gesehen hatten, daß sie in $\mathbb{C} \sqcup \{\infty\}$ verallgemeinerte Kreise in verallgemeinerte Kreise überführen.

Ergänzende Übung 8.7.10. Man zeige, daß für $n \geq 2$ jede bijektive Abbildung $\mathbb{R}^n \sqcup \{\infty\} \xrightarrow{\sim} \mathbb{R}^n \sqcup \{\infty\}$ mit der Eigenschaft, daß das Bild jeder verallgemeinerten Sphäre eine verallgemeinerte Sphäre ist, bereits eine Möbiustransformation sein muß. Hinweis: Ohne Beschränkung der Allgemeinheit darf man annehmen, daß ∞ ein Fixpunkt unserer Abbildung ist; mithilfe von 1.7.33 folgere man dann, daß unsere Abbildung auf $\mathbb{R}^n$ affin sein muß; mit 4.5.6 folgere man schließlich, daß diese affine Abbildung eine Ähnlichkeit sein muß.

Ergänzende Übung 8.7.11. Die Möbiustransformationen $\mathbb{R}^n \sqcup \{\infty\} \xrightarrow{\sim} \mathbb{R}^n \sqcup \{\infty\}$ mit Fixpunkt ∞ sind genau die Fortsetzungen der Ähnlichkeiten auf $\mathbb{R}^n$ durch die Vorschrift $\infty \mapsto \infty$.

Ergänzende Übung 8.7.12. Wir betrachten für $n \geq 1$ das Anfügen einer Null $\mathbb{R}^n \sqcup \{\infty\} \hookrightarrow \mathbb{R}^{n+1} \sqcup \{\infty\}$. Man zeige, daß eine Selbstabbildung von $\mathbb{R}^n \sqcup \{\infty\}$ eine Möbiustransformation ist genau dann, wenn sie sich zu einer Möbiustransformation auf $\mathbb{R}^{n+1} \sqcup \{\infty\}$ fortsetzen läßt. Hinweis: Will man direkte Rechnung vermeiden, mag man mit 8.7.10 argumentieren.

Die Inversion an dem als durchgezogene Linie eingezeichneten Kreis hält jeden Punkt auf dem Kreis fest und wirft sein Zentrum nach ∞. Folglich vertauscht diese Inversion den gestrichelten Kreis mit der gestrichelten Geraden. Die gezackte Gerade oder vielmehr der zugehörige verallgemeinerte Kreis wird von der Inversion auf sich selbst geworfen, folglich wirkt unsere Inversion auf den Punkten des gestrichelten Kreises wie die stereographische Projektion.

Ergänzende Übung 8.7.13. Hält eine Möbiustransformation auf $\mathbb{R}^n \sqcup \{\infty\}$ für $n \geq 1$ eine verallgemeinerte Sphäre punktweise fest, so ist sie entweder die Identität, oder aber die Inversion an besagter verallgemeinerter Sphäre. Hinweis: 8.7.11

Ergänzende Übung 8.7.14. Man betrachte die **stereographische Projektion** der Einheitssphäre auf die xy-Ebene vermehrt um einen Punkt ∞, die jedem Punkt außer dem Nordpol $n = (0, 0, 1)$ den Schnittpunkt mit der xy-Ebene der Geraden durch diesem Punkt und den Nordpol zuordnet, und die den Nordpol auf ∞ wirft. Sie kann verstanden werden als Restriktion der Inversion an derjenigen Sphäre mit Zentrum im Nordpol, die die xy-Ebene im Einheitskreis schneidet. Mit der vorhergehenden Übung 8.7.8 erkennt man so, daß unter der stereographischen Projektion Kreise auf der Einheitssphäre als Schnitte der Einheitssphäre mit anderen Sphären übergehen in verallgemeinerte Kreise in der xy-Ebene, und daß die stereographische Projektion Winkel erhält.

Ergänzung 8.7.15. Gegeben ein affiner Raum E können wir auch den projektiven Raum $\mathbb{P}\,\mathrm{Lin}(E)$ seiner Linearisierung aus 1.7.35 betrachten. Unsere Bijektion $(E \times k^\times) \sqcup \vec{E} \xrightarrow{\sim} \mathrm{Lin}(E)$ aus 1.7.35 liefert dann eine Bijektion

$$E \sqcup \mathbb{P}\vec{E} \xrightarrow{\sim} \mathbb{P}\,\mathrm{Lin}(E)$$

Anschaulich gesprochen entsteht also $\mathbb{P}\,\mathrm{Lin}(E)$ aus E, indem man "für jede Richtung alias jede Parallelenschar von affinen Geraden noch einen Punkt im Unendlichen ergänzt". Ich nenne $\mathbb{P}\,\mathrm{Lin}(E)$ die **projektive Vervollständigung** des affinen Raums E. Ist V ein Vektorraum und $E \subset V$ eine affine Hyperebene, die den Ursprung nicht enthält, so kann man die Abbildung $E \to \mathbb{P}V$, $e \mapsto \langle e \rangle$ zu einer Bijektion

$$\mathbb{P}\,\mathrm{Lin}(E) \xrightarrow{\sim} \mathbb{P}V$$

fortsetzen, indem man jeder Richtung aus $\mathbb{P}\vec{E}$ dieselbe Richtung in $\mathbb{P}V$ zuordnet.

9 Universelle Konstruktionen

9.1 Quotientenvektorräume

Satz 9.1.1 (Quotientenvektorraum). *Sei k ein Körper. Gegeben $V \supset U$ ein k-Vektorraum mit einem Teilraum existiert auf der Restklassengruppe V/U aus 7.2.6 genau eine Struktur als k-Vektorraum $k\times V/U \to V/U$ derart, daß die kanonische Projektion*

$$\mathrm{can} : V \twoheadrightarrow V/U$$

aus 7.2.8 eine k-lineare Abbildung wird. Mit dieser Vektorraumstruktur heißt V/U der **Quotient von V nach U.**

Beweis. Wir betrachten die Abbildung

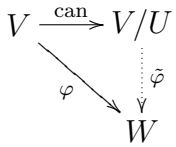
$$\begin{array}{ccc} k \times \mathcal{P}(V) & \to & \mathcal{P}(V) \\ (\lambda\ ,\ A) & \mapsto & \lambda.A := \lambda A + U \end{array}$$

Für $A = v + U$ finden wir $\lambda.A = \lambda A + U = \lambda v + U$, so daß unsere Abbildung eine Abbildung $k \times V/U \to V/U$ induziert, die die Eigenschaft $\overline{\lambda v} = \lambda.\bar v$ hat für alle $\lambda \in k$, $v \in V$. Damit folgt sofort, daß unsere Abbildung $k \times V/U \to V/U$ auf der abelschen Gruppe V/U eine Struktur als k-Vektorraum definiert, und daß die Projektion $V \twoheadrightarrow V/U$ für diese Struktur k-linear ist. Umgekehrt ist auch klar, daß das die einzige Struktur als k-Vektorraum auf der abelschen Gruppe V/U ist, für die die Projektion $V \twoheadrightarrow V/U$ eine k-lineare Abbildung sein kann. □

Satz 9.1.2 (Universelle Eigenschaft des Quotientenvektorraums). *Seien k ein Körper und $V \supset U$ ein k-Vektorraum mit einem Untervektorraum. So hat die kanonische Projektion $\mathrm{can} : V \twoheadrightarrow V/U$ den Kern $\ker(\mathrm{can}) = U$ und für jeden weiteren Vektorraum W liefert das Vorschalten der kanonischen Projektion eine Bijektion*

$$\mathrm{Hom}_k(V/U, W) \xrightarrow{\circ\,\mathrm{can}}_{\sim} \{\varphi \in \mathrm{Hom}_k(V, W) \mid \varphi(U) = 0\}$$

9.1.3. Mit dem Diagramm



können wir die Aussage dieses Satzes auch dahingehend formulieren, daß jede lineare Abbildung $\varphi : V \to W$ mit $\varphi(U) = 0$ auf genau eine Weise k-linear "über die kanonische Projektion $\mathrm{can} : V \twoheadrightarrow V/U$ faktorisiert". Genau genommen hat also gar nicht der Quotientenvektorraum die universelle Eigenschaft, sondern der Homomorphismus $\mathrm{can} : V \to V/U$ in den Quotientenvektorraum.

Beweis. Es muß nur gezeigt werden, daß der nach der universellen Eigenschaft der Restklassengruppe 7.2.8 wohldefinierte Gruppenhomomorphismus $\tilde{\varphi}$ in unserer Situation auch k-linear ist. Das folgt jedoch aus $\tilde{\varphi}(\lambda\bar{v}) = \tilde{\varphi}(\overline{\lambda v}) = \varphi(\lambda v) = \lambda\varphi(v) = \lambda\tilde{\varphi}(\bar{v})$. □

9.1.4. Jeder Vektorraumhomomorphismus $f : V \to W$ induziert einen Vektorraumisomorphismus $V/\ker f \xrightarrow{\sim} \operatorname{im} f$: Das folgt unmittelbar aus der entsprechenden Aussage für Gruppen 7.2.12.

9.1.5. Gegeben Vektorräume $V \supset W \supset U$ induziert die Komposition von kanonischen Abbildungen $V \twoheadrightarrow V/U \twoheadrightarrow (V/U)/(W/U)$ einen Vektorraumisomorphismus $V/W \xrightarrow{\sim} (V/U)/(W/U)$. Das folgt unmittelbar aus dem Noether'schen Isomorphiesatz 7.2.14.

Definition 9.1.6. Gegeben $V \supset U$ ein Vektorraum mit einem Untervektorraum heißt $\dim(V/U)$ auch die **Kodimension von U in V**.

Bemerkung 9.1.7. Ist V endlichdimensional, so haben wir nach 9.1.2 und der Dimensionsformel 1.6.12 die Identität $\dim(V/U) = \dim(V) - \dim(U)$, aber es gibt auch in unendlichdimensionalen Räumen durchaus Teilräume endlicher Kodimension. Eine Teilmenge eines Vektorraums ist eine lineare Hyperebene im Sinne von 1.3.24 genau dann, wenn sie ein Untervektorraum der Kodimension Eins ist.

Ergänzende Übung 9.1.8. Gegeben eine bilineare Abbildung $b : V \times W \to L$ und Untervektorräume $A \subset V$ und $B \subset W$ mit $b(A \times W) = 0 = b(V \times B)$ gibt es genau eine bilineare Abbildung $\bar{b} : (V/A) \times (W/B) \to L$ derart, daß das folgende Diagramm kommutiert:

$$\begin{array}{ccc} V \times W & \xrightarrow{b} & L \\ {\scriptstyle \mathrm{can} \times \mathrm{can}}\downarrow & & \| \\ V/A \times W/B & \xrightarrow{\bar{b}} & L \end{array}$$

Ergänzende Übung 9.1.9. Man zeige: Eine Menge von paarweise kommutierenden trigonalisierbaren Endomorphismen eines endlichdimensionalen Vektorraums ist stets simultan trigonalisierbar, als da heißt, es gibt eine Basis, bezüglich derer alle unsere Endomorphismen eine Matrix von oberer Dreiecksgestalt haben. Hinweis: 6.3.9.

9.2 Kurze exakte Sequenzen*

9.2.1. Um die Beziehung des Quotientenraums zu anderen Konstruktionen wie etwa dem Dualraum zu diskutieren, ist die Sprache der exakten Sequenzen aus 7.5.2 und besonders die Sprache der kurzen exakten Sequenzen, wie wir sie gleich einführen werden, besonders gut geeignet.

Definition 9.2.2. Eine Sequenz von Gruppen $A' \to A \to A''$ heißt eine **kurze exakte Sequenz** genau dann, wenn sie im Sinne von 7.5.2 exakt ist in der Mitte und außerdem die erste Abbildung injektiv ist und die zweite surjektiv. Gleichbedeutend ist die Forderung, daß die in trivialer Weise erweiterte Sequenz $1 \to A' \to A \to A'' \to 1$ an jeder Stelle exakt ist. Wir notieren kurze exakte Sequenzen meist $A' \hookrightarrow A \twoheadrightarrow A''$.

Beispiel 9.2.3. Für jeden Normalteiler $N \subset G$ ist $N \hookrightarrow G \twoheadrightarrow G/N$ eine kurze exakte Sequenz von Gruppen. Für jeden Untervektorraum $U \subset V$ ist speziell $U \hookrightarrow V \twoheadrightarrow V/U$ eine kurze exakte Sequenz von Vektorräumen.

Beispiel 9.2.4. Für jeden surjektiven Gruppenhomomorphismus $x : G \twoheadrightarrow G''$ ist $(\ker x) \hookrightarrow G \twoheadrightarrow G''$ eine kurze exakte Sequenz von Gruppen. Für jede surjektive lineare Abbildung $V \twoheadrightarrow W$ ist speziell $(\ker x) \hookrightarrow V \twoheadrightarrow W$ eine kurze exakte Sequenz von Vektorräumen.

9.2.5. Die Dimensionsformel 1.6.12 kann in dieser Terminologie auch dahingehend formuliert werden, daß für jede kurze exakte Sequenz $V' \hookrightarrow V \twoheadrightarrow V''$ von Vektorräumen gilt

$$\dim V = \dim V' + \dim V''$$

Definition 9.2.6. Gegeben Sequenzen $A \xrightarrow{r} B \xrightarrow{s} C$ und $A' \xrightarrow{r'} B' \xrightarrow{s'} C'$ verstehen wir unter einem **Homomorphismus von Sequenzen** ein Tripel (f, g, h) von Homomophismen derart, daß das folgende Diagramm kommutiert:

$$\begin{array}{ccccc} A & \xrightarrow{r} & B & \xrightarrow{s} & C \\ \downarrow f & & \downarrow g & & \downarrow h \\ A' & \xrightarrow{r'} & B' & \xrightarrow{s'} & C' \end{array}$$

Solch ein Morphismus heißt ein **Isomorphismus von Sequenzen** genau dann, wenn alle drei vertikalen Abbildungen f, g und h Isomorphismen sind.

9.2.7. Offensichtlich ist mit einer exakten Sequenz auch jede dazu isomorphe Sequenz exakt. Für jede kurze exakte Sequenz $A' \hookrightarrow A \twoheadrightarrow A''$ von Gruppen ist das Bild $N \subset A$ von A' ein Normalteiler und wir erhalten einen Isomorphismus von kurzen exakten Sequenzen

$$\begin{array}{ccccc} N & \hookrightarrow & A & \twoheadrightarrow & A/N \\ \wr\downarrow f & & \| & & \wr\downarrow h \\ A' & \hookrightarrow & A & \twoheadrightarrow & A'' \end{array}$$

indem wir für f die Inverse der von der Einbettung $A' \hookrightarrow A$ induzierten Bijektion $A' \xrightarrow{\sim} N$ nehmen und für h die von der universellen Eigenschaft des Quotienten 7.2.8 induzierte Abbildung. Arbeiten wir speziell mit Vektorräumen, so finden wir

mit 1.5.21 in A einen zu N komplementären Teilraum U und nach 1.6.11 induziert die kanonische Abbildung einen Isomorphismus $U \xrightarrow{\sim} A/N$. In diesem Fall erhalten wir also zusätzlich einen Isomorphismus von kurzen exakten Sequenzen

$$\begin{array}{ccccc} N & \hookrightarrow & N \oplus U & \twoheadrightarrow & U \\ \| & & \wr\downarrow g & & \wr\downarrow h \\ N & \hookrightarrow & A & \twoheadrightarrow & A/N \end{array}$$

wobei implizit zu verstehen ist, daß die Morphismen der oberen Horizontale schlicht die kanonische Injektion und Projektion sein sollen. Im Fall von Gruppen, selbst im Fall von abelschen Gruppen, liegen die Verhältnisse komplizierter, wie bereits der Fall der kurzen exakten Sequenz $\mathbb{Z} \hookrightarrow \mathbb{Z} \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}$ zeigt, mit der Multiplikation mit Zwei als erster Abbildung.

9.2.8. Gegeben eine kurze exakte Sequenz von Vektorräumen ist auch die duale Sequenz eine kurze exakte Sequenz. Das ist in der Tat offensichtlich im Fall einer kurzen exakten Sequenz der Gestalt $N \hookrightarrow N \oplus U \twoheadrightarrow U$ und folgt dann mit 9.2.7 im allgemeinen. Speziell ist die Transponierte einer Injektion eine Surjektion und die Transponierte einer Surjektion eine Injektion. Wir verallgemeinern diese Argumente nun noch auf den Fall beliebiger exakter Sequenzen von Vektorräumen.

Proposition 9.2.9. *Jede exakte drei-Term-Sequenz von Vektorräumen ist isomorph zu einer direkten Summe von vier exakten Sequenzen der folgenden vier Typen:*

$$\begin{array}{ccccc} U & \to & 0 & \to & 0 \\ V & \xrightarrow{\mathrm{id}} & V & \to & 0 \\ 0 & \to & W & \xrightarrow{\mathrm{id}} & W \\ 0 & \to & 0 & \to & X \end{array}$$

Beweis. Sei $A \xrightarrow{r} B \xrightarrow{s} C$ unsere Sequenz. Nach 1.5.21 besitzt $(\operatorname{im} r) = (\ker s)$ ein Komplement $W \subset B$, und nach 1.6.11 induziert s einen Isomorphismus $W \xrightarrow{\sim} (\operatorname{im} s)$. Nach 1.5.21 besitzt auch $(\ker r)$ ein Komplement $V \subset A$ und nach 1.6.11 induziert r einen Isomorphismus $V \xrightarrow{\sim} (\operatorname{im} r)$. Wählen wir nun noch ein Komplement $X \subset C$ von $(\operatorname{im} s)$, so induziert die Einbettung folglich einen Isomorphismus zwischen unserer ursprünglichen Sequenz und der direkten Summe der vier Sequenzen

$$\begin{array}{ccccc} (\ker r) & \to & 0 & \to & 0 \\ V & \xrightarrow{\sim} & (\operatorname{im} r) & \to & 0 \\ 0 & \to & W & \xrightarrow{\sim} & (\operatorname{im} s) \\ 0 & \to & 0 & \to & X \end{array}$$

Die Proposition folgt unmittelbar. □

Korollar 9.2.10. *Gegeben eine exakte Sequenz $U \xrightarrow{r} V \xrightarrow{s} W$ von Vektorräumen erhalten wir für jeden weiteren Vektorraum L exakte Sequenzen*

$$\begin{array}{ccccc} \mathrm{Hom}(W,L) & \xrightarrow{\circ s} & \mathrm{Hom}(V,L) & \xrightarrow{\circ r} & \mathrm{Hom}(U,L) \\ \mathrm{Hom}(L,U) & \xrightarrow{r\circ} & \mathrm{Hom}(L,V) & \xrightarrow{s\circ} & \mathrm{Hom}(L,W) \end{array}$$

Beweis. Das folgt unmittelbar aus der vorhergehenden Proposition 9.2.9 zusammen mit der Erkenntnis, daß das Bilden des Homomorphismenraums, wie in 1.5.18 und 1.5.19 ausgeführt wird, "mit endlichen direkten Summen vertauscht". □

9.2.11. Nehmen wir in diesem Korollar als L den Grundkörper, so folgt insbesondere, daß jede exakte drei-Term-Sequenz beim Dualisieren wieder eine exakte Sequenz liefert.

9.2.12. Ich gebe nun noch eine Verallgemeinerung des Noether'schen Isomorphiesatzes, die in vielen Anwendungen eine übersichtlichere Argumentation ermöglicht.

Lemma 9.2.13 (Neunerlemma). *Sei gegeben ein Diagramm von Gruppen mit im Sinne von 9.2.2 kurzen exakten Zeilen der Gestalt*

$$\begin{array}{ccccc} A' & \hookrightarrow & A & \twoheadrightarrow & A'' \\ \downarrow & & \downarrow & & \downarrow \\ B' & \hookrightarrow & B & \twoheadrightarrow & B'' \\ \downarrow & & \downarrow & & \downarrow \\ C' & \hookrightarrow & C & \twoheadrightarrow & C'' \end{array}$$

und seien die senkrechten Kompositionen jeweils Null. Sei unser Diagramm **kommutativ** *in dem Sinne, daß alle vier Quadrate "kommutieren", daß also die Komposition $A' \to A \to B$ übereinstimmt mit der Komposition $A' \to B' \to B$ etc. Sind unter diesen Voraussetzungen zwei der Spalten kurze exakte Sequenzen, so auch die Dritte.*

9.2.14. Der folgende Beweis ist ein schönes Beispiel für eine Beweismethode, die als **Diagrammjagd** bekannt ist.

Beweis. Der Beweis ist etwas mühsam, aber nicht schwer. Wir zeigen nur, daß die Exaktheit der beiden linken Spalten die Exaktheit der rechten Spalte impliziert und überlassen die beiden anderen Nachweise dem Leser zur Übung. Die Surjektivität von $B'' \to C''$ folgt, da sich $B \to C''$ als Komposition von zwei Surjektionen schreiben läßt. Der Nachweis der Injektivität von $A'' \to B''$ braucht mehr Arbeit. Geht ein Element $a'' \in A''$ nach 1, so wählen wir ein Urbild $a \in A$ von a'' und sein Bild $b \in B$ geht auch nach 1 in B'' und nach 1 in C. Also gibt es ein Urbild $b' \in B'$ von b und die Urbild geht nach 1 in C und sogar schon in

C'. Dann besitzt aber b' ein Urbild a' in A' und dies a' geht auf unser a unter der oberen linken Horizontale. Daraus folgt dann $a'' = 1$. Geht schließlich $b'' \in B''$ nach $1 \in C''$, so wählen wir ein Urbild $b \in B$ von b'' und dessen Bild $c \in C$ geht auch nach 1 in C'', kommt also von einem $c' \in C'$. Dies c' kommt hinwiederum von einem $b' \in B'$, und bezeichnen wir das Bild von b' in B auch mit b' und betrachten $b(b')^{-1}$, so geht dies Element in B'' wieder nach b'' aber in C nach 1. Wir dürfen also davon ausgehen, daß wir unser $b \in B$ schon von Anfang an so gewählt hätten, daß es in B'' nach b'' geht und in C nach 1. Dann kommt aber b von $a \in A$ und b'' kommt vom Bild a'' von a in A'', was zu zeigen war. □

Übung 9.2.15. Man gebe einen vollständigen Beweis des Neunerlemmas.

Übung 9.2.16. Man folgere den Noether'schen Isomorphiesatz 7.2.14 aus dem Neunerlemma. Man folgere die zweite Aussage von 7.5.5 aus dem Neunerlemma.

Ergänzende Übung 9.2.17 (**Additivität der Spur**). Gegeben ein kommutatives Diagramm von endlichdimensionalen Vektorräumen mit zweimal derselben kurzen exakten Zeile

$$\begin{array}{ccccc} V' & \hookrightarrow & V & \twoheadrightarrow & V'' \\ f'\downarrow & & f\downarrow & & f''\downarrow \\ V' & \hookrightarrow & V & \twoheadrightarrow & V'' \end{array}$$

gilt für die Spuren der Vertikalen die Identität $\operatorname{tr}(f) = \operatorname{tr}(f') + \operatorname{tr}(f'')$. Allgemeiner hat im Fall beliebiger Vektorräume der Homomorphismus f endlichen Rang genau dann, wenn f' und f'' endlichen Rang haben, und unter dieser Voraussetzung gilt für die Spuren der Vertikalen auch wieder die Identität $\operatorname{tr}(f) = \operatorname{tr}(f') + \operatorname{tr}(f'')$.

9.3 Tensorprodukte von Vektorräumen

9.3.1. Gegeben eine Menge X und ein Körper k hatten wir in 1.3.21 den freien Vektorraum $k\langle X\rangle$ über X eingeführt durch die Vorschrift

$$k\langle X\rangle = \left\{ f : X \to k \;\middle|\; \begin{array}{l} f \text{ nimmt nur an endlich vielen Stellen} \\ x \in X \text{ einen Wert ungleich Null an.} \end{array} \right\}$$

Wir hatten weiter in 1.5.15 die kanonische Abbildung $\operatorname{can} : X \to k\langle X\rangle$ eingeführt, die jedem $x \in X$ diejenige Funktion zuordnet, die Eins ist an der Stelle x und Null sonst. Oft kürzen wir im folgenden $\operatorname{can}(x)$ schlicht mit x ab. Schließlich hatten wir in 1.5.16 die universelle Eigenschaft freier Vektorräume diskutiert, nach der es für jeden k-Vektorraum V und jede Abbildung $f : X \to V$ genau eine k-lineare Abbildung $\tilde{f} : k\langle X\rangle \to V$ gibt mit $\tilde{f} \circ \operatorname{can} = f$. In anderen Worten liefert also für jeden k-Vektorraum V und jede Menge X das Vorschalten der

kanonischen Einbettung eine Bijektion

$$\mathrm{Hom}_k(k\langle X\rangle, V) \overset{\circ\,\mathrm{can}}{\xrightarrow{\sim}} \mathrm{Ens}(X, V)$$

Definition 9.3.2. Sind V und W zwei Vektorräume über einem Körper k, so definieren wir einen weiteren k-Vektorraum $V \otimes W = V \otimes_k W$, das **Tensorprodukt** von V und W, mitsamt einer k-bilinearen Abbildung

$$\begin{array}{rccc} \tau: & V \times W & \to & V \otimes W \\ & (v, w) & \mapsto & v \otimes w \end{array}$$

wie folgt: Wir betrachten die Menge $V \times W$, darüber den freien k-Vektorraum $k\langle V \times W\rangle$, und darin den Untervektorraum $U \subset k\langle V \times W\rangle$, der erzeugt wird von allen Ausdrücken

$$\begin{array}{l} (v + v', w) - (v, w) - (v', w) \\ (\lambda v, w) - \lambda(v, w) \\ (v, w + w') - (v, w) - (v, w') \\ (v, \lambda w) - \lambda(v, w) \end{array}$$

für $v, v' \in V$, $w, w' \in W$ und $\lambda \in k$. Dann definieren wir unser Tensorprodukt als den Quotientenvektorraum

$$V \otimes W := k\langle V \times W\rangle / U$$

und erklären $v \otimes w$ als die Nebenklasse von (v, w). Die Bilinearität von $(v, w) \mapsto v \otimes w$ folgt hierbei unmittelbar aus der Definition des herausgeteilten Untervektorraums U.

9.3.3. In 2.7.2 haben wir bereits das Tensorprodukt mit eindimensionalen Räumen diskutiert und wir werden bald zeigen, daß die hier gegebene Konstruktion in diesem Fall "im Wesentlichen dasselbe" liefert. Ich fürchte, daß die hier für den allgemeinen Fall gegebene Definition auf den ersten Blick wenig überzeugend wirken mag: Schon im Fall des Tensorprodukts von zwei eindimensionalen reellen Vektorräumen $\mathbb{R} \otimes_{\mathbb{R}} \mathbb{R}$ erhalten wir den Quotienten des freien $\mathbb{R}$-Vektorraums über der Menge $\mathbb{R} \times \mathbb{R}$, mithin den Quotienten eines reellen Vektorraums überabzählbarer Dimension, nach einem wenig unübersichtlich definierten Teilraum. Für diesen Teilraum ist a priori noch nicht einmal klar, daß er nicht mit dem Raum selbst zusammenfällt, so daß unser Tensorprodukt Null wäre. Noch viel weniger klar ist, daß er die Kodimension Eins hat, so daß sich als $\mathbb{R} \otimes_{\mathbb{R}} \mathbb{R}$ schlicht wieder ein eindimensionaler reeller Vektorraum entpuppt. Unter diesem Blickwinkel betrachtet ist die vorstehende Definition ungeschickt, und man mag eine "Definition durch die universelle Eigenschaft" vorziehen, wie sie in 9.3.5 diskutiert wird. Eine solche Definition wäre zwar sehr viel natürlicher, hätte aber hinwiederum den Nachteil, daß sie recht eigentlich gar nicht einen wohlbestimmten Vektorraum liefert,

sondern vielmehr nur einen "bis auf eindeutigen Isomorphismus wohlbestimmten Vektorraum". Mit derartigen Objekten wird der Leser intuitiv schon richtig umzugehen wissen, aber wir müßten dafür doch entweder unsere Spielregeln ändern oder den begrifflichen Rahmen der sogenannten "Kategorientheorie" aufbauen, in dem die präzise Formulierung des Konzepts eines "bis auf eindeutigen Isomorphismus wohlbestimmten Vektorraums" erst übersichtlich und handhabbar wird. Ich vermute fast, daß sich das Wesen und die Sinnhaftigkeit unserer Konstruktionen erst im Rahmen der Kategorientheorie voll erschließen läßt, vergleiche etwa 10.2.11.

Satz 9.3.4 (Universelle Eigenschaft des Tensorprodukts). *Gegeben ein Körper k, Vektorräume V, W, L über k und eine k-bilineare Abbildung $b : V \times W \to L$ existiert genau eine k-lineare Abbildung $\hat{b} : V \otimes W \to L$ mit $b(v, w) = \hat{b}(v \otimes w) \quad \forall v \in V, w \in W$. In Formeln liefert also das Vorschalten der kanonischen Abbildung $\tau : V \times W \to V \otimes W$ eine Bijektion*

$$\mathrm{Hom}_k(V \otimes W, L) \overset{\circ\tau}{\tilde{\to}} \mathrm{Hom}_k^{(2)}(V \times W, L)$$

Beweis. Wir arbeiten mit dem Diagramm

$$\begin{array}{ccccc} V \times W & \longrightarrow & k(V \times W) & \longrightarrow & V \otimes W \\ & \searrow & \downarrow & \swarrow & \\ & & L & & \end{array}$$

Für jede Abbildung $b : V \times W \to L$ gibt es nach 9.3.1 genau eine k-lineare Abbildung $\tilde{b} : k(V \times W) \to L$ mit $\tilde{b} \circ \mathrm{can} = b$. Ist b bilinear, so gilt offensichtlich $\tilde{b}(U) = 0$, also gibt es $\hat{b} : V \otimes W \to L$ linear mit $\hat{b}(v \otimes w) = b(v, w)$. Diese Abbildung $\hat{b}$ ist eindeutig bestimmt durch b, da die $v \otimes w$ das Tensorprodukt als Vektorraum erzeugen. □

9.3.5. Das Tensorprodukt wird durch seine universelle Eigenschaft bereits bis auf eindeutigen Isomorphismus festgelegt. Seien genauer gegeben ein Körper k, Vektorräume V, W über k und eine k-bilineare Abbildung $c : V \times W \to T$ in einen weiteren k-Vektorraum T mit der Eigenschaft, daß für jede k-bilineare Abbildung $b : V \times W \to L$ in einen k-Vektorraum L genau eine k-lineare Abbildung $\tilde{b} : T \to L$ existiert mit $b(v, w) = \tilde{b}(c(v, w)) \quad \forall v \in V, w \in W$. So ist die Abbildung $\hat{c}$ ein Isomorphismus

$$\hat{c} : V \otimes W \overset{\sim}{\to} T$$

Um das einzusehen, betrachten wir das nebenstehende Diagramm. Notieren wir $\tau : V \times W \to V \otimes W$ unsere kanonische bilineare Abbildung $(v, w) \mapsto v \otimes w$, so ist nämlich $\tilde{\tau}$ invers zu $\hat{c}$. In der Tat gilt $\tilde{\tau} \circ \hat{c} \circ \tau = \tilde{\tau} \circ c = \tau$ und aus der universellen

Illustration zum Beweis der Festlegbarkeit des Tensorprodukts bis auf eindeutigen Isomorphismus durch seine universelle Eigenschaft.

Eigenschaft von τ folgt, daß es nur eine lineare Abbildung $f = \hat{\tau} : V \otimes W \to V \otimes W$ geben darf mit $f \circ \tau = \tau$. Da nun die Identität auf dem Tensorprodukt eine mögliche derartige lineare Abbildung ist, folgt schon einmal $\hat{\tau} = \mathrm{id} = \tilde{\tau} \circ \hat{c}$. Weiter gilt $\hat{c} \circ \tilde{\tau} \circ c = \hat{c} \circ \tau = c$ und aus der universellen Eigenschaft von c folgt, daß es nur eine lineare Abbildung $g = \tilde{c} : T \to T$ geben darf mit $g \circ c = c$. Da nun die Identität auf T eine mögliche derartige lineare Abbildung ist, folgt auch $\tilde{c} = \mathrm{id} = \hat{c} \circ \tilde{\tau}$.

9.3.6. Da es uns eigentlich nur auf die universelle Eigenschaft ankommt, kann man natürlich auch andere Konstruktionen versuchen. Ist V endlichdimensional, so hat auch der Raum $T_1 = \mathrm{Hom}_k(V^\top, W)$ mit der bilinearen Abbildung $c_1 : V \times W \to T_1, (v, w) \mapsto (f \mapsto f(v)w)$ die geforderte universelle Eigenschaft, und ist darüber hinaus auch W endlichdimensional, so gilt dasselbe für das Paar (T_2, c_2) mit $T_2 = \mathrm{Hom}^{(2)}(V^\top \times W^\top, k)$ und $c_2 : (v, w) \mapsto ((f, g) \mapsto f(v)g(w))$. In vielen Quellen wählt man letztere Konstruktion zur Definition des Tensorprodukts, vermutlich mit dem Ziel, diese riesigen freien Vektorräume und das Bilden von Quotienten zu vermeiden. Das geschieht dann aber doch um den Preis einer eingeschränkten Allgemeinheit. Daß es durchaus sinnvoll und nützlich sein kann, auch unendlichdimensionale Vektorräume tensorieren zu können, mögen die Übungen 9.3.18 und 9.3.19 illustrieren.

9.3.7. Ein in der Literatur auch oft beschrittener Zugang, der sogar Tensorprodukte unendlichdimensionaler Räume liefert, geht so: Man wählt Basen $A \subset V$ und $B \subset W$, setzt $T_3 = k\langle A \times B\rangle$ und erklärt die kanonische bilineare Abbildung $c_3 : V \times W \to T_3$ als die eindeutig bestimmte bilineare Abbildung mit $(a, b) \mapsto (a, b)$ für alle $a \in A$ und $b \in B$. Im zweiten Beweis von 9.3.10 führen wir aus, warum auch diese Konstruktion eine bilineare Abbildung mit der das Tensorprodukt charakterisierenden universellen Eigenschaft liefert. Ich mag diesen Zugang weniger aus den folgenden zwei Gründen: Erstens hängt unser so konstruierter Raum T_3 von den gewählten Basen ab, so daß wir nicht eigentlich einen Vektorraum, sondern vielmehr eine durch die möglichen Wahlen von Basen indizierte Familie von paarweise in kanonischer und verträglicher Weise isomorphen Vektorräumen erhalten. Und zweitens läßt sich diese Konstruktion im Gegensatz zu der in diesem Text gewählten Konstruktion nicht unmittelbar zu einer Konstruktion von Tensorprodukten über Ringen **??** verallgemeinern. Tensorprodukte über Ringen spielen jedoch in weiten Teilen der Mathematik eine zentrale Rolle.

9.3.8. Keineswegs jedes Element eines Tensorprodukts ist von der Form $v \otimes w$, die Elemente dieser Gestalt erzeugen jedoch das Tensorprodukt als Vektorraum und sogar als abelsche Gruppe. Besitzt weiter ein von Null verschiedenes Element eines Tensorprodukts eine Darstellung der Gestalt $v \otimes w$, so sind seine möglichen Darstellungen dieser Gestalt genau alle Ausdrücke $\lambda v \otimes \lambda^{-1} w$ mit $\lambda \in k^\times$ einer Einheit des Grundkörpers k. Geben wir eine Abbildung von einem Tensorprodukt

in einen Vektorraum L an durch eine Vorschrift der Gestalt $v \otimes w \mapsto b(v,w)$, so ist der Leser implizit gefordert, die Bilinearität der Abbildung $b : V \times W \to L$ zu prüfen, und gemeint ist dann die durch die universelle Eigenschaft definierte Abbildung $\hat{b} : V \otimes W \to L$.

Definition 9.3.9. Sind $f : V \to V'$ und $g : W \to W'$ lineare Abbildungen, so definieren wir eine lineare Abbildung $f \otimes g : V \otimes W \to V' \otimes W'$ durch die Vorschrift $(f \otimes g)(v \otimes w) := f(v) \otimes g(w)$.

Lemma 9.3.10 (Basen von Tensorprodukten). *Ist $v_1, \ldots, v_n$ eine Basis von V und $w_1, \ldots w_m$ eine Basis von W, so bilden die $v_i \otimes w_j$ eine Basis von $V \otimes W$. Insbesondere gilt im endlichdimensionalen Fall*

$$\dim_k(V \otimes W) = (\dim_k V)(\dim_k W)$$

9.3.11. Dieselbe Aussage gilt mit demselben Beweis auch für nicht notwendig endliche Basen: Sind $A \subset V$ und $B \subset W$ Basen von k-Vektorräumen V und W, so ist die Familie von Tensoren $(a \otimes b)_{(a,b)\in A\times B}$ eine Basis des Tensorprodukts $V \otimes W$.

Erster Beweis. Nur die lineare Unabhängigkeit der $v_i \otimes w_j$ ist nicht auf Anhieb klar. Aber sind $v_1^\top, \ldots, v_n^\top \in V^\top$ und $w_1^\top, \ldots, w_m^\top \in W^\top$ die Vektoren der dualen Basen und betrachten wir die bilinearen Abbildungen

$$\begin{array}{rccc} b_{ij} : & V \times W & \to & k \\ & (v,w) & \mapsto & v_i^\top(v) w_j^\top(w) \end{array}$$

so ist $\hat{b}_{ij} : V \otimes W \to k$ eine lineare Abbildung, die $v_i \otimes w_j$ auf 1 abbildet und alle anderen $v_\nu \otimes w_\mu$ auf Null. □

Zweiter Beweis. Wir führen den zweiten Beweis gleich für den Fall beliebiger Dimension. Sind $A \subset V$ und $B \subset W$ Basen, so liefern nach 1.5.27 und 9.3.1 die Einschränkung bzw. das Vorschalten der kanonischen Einbettung Bijektionen

$$\mathrm{Hom}_k^{(2)}(V \times W, L) \xrightarrow{\sim} \mathrm{Ens}(A \times B, L) \xleftarrow{\sim} \mathrm{Hom}_k(k\langle A \times B\rangle, L)$$

Bezeichnet $c : V \times W \to k\langle A \times B\rangle$ die bilineare Abbildung, die unter diesen Isomorphismen der Identität auf $k\langle A \times B\rangle$ entspricht, so kann man unschwer einsehen, daß c auch die von einem Tensorprodukt geforderte universelle Eigenschaft hat. Dann muß jedoch nach 9.3.5 die durch diese universelle Eigenschaft gegebene Abbildung einen Isomorphismus $\tilde{\tau} : k\langle A \times B\rangle \xrightarrow{\sim} V \otimes W$ liefern, und man prüft leicht, daß dieser Isomorphismus $(a,b) \in k\langle A \times B\rangle$ auf $a \otimes b \in V \otimes W$ abbildet. Aus 1.4.14 folgt dann unmittelbar, daß die $a \otimes b$ eine Basis von $V \otimes W$ bilden. □

9.3.12. An dieser Stelle kann man auch die Beziehung zu unserem Tensorprodukt mit eindimensionalen Räumen aus 2.7.2 bequem sehen: Bezeichnen wir nur an dieser Stelle das in 2.7.2 erklärte Tensorprodukt einmal mit $\tilde{\otimes}$, so liefert die universelle Eigenschaft eine lineare Abbildung $V \otimes L \to V\tilde{\otimes}L$ mit $v \otimes l \mapsto v\tilde{\otimes}l$, und nach 9.3.11 und 2.7.9 liefert diese Abbildung eine Bijektion zwischen Basen der betraffenden Räume und ist folglich ein Isomorphismus.

Ergänzende Übung 9.3.13. Jede exakte Sequenz von Vektorräumen bleibt beim Darantensorieren eines weiteren Vektorraums exakt. Hinweis: 9.2.9, oder 9.3.26 und 7.5.6.

9.3.14. Gegeben Vektorräume V, W mit angeordneten Basen $\mathcal{A} = (v_1, \dots v_n)$ und $\mathcal{B} = (w_1, \dots, w_n)$ bilden wir in $V \otimes W$ die angeordnete Basis

$$\begin{aligned}\mathcal{A} \otimes \mathcal{B} \quad := \quad & (v_1 \otimes w_1, v_1 \otimes w_2, \dots, v_1 \otimes w_m,\\ & v_2 \otimes w_1, v_2 \otimes w_2, \dots, v_2 \otimes w_m,\\ & \qquad \dots \quad \dots \quad \dots\\ & v_n \otimes w_1, v_n \otimes w_2, \dots, v_n \otimes w_m)\end{aligned}$$

Gegeben zusätzlich weitere Vektorräume V', W' mit angeordneten Basen $\mathcal{A}' = (v'_1, \dots, v'_{n'})$ und $\mathcal{B}' = (w'_1, \dots, w'_{m'})$ und lineare Abbildungen $f : V \to V'$ und $g : W \to W'$ können wir die Matrix ${}_{\mathcal{A}'\otimes\mathcal{B}'}[f \otimes g]_{\mathcal{A}\otimes\mathcal{B}}$ von $f \otimes g$ in den Basen $\mathcal{A} \otimes \mathcal{B}$ und $\mathcal{A}' \otimes \mathcal{B}'$ wie folgt durch die Matrizen $A = {}_{\mathcal{A}'}[f]_{\mathcal{A}}$ und $B = {}_{\mathcal{B}'}[g]_{\mathcal{B}}$ ausdrücken: Haben wir etwa $A = (a_{ij})$, so wird

$${}_{\mathcal{A}'\otimes\mathcal{B}'}[f \otimes g]_{\mathcal{A}\otimes\mathcal{B}} \quad = \quad \begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & & \vdots \\ a_{n'1}B & \dots & a_{n'n}B \end{pmatrix}$$

Auf der rechten Seite ist hier die Matrix geblockt geschrieben, es handelt sich ja eigentlich um eine $(n'm' \times nm)$-Matrix. Sie heißt auch das **Kronecker-Produkt** der Matrizen A und B und wird $A \otimes B$ notiert, so daß wir unsere Identität oben also auch schreiben können in der Form

$${}_{\mathcal{A}'\otimes\mathcal{B}'}[f \otimes g]_{\mathcal{A}\otimes\mathcal{B}} = {}_{\mathcal{A}'}[f]_{\mathcal{A}} \otimes {}_{\mathcal{B}'}[g]_{\mathcal{B}}$$

Um diese Identität zu prüfen beginnen wir mit den Identitäten

$$f(v_i) = \sum_j a_{ji}v'_j \quad \text{und} \quad g(w_k) = \sum_l b_{lk}w'_l$$

und folgern

$$(f \otimes g)(w_i \otimes w_k) = \sum_{j,l} a_{ji}b_{lk}v'_j \otimes w'_l$$

Die Einträge der Matrix von $f \otimes g$ sind also alle Produkte von einem Eintrag der Matrix von f mit einem Eintrag der Matrix von g. Daß diese Einträge dann auch noch an den oben beschriebenen Stellen der Matrix von $f \otimes g$ stehen, mag sich der Leser am einfachsten selbst überlegen.

Ergänzende Übung 9.3.15. Gegeben ein Körper k und k-Vektorräume V, W und Endomorphismen $f \in \operatorname{End} V$ und $g \in \operatorname{End} W$ endlichen Ranges hat auch $f \otimes g \in \operatorname{End}(V \otimes W)$ endlichen Rang und es gilt

$$\operatorname{tr}(f \otimes g) = \operatorname{tr}(f) \operatorname{tr}(g)$$

Proposition 9.3.16. *Gegeben Vektorräume U, V, W erhalten wir einen Isomorphismus*

$$\operatorname{Hom}(U, \operatorname{Hom}(V, W)) \xrightarrow{\sim} \operatorname{Hom}(U \otimes V, W)$$

durch die Vorschrift $f \mapsto \tilde{f}$ mit $\tilde{f}(u \otimes v) = (f(u))(v)$.

Beweis. Beide Seiten sind in offensichtlicher und mit der angegebenen Abbildung verträglicher Weise in Bijektion zur Menge $\operatorname{Hom}^{(2)}(U \times V, W)$ aller bilinearen Abbildungen $U \times V \to W$. □

Ergänzende Übung 9.3.17. Für jeden k-Vektorraum V definiert das Auswerten oder lateinisierend "Evaluieren" eine lineare Abbildung $\operatorname{ev} : V^\top \otimes V \to k$, $\xi \otimes v \mapsto \xi(v)$. Man zeige, daß sie unter dem Isomorphismus aus 9.3.16 der Identität auf $V^\top$ entspricht.

Ergänzende Übung 9.3.18. Gegeben ein Körper k induziert die Multiplikation einen Isomorphismus $k[X] \otimes_k k[Y] \xrightarrow{\sim} k[X, Y]$.

Ergänzende Übung 9.3.19. Die Multiplikation induziert einen Isomorphismus von reellen Vektorräumen $\mathbb{R} \otimes_{\mathbb{Q}} \mathbb{Q}[X] \xrightarrow{\sim} \mathbb{R}[X]$. Analoges gilt, wenn man $\mathbb{R} \supset \mathbb{Q}$ ersetzt durch ein beliebiges Paar $K \supset k$ bestehend aus einem Körper mit einem Teilkörper.

Definition 9.3.20. Induktiv bilden wir auch längere Tensorprodukte durch die Vorschrift $V_1 \otimes \ldots \otimes V_{n-1} \otimes V_n := (V_1 \otimes \ldots \otimes V_{n-1}) \otimes V_n$ und definieren darin die Vektoren $v_1 \otimes \ldots \otimes v_n := (v_1 \otimes \ldots \otimes v_{n-1}) \otimes v_n$.

Proposition 9.3.21. *1. Gegeben Vektorräume $V_1, \ldots, V_n$ erhalten wir durch das Tensorieren von Vektoren eine multilineare Abbildung*

$$\begin{array}{rcl} V_1 \times \ldots \times V_n & \to & V_1 \otimes \ldots \otimes V_n \\ (v_1, \ldots, v_n) & \mapsto & v_1 \otimes \ldots \otimes v_n \end{array}$$

2. *Ist L ein weiterer k-Vektorraum und $F : V_1 \times \ldots \times V_n \to L$ eine beliebige multilineare Abbildung, so gibt es genau eine lineare Abbildung $\hat{F} : V_1 \otimes \ldots \otimes V_n \to L$ mit $F(v_1, \ldots, v_n) = \hat{F}(v_1 \otimes \ldots \otimes v_n)$ für alle $v_1 \in V_1, \ldots, v_n \in V_n$.*

9.3.22. Damit diese Proposition auch im Fall $n = 0$ gilt, vereinbaren wir für das Tensorprodukt mit überhaupt keinem Faktor, daß damit schlicht der Grundkörper gemeint sein soll, und als kanonische multilineare Abbildung des kartesischen Produkts von Vektorräumen mit überhaupt keinem Faktor, das ja nach unseren Konventionen "die" einpunktige Menge ist, in sein Tensorprodukt vereinbaren wir die Abbildung, die diesen einzigen Punkt auf $1 \in k$ wirft.

Beweis. Mit Induktion über n. Wir argumentieren mit dem Diagramm

$$\begin{array}{ccccc} V_1 \times \ldots \times V_n & \longrightarrow & (V_1 \otimes \ldots \otimes V_{n-1}) \times V_n & \longrightarrow & V_1 \otimes \ldots \otimes V_n \\ & \searrow & \downarrow & \swarrow & \\ & & L & & \end{array}$$

mit hoffentlich offensichtlichen horizontalen Morphismen. Wir zeigen nur die Existenz von $\hat{F}$ und überlassen den Nachweis der anderen Behauptungen dem Leser. Für jedes feste $v_n \in V_n$ ist die Abbildung $(v_1, \ldots, v_{n-1}) \mapsto F(v_1, \ldots, v_n)$ multilinear und induziert so nach Induktionsannahme eine lineare Abbildung $V_1 \otimes \ldots \otimes V_{n-1} \to L$. Das liefert die mittlere Vertikale. Man überzeugt sich nun leicht, daß die mittlere Vertikale auch in $v_n \in V_n$ linear sein muß. Als bilineare Abbildung faktorisiert sie also über $V_1 \otimes \ldots \otimes V_n$. □

Proposition 9.3.23. *1. Sind V, W Vektorräume, so so liefert die Abbildungsvorschrift $v \otimes w \mapsto w \otimes v$ einen Isomorphismus*

$$V \otimes W \xrightarrow{\sim} W \otimes V$$

2. *Sind $V_1, \ldots, V_p, V_{p+1}, \ldots, V_n$ Vektorräume, so liefert die Abbildungsvorschrift $v_1 \otimes \ldots \otimes v_p \otimes v_{p+1} \otimes \ldots \otimes v_n \mapsto (v_1 \otimes \ldots \otimes v_p) \otimes (v_{p+1} \otimes \ldots \otimes v_n)$ einen Isomorphismus*

$$V_1 \otimes \ldots \otimes V_p \otimes V_{p+1} \otimes \ldots \otimes V_n \xrightarrow{\sim} (V_1 \otimes \ldots \otimes V_p) \otimes (V_{p+1} \otimes \ldots \otimes V_n)$$

3. *Die Abbildung $\lambda \otimes v \mapsto \lambda v$ liefert einen Isomorphismus*

$$k \otimes V \xrightarrow{\sim} V$$

vom Tensorprodukt des Grundkörpers mit einem Vektorraum in besagten Vektorraum selber. Analoges gilt für den zweiten Tensorfaktor.

4. *Gegeben Vektorräume W, V, V' liefert $w \otimes (v, v') \mapsto (w \otimes v, w \otimes v')$ einen Isomorphismus*

$$W \otimes (V \oplus V') \xrightarrow{\sim} (W \otimes V) \oplus (W \otimes V')$$

Analoges gilt auch für den ersten Tensorfaktor.

9.3.24. Die Abbildungsvorschrift in Teil 2 ist analog zu unserer Vereinbarung 9.3.8 zu lesen als diejenige lineare Abbildung, über die die multilineare Abbildung $(v_1, \ldots, v_p, v_{p+1}, \ldots, v_n) \mapsto (v_1 \otimes \ldots \otimes v_p) \otimes (v_{p+1} \otimes \ldots \otimes v_n)$ im Sinne von 9.3.21 faktorisiert.

Beweis. Man kann in allen diesen Fällen leicht einsehen, daß die betrachteten Abbildungen eine geeignete Basis des Ausgangsraums bijektiv mit einer Basis des Zielraums identifizieren. Die Details seien dem Leser überlassen. □

Bemerkung 9.3.25. In gewisser Weise liefert das die Kommutativität, Assoziativität und das neutrale Element für das Tensorprodukt, nebst der Distributivität mit direkten Summen. In größerer Abstraktion formalisiert das der Formalismus der "Tensorkategorie", wie er in **??** diskutiert wird.

Ergänzende Übung 9.3.26. Gegeben ein Vektorraum V und eine Familie von Vektorräumen $(W_i)_{i \in I}$ liefert die kanonische Abbildung stets einen Isomorphismus

$$V \otimes \left(\bigoplus W_i \right) \xrightarrow{\sim} \bigoplus (V \otimes W_i)$$

Analoges gilt für den anderen Tensorfaktor.

Ergänzende Übung 9.3.27. Gegeben Körper $k \subset K$ und ein k-Vektorraum V wird $V_K = K \otimes_k V$ in offensichtlicher Weise ein K-Vektorraum. Man sagt, er entstehe aus V durch **Erweiterung der Skalare**. Die "kanonische" k-lineare Abbildung $\mathrm{can} : V \to V_K$, $v \mapsto 1 \otimes v$ hat dann die universelle Eigenschaft, daß für jeden K-Vektorraum W das Vorschalten von can eine Bijektion

$$\mathrm{Hom}_K(V_K, W) \xrightarrow{\sim} \mathrm{Hom}_k(V, W)$$

liefert. Weiter ist das Bild unter can jeder k-Basis von V eine K-Basis von V_K, und gegeben ein weiterer k-Vektorraum W induziert die k-lineare Abbildung $V \otimes_k W \to V_K \otimes_K W_K$, $v \otimes w \mapsto \mathrm{can}(v) \otimes \mathrm{can}(w)$ einen Isomorphismus

$$(V \otimes_k W)_K \xrightarrow{\sim} V_K \otimes_K W_K$$

Ist V oder K endlichdimensional über k, so liefert auch die k-lineare Abbildung $\mathrm{Hom}_k(V, W) \to \mathrm{Hom}_K(V_K, W_K)$ gegeben durch $f \mapsto \mathrm{id} \otimes f$ einen Isomorphismus

$$(\mathrm{Hom}_k(V, W))_K \xrightarrow{\sim} \mathrm{Hom}_K(V_K, W_K)$$

und insbesondere "vertauscht das Erweitern der Skalare mit dem Bilden des Dualraums" sowohl unter der Annahme $\dim_k K < \infty$ als auch unter der Annahme $\dim_k V < \infty$. In voller Allgemeinheit vertauschen diese Operationen jedoch nicht. Im Spezialfall $\mathbb{R} \subset \mathbb{C}$ bezeichnet man $V_{\mathbb{C}}$ als die **Komplexifizierung** von V.

Ergänzung 9.3.28. Ein alternativer vom Tensorprodukt unabhängiger Zugang zur Komplexifizierung wird in **??** erklärt. Etwas allgemeiner können wir, nun wieder mit unserem Tensorprodukt, für jeden Körperhomomorphismus $\varphi : k \hookrightarrow K$ zu einem k-Vektorraum V den k-Vektorraum $K \otimes_k^\varphi V$ erklären. Ist speziell $\varphi : \mathbb{C} \to \mathbb{C}$ die komplexe Konjugation, so erhalten wir einen Isomorphismus $\mathbb{C} \otimes_{\mathbb{C}}^{\varphi} V \xrightarrow{\sim} \overline{V}$ mit unserem komplex konjugierten Vektorraum $\overline{V}$ aus 4.6.14 vermittels der Abbildungsvorschrift $1 \otimes v \mapsto \bar{v}$.

9.4 Kanonische Injektionen bei Tensorprodukten

Satz 9.4.1 (Homomorphismenräume als Tensorprodukt). *Für beliebig vorgegebene k-Vektorräume V, W liefert die Vorschrift $f \otimes w \mapsto (v \mapsto f(v)w)$ eine Injektion*

$$\text{can} : V^\top \otimes W \hookrightarrow \text{Hom}(V, W)$$

Sind V oder W endlichdimensional, so ist diese Injektion ein Isomorphismus. Im allgemeinen besteht ihr Bild genau aus allen Homomorphismen endlichen Ranges.

9.4.2. Ist $v_1, \ldots, v_n \in V$ eine Basis von V und $v_1^\top, \ldots, v_n^\top \in V^\top$ die duale Basis von $V^\top$, so können wir im Satz die inverse Abbildung explizit angeben durch die Vorschrift $f \mapsto v_1^\top \otimes f(v_1) + \ldots + v_n^\top \otimes f(v_n)$. Ist zusätzlich $w_1, \ldots, w_m$ eine Basis von W, so wird $v_i^\top \otimes w_j$ abgebildet auf diejenige lineare Abbildung, deren Matrix in Bezug auf die gegebenen Basen die Basismatrix E_{ji} aus 1.9.3 ist. Im Fall endlichdimensionaler Räume kann der Satz also leicht mit Basen überprüft werden. Der Beweis gilt den unendlichdimensionalen Fällen.

Beweis. Im Fall $W = k$ liefert die Abbildung des Satzes offensichtlich eine Bijektion. Da beide Seiten mit endlichen direkten Summen vertauschen, folgt die Bijektivität im Fall $\dim W < \infty$. Nun betrachten wir für alle endlichdimensionalen Teilräume $W_1 \subset W$ das kommutative Diagramm

$$\begin{array}{rccc} \text{can}: & V^\top \otimes W & \to & \text{Hom}(V, W) \\ & \uparrow & & \uparrow \\ \text{can}: & V^\top \otimes W_1 & \xrightarrow{\sim} & \text{Hom}(V, W_1) \end{array}$$

mit den offensichtlichen Injektionen in den Vertikalen. Es zeigt, daß alle Abbildungen endlichen Ranges im Bild liegen. Da jeder Tensor $t \in V^\top \otimes W$ nun nach

9.3.8 bereits für einen geeigneten endlichdimensionalen Teilraum $W_1 \subset W$ im Bild von $V^\top \otimes W_1$ liegt, zeigt es auch die Injektivität der oberen Horizontalen und zeigt zusätzlich, daß alle Abbildungen im Bild endlichen Rang haben. □

Ergänzende Übung 9.4.3. Gegeben ein Vektorraum V und eine Teilmenge $T \subset V$ setzen wir $T^\perp = \{f \in V^\top \mid f(t) = 0 \quad \forall t \in T\}$. Ist V endlichdimensional und $W \subset V$ ein Teilraum, so zeige man, daß unter der Identifikation $\operatorname{End} V \xrightarrow{\sim} V \otimes V^\top$ die Identität id_V stets im Teilraum $W \otimes V^\top + V \otimes W^\perp$ landet.

Übung 9.4.4. Gegeben Vektorräume U, V, W kommutiert das Diagramm

$$\begin{array}{ccc} U^\top \otimes V \otimes V^\top \otimes W & \hookrightarrow & \operatorname{Hom}(U,V) \otimes \operatorname{Hom}(V,W) \\ \downarrow & & \downarrow \\ U^\top \otimes W & \hookrightarrow & \operatorname{Hom}(U,W) \end{array}$$

mit den von den kanonischen Injektionen 9.4.1 induzierten Horizontalen, dem Verknüpfen von linearen Abbildungen als rechter Vertikale, und in der linken Vertikalen der Verknüpfung

$$U^\top \otimes V \otimes V^\top \otimes W \to U^\top \otimes k \otimes W \xrightarrow{\sim} U^\top \otimes W$$

der vom Auswerten $\mathrm{id} \otimes \mathrm{ev} \otimes \mathrm{id}$ induzierten Abbildung gefolgt vom Isomorphismus $U^\top \otimes k \otimes W \xrightarrow{\sim} U^\top \otimes W$, $f \otimes \lambda \otimes w \mapsto \lambda(f \otimes w)$. Die eben erklärte Abbildung in der linken Vertikalen bezeichnet man in dieser und ähnlichen Situationen auch als die **Verjüngung von Tensoren**.

Ergänzende Übung 9.4.5. Gegeben ein endlichdimensionaler k-Vektorraum V kommutiert das Diagramm

$$\begin{array}{ccccc} \sum_{i=1}^n v_i \otimes v_i^\top & \in & V \otimes V^\top & \xrightarrow{\mathrm{ev}} & k \\ \downarrow & & \downarrow \wr & & \| \\ \mathrm{id} & \in & \operatorname{End} V & \xrightarrow{\mathrm{tr}} & k \end{array}$$

wo $v_1, \ldots, v_n$ eine beliebige Basis von V bedeuten möge und $v_1^\top, \ldots, v_n^\top$ die duale Basis von $V^\top$ meint und die mittlere Vertikale die in 9.4.1 erklärte Injektion und ev das Auswerten im Sinne von 9.3.17. Hat V unendliche Dimension, so kommutiert das rechte Quadrat immer noch, wenn wir unten links nur Endomorphismen endlichen Ranges betrachten und ihre Spur wie in 1.10.18 nehmen. Allerdings ist dann unser Tensorausdruck nicht mehr sinnvoll definiert und die Identität gehört auch nicht mehr zu den Endomorphismen endlichen Ranges.

Korollar 9.4.6 (Tensorprodukt und Dualität). *Gegeben Vektorräume V, W liefert die Abbildung $f \otimes g \mapsto (v \otimes w \mapsto f(v)g(w))$ eine Injektion*

$$V^\top \otimes W^\top \hookrightarrow (V \otimes W)^\top$$

vom Tensorprodukt der Dualräume in den Dualraum des Tensorprodukts. Sie ist ein Isomorphismus genau dann, wenn einer unserer beiden Räume endlichdimensional ist.

9.4.7. Im Fall endlichdimensionaler Räume kann das Korollar leicht mit Basen überprüft werden. Der Beweis gilt den unendlichdimensionalen Fällen.

Beweis. Wir argumentieren mit dem Diagramm

$$\begin{array}{ccc} (V\otimes W)^\top & = & \mathrm{Hom}(V\otimes W,k) \\ & & \uparrow\wr \\ & & \mathrm{Hom}(V,\mathrm{Hom}(W,k)) \\ & & \| \\ V^\top\otimes W^\top & \hookrightarrow & \mathrm{Hom}(V,W^\top) \end{array}$$

Der vertikale Isomorphismus kommt aus 9.3.16, die horizontale Injektion aus 9.4.1. Daß deren Komposition genau die im Korollar beschriebene Abbildung ist, mag der Leser selbst prüfen. □

Ergänzende Übung 9.4.8. Gegeben Mengen X, Y und ein beliebiger Körper k liefert die offensichtliche Abbildung $f \otimes g \mapsto f \boxtimes g$ gegeben durch die Vorschrift $(f \boxtimes g)(x, y) := f(x)g(y)$ eine Injektion

$$\mathrm{Ens}(X, k) \otimes \mathrm{Ens}(Y, k) \hookrightarrow \mathrm{Ens}(X \times Y, k)$$

Man mag sich dazu auf 9.4.6 stützen, oder auch unabhängig zeigen, daß für $g_1, \ldots, g_n \in \mathrm{Ens}(Y, k)$ linear unabhängig und $f_1, \ldots, f_n \in \mathrm{Ens}(X, k)$ beliebig aus $\sum f_i(x)g_i(y) = 0$ für alle x, y bereits folgt, daß alle f_i die Nullfunktion sein müssen.

Ergänzende Übung 9.4.9. Gegeben ein Vektorraum V und eine Familie von Vektorräumen $(W_i)_{i\in I}$ und liefert die kanonische Abbildung stets eine Injektion

$$V \otimes \left(\prod W_i\right) \hookrightarrow \prod (V \otimes W_i)$$

die jedoch im allgemeinen kein Isomorphismus ist. Genauer ist sie nur ein Isomorphismus, wenn entweder V endlichdimensional ist oder wenn nur für endlich viele i der zugehörige Vektorraum W_i von Null verschieden ist. Hinweis: Man folgere aus 9.4.1 die Injektivität der Komposition $V \otimes W \to V^{**} \otimes W \to \mathrm{Hom}(V^\top, W)$ und bette beide Seiten verträglich ein in $\prod \mathrm{Hom}(V^\top, W_i) \cong \mathrm{Hom}(V^\top, \prod W_i)$.

Ergänzende Übung 9.4.10. Gegeben Vektorräume V, V', W, W' liefert das Tensorieren von Abbildungen eine Injektion

$$\mathrm{Hom}(V, V') \otimes \mathrm{Hom}(W, W') \hookrightarrow \mathrm{Hom}(V \otimes W, V' \otimes W')$$

Hinweis: Man mag V und W als direkte Summe eindimensionaler Räume schreiben und 9.4.9 anwenden. Alternative: Man mag ohne Beschränkung der Allgemeinheit annehmen, daß unsere Vektorräume frei sind über den Mengen X, X', Y, Y', und kann dann unter Verwendung von 9.4.8 beide Seiten in verträglicher Weise einbetten in den Raum $\mathrm{Ens}(X \times X' \times Y \times Y', k)$ aller Abbildungen von besagtem Produkt in den Grundkörper k.

9.5 Alternierende Tensoren und äußere Potenzen

9.5.1 (**Tensorpotenzen**). Gegeben ein Körper k und ein k-Vektorraum V und eine natürliche Zahl $r \in \mathbb{N}$ vereinbaren wir

$$V^{\otimes r} := \underbrace{V \otimes \ldots \otimes V}_{r \text{ Faktoren}}$$

und verstehen $V^{\otimes 0} := k$ im Sinne der vorhergehenden Bemerkung 9.3.22. Gegeben eine lineare Abbildung $f : V \to W$ verwenden wir weiter die Abkürzung $f^{\otimes r} := (f \otimes \ldots \otimes f) : V^{\otimes r} \to W^{\otimes r}$. Gegeben $v \in V$ schreiben wir kurz $v^{\otimes r} := (v \otimes \ldots \otimes v)$ für das Bild von $(v, \ldots, v)$ unter der kanonischen multilinearen Abbildung $V^{\times r} \to V^{\otimes r}$ und verstehen insbesondere $v^{\otimes 0} := 1 \in k$.

Ergänzung 9.5.2 (**Negative Tensorpotenzen im eindimensionalen Fall**). Im Fall eines eindimensionalen Vektorraums V über einem Körper k erklären wir die r-te Tensorpotenz von V sogar für alle $r \in \mathbb{Z}$, indem wir unsere Definition 9.5.1 für nichtnegative Tensorpotenzen ergänzen durch die Vorschrift, daß negative Tensorpotenzen zu verstehen sein mögen als die entsprechenden positiven Potenzen des Dualraums, in Formeln

$$V^{\otimes r} := (V^\top)^{\otimes(-r)} \quad \text{für } r < 0.$$

Erklären wir dann weiter für jedes $v \in V \backslash 0$ und $r < 0$ den Vektor $v^{\otimes r} \in V^{\otimes r}$ als $v^{\otimes r} := (v^\top)^{\otimes r}$ mit $v^\top \in V^\top$ definiert durch $v^\top(v) = 1$, so gibt es für beliebige $r, s \in \mathbb{Z}$ eindeutig bestimmte Isomorphismen

$$V^{\otimes r} \otimes V^{\otimes s} \xrightarrow{\sim} V^{\otimes(r+s)}$$

mit der Eigenschaft $v^{\otimes r} \otimes v^{\otimes s} \mapsto v^{\otimes(r+s)}$ für alle $v \in V \backslash 0$.

9.5.3 (**Äußere Potenzen und alternierende Multilinearformen**). Ich erinnere daran, daß wir in 3.3.6 die Determinante

$$\det : \mathrm{M}(n \times n; k) \to k$$

charakterisiert hatten als die eindeutig bestimmte multilineare alternierende Funktion der Spaltenvektoren, die der Einheitsmatrix die Eins zuordnet. Gegeben ein beliebiger k-Vektorraum V und $r \geq 0$ setzen wir nun wie in **??**

$$\mathrm{Alt}^r(V) := \{f : \underbrace{V \times \ldots \times V}_{r \text{ Faktoren}} \to k \mid f \text{ ist multilinear und alternierend}\}$$

Im Spezialfall $r = 0$ ist das leere Produkt als einpunktige Menge zu verstehen und $\mathrm{Alt}^0(V)$ als die Menge aller "0-multilinearen" alias beliebigen Abbildungen von dieser einpunktigen Menge nach k, so daß das Auswerten auf diesem einzigen Punkt einen kanonischen Isomorphismus $\mathrm{Alt}^0(V) \xrightarrow{\sim} k$ definiert. Wir fassen diesen Isomorphismus in unserer Notation hinfort als Gleichheit $\mathrm{Alt}^0(V) = k$ auf. Bezeichnet $J_r \subset V^{\otimes r}$ das Erzeugnis aller Tensoren mit zwei gleichen Einträgen, so liefert das Vorschalten der Verknüpfung $V \times \ldots \times V \to V^{\otimes r} \twoheadrightarrow V^{\otimes r}/J_r$ der kanonischen multilinearen Abbildung mit der kanonischen Abbildung auf den Quotienten aufgrund der universellen Eigenschaften 9.3.21 und 9.1.2 Isomorphismen

$$\mathrm{Alt}^r(V) \quad \xleftarrow{\sim} \quad \{g \in \mathrm{Hom}(V^{\otimes r}, k) \mid g(J_r) = 0\} \quad \xleftarrow{\sim} \quad \mathrm{Hom}(V^{\otimes r}/J_r, k)$$

Der Quotient $V^{\otimes r}/J_r$ heißt die r**-te äußere Potenz von** V und wird für gewöhnlich

$$\bigwedge^r V := V^{\otimes r}/J_r$$

notiert. Mit dieser Notation haben wir also einen kanonischen Isomorphismus $(\bigwedge^r V)^\top \xrightarrow{\sim} \mathrm{Alt}^r(V)$ erhalten. Im Extremfall $r = 0$ verstehen wir hier wieder $V^{\otimes 0} = \bigwedge^0 V = k$ und unsere Aussage behält ihre Gültigkeit.

Ergänzende Übung 9.5.4. Das Erzeugnis $J_r \subset V^{\otimes r}$ aller Tensoren mit zwei gleichen Einträgen fällt zusammen mit dem Erzeugnis $J'_r \subset V^{\otimes r}$ aller Tensoren mit zwei benachbarten gleichen Einträgen.

9.5.5. Gegeben $r, s \geq 0$ gibt es genau eine Abbildung

$$\bigwedge^r V \times \bigwedge^s V \quad \to \quad \bigwedge^{r+s} V$$

derart, daß mit dem Zusammentensorieren von Tensoren in der oberen Horizontale und besagter Abbildung in der unteren Horizontale das Diagramm

$$\begin{array}{ccc} V^{\otimes r} \times V^{\otimes s} & \longrightarrow & V^{\otimes (r+s)} \\ \downarrow & & \downarrow \\ \bigwedge^r V \times \bigwedge^s V & \longrightarrow & \bigwedge^{r+s} V \end{array}$$

kommutiert. Man folgert das unschwer aus Übung 9.1.8, da die obere Horizontale unseres Diagramms sowohl $J_r \times V^{\otimes s}$ als auch $V^{\otimes r} \times J_s$ auf Teilmengen von J_{r+s} abbildet. Unsere so konstruierte Abbildung $\bigwedge^r V \times \bigwedge^s V \to \bigwedge^{r+s} V$ ist offensichtlich bilinear. Sie wird $(\omega, \eta) \mapsto \omega \wedge \eta$ notiert und heißt das **Dachprodukt**, englisch **wedge-product**, französisch **produit extérieur**. Aus der Konstruktion ergibt sich unmittelbar seine Assoziativität, in $\bigwedge^{r+s+t} V$ gilt also

$$(\omega \wedge \eta) \wedge \xi = \omega \wedge (\eta \wedge \xi)$$

für alle $\omega \in \bigwedge^r V$, $\eta \in \bigwedge^s V$ und $\xi \in \bigwedge^t V$. Die direkte Summe

$$\bigwedge V = \bigoplus_{r \geq 0} \bigwedge^r V$$

wird mit dem komponentenweisen Dachprodukt insbesondere ein Ring mit Eins-Element $1 \in k = \bigwedge^0 V$.

9.5.6. Ganz allgemein bezeichnet man einen k-Vektorraum A mit einer bilinearen Verknüpfung $A \times A \to A$ als eine **k-Algebra** und versteht unter einem **Algebrenhomomorphismus** in eine weitere k-Algebra eine k-lineare Abbildung, die mit den jeweiligen Verknüpfungen verträglich ist. Ist die Verknüpfung einer Algebra assoziativ, so spricht man von einer **assoziativen Algebra**. Gibt es für diese Verknüpfung ein neutrales Element, so spricht man von einer **unitären Algebra** und nennt das fragliche Element das **Eins-Element**. Eine Algebra ist also genau dann assoziativ und unitär, wenn die zugrundeliegende Menge mit der Vektorraum-Addition als Addition und der bilinearen Verknüpfung als Multiplikation ein Ring ist. Ich schlage deshalb vor, derartige Algebren **Ringalgebren** und im Fall, daß sie auch noch kommutativ sind, **Kringalgebren** zu nennen. Unter einem **Homomorphismus von Ringalgebren** verstehen wir dann einen Algebrenhomomorphismus, der auch ein Ringhomomorphismus ist. Wir können diese Abbildungen sowohl charakterisieren als Algebrenhomomorphismen, die das Einselement auf das Einselement werfen, als auch als Ringhomomorphismen, die über dem Grundkörper linear sind. Wir vereinbaren für die Menge der Ringalgebrenhomomorphismen von einer k-Ringalgebra A in eine k-Ringalgebra B die Notation $\mathrm{Ralg}_k(A, B)$.

9.5.7. Eine **Unteralgebra** einer Algebra ist ein unter der Verknüpfung stabiler Untervektorraum. Eine **Unterringalgebra** einer Ringalgebra ist dahingegen ein unter der Verknüpfung stabiler Untervektorraum, der das Eins-Element enthält. Beide Begriffsbildungen ordnen sich der allgemeinen wenn auch etwas vagen Begriffsbildung 1.3.13 eines “Unterdings” unter.

9.5.8. In dieser Terminologie ist unser $\bigwedge V$ aus 9.5.5 eine Ringalgebra. Sie heißt die **äußere Algebra** oder auch **Graßmann-Algebra** des Vektorraums V. Die offensichtliche Identifikation $V \xrightarrow{\sim} \bigwedge^1 V$ notieren wir kurzerhand $v \mapsto v$ und behandeln sie auch sprachlich als Gleichheit. Gegeben $v \in V$ gilt in $\bigwedge^2 V$ wegen $v \otimes v \in J_2$ natürlich $v \wedge v = 0$. Mit 3.3.2 folgt daraus

$$v \wedge w = -w \wedge v \quad \forall v, w \in V$$

Ergänzung 9.5.9. Sei V ein Vektorraum über einem Körper k. Eine weitere Ringalgebra, die man jedem k-Vektorraum in natürlicher Weise zuordnen kann, ist die sogenannte **Tensoralgebra** $\mathrm{T}_k V$ **über** V. Sie ist definiert als

$$T(V) = \mathrm{T}_k V = \bigoplus_{r \geq 0} V^{\otimes r} = k \oplus V \oplus (V \otimes V) \oplus (V \otimes V \otimes V) \oplus \dots$$

mit der k-bilinearen Multiplikation, die festgelegt wird durch die Vorschrift $(v_1 \otimes \dots \otimes v_r) \cdot (w_1 \otimes \dots \otimes w_t) = (v_1 \otimes \dots v_r \otimes w_1 \otimes \dots w_t)$. Für die k-lineare Einbettung $\mathrm{can} : V \hookrightarrow \mathrm{T}_k V$ des zweiten Summanden gilt dabei die folgende universelle Eigenschaft: Ist A eine k-Ringalgebra und $\varphi : V \to A$ eine k-lineare Abbildung, so gibt es genau einen Homomorphismus von k-Ringalgebren $\hat{\varphi} : \mathrm{T}_k V \to A$ mit $\varphi = \hat{\varphi} \circ \mathrm{can}$, im Diagramm

$$\begin{array}{ccc} V & \xrightarrow{\mathrm{can}} & \mathrm{T}_k V \\ & \searrow^{\varphi} & \downarrow{\scriptstyle \hat{\varphi}} \\ & & A \end{array}$$

In der Tat sieht man leicht, daß die Vorschrift $\hat{\varphi}(v_1 \otimes \dots \otimes v_r) = \varphi(v_1) \dots \varphi(v_r)$ das einzig mögliche $\hat{\varphi}$ liefert.

Ergänzung 9.5.10. Es gibt noch eine weitere k-Ringalgebra, die man jedem k-Vektorraum V in natürlicher Weise zuordnen kann. Diese sogenannte "symmetrische Algebra" SV diskutieren wir in **??**.

Definition 9.5.11. Sei k ein Körper, V ein k-Vektorraum, $(v_i)_{i \in I}$ eine Basis von V und $\leq$ eine Anordnung von I. Gegeben eine endliche Teilmenge $J \subset I$ mit $|J| = r$ erklären wir dann ein Element $v_J \in \bigwedge^r V$ als das Dachprodukt

$$v_J = v_{i_1} \wedge \dots \wedge v_{i_r}$$

für $i_1 < i_2 < \dots < i_r$ die der Größe nach geordneten Elemente von J. Im Extremfall $r = 0$ vereinbaren wir $v_\emptyset = 1 \in k = \bigwedge^0 V$.

Proposition 9.5.12 (Basen der äußeren Potenzen). *Sei k ein Körper, V ein k-Vektorraum und $(v_i)_{i \in I}$ eine Basis von V. Sei eine Anordnung auf I gewählt. Gegeben $r \geq 0$ bilden dann die v_J mit $J \subset I$ und $|J| = r$ eine Basis der r-ten äußeren Potenz $\bigwedge^r V$.*

Beweis. Alle Tensoren $v_{i_1} \otimes \ldots \otimes v_{i_r}$ für $i_1, \ldots, i_r \in I$ beliebig erzeugen nach 9.3.10 die r-te Tensorpotenz $V^{\otimes r}$. Alle Dachprodukte $v_{i_1} \wedge \ldots \wedge v_{i_r}$ erzeugen folglich die r-te äußere Potenz $\bigwedge^r V$. Beim Umordnen derartiger Dachprodukte ändert sich höchstens das Vorzeichen, und kommt ein Vektor doppelt vor, ist das fragliche Dachprodukt eh null. Folglich erzeugen die Dachprodukte $v_{i_1} \wedge \ldots \wedge v_{i_r}$ mit $i_1 < \ldots < i_r$ unsere r-te äußere Potenz, und es bleibt nur, ihre lineare Unabhängigkeit nachzuweisen. Dazu betrachten wir für $f_1, \ldots, f_r \in V^\top$ beliebig die lineare Abbildung

$$\begin{array}{rccc} \operatorname{alt}(f_1, \ldots, f_r): & V^{\otimes r} & \to & k \\ & w_1 \otimes \ldots \otimes w_r & \mapsto & \det(f_i(w_j)) \end{array}$$

Sie verschwindet offensichtlich auf J_r und induziert folglich eine lineare Abbildung $\bigwedge^r V \to k$. Betrachten wir nun die Koordinatenfunktionen $v_i^\top \in V^\top$ zu unserer Basis $(v_i)_{i\in I}$ und bezeichnen für jedes r-elementige $J \subset I$ bestehend aus den der Größe nach geordneten Elementen $i_1 < \ldots < i_r$ mit $\operatorname{alt}(v_{i_1}^\top, \ldots, v_{i_r}^\top) = v_J^\top : \bigwedge^r V \to k$ die zu $v_{i_1}^\top, \ldots, v_{i_r}^\top$ gehörige Linearform, so folgt aus den Eigenschaften der Determinante für je zwei r-elementige Teilmengen $J, K \subset I$ unmittelbar

$$v_J^\top(v_K) = \begin{cases} 1 & J = K; \\ 0 & \text{sonst.} \end{cases}$$

Das impliziert die lineare Unabhängigkeit der v_K. □

9.5.13 (**Dimensionen der äußeren Potenzen**). Aus 9.5.12 folgt für einen Vektorraum V endlicher Dimension $\dim V = d < \infty$ sofort

$$\dim \bigwedge^r V = \binom{d}{r}$$

und insbesondere $\dim \bigwedge^d V = 1$ und $\bigwedge^r V = 0$ für $r > d$. Man schreibt deshalb im endlichdimensionalen Fall oft $\bigwedge^{\max} V := \bigwedge^{\dim V} V$.

Beispiel 9.5.14. Eine Basis von $\bigwedge^2 \mathbb{R}^4$ besteht etwa aus den sechs Vektoren $\mathrm{e}_1 \wedge \mathrm{e}_2, \mathrm{e}_1 \wedge \mathrm{e}_3, \mathrm{e}_1 \wedge \mathrm{e}_4, \mathrm{e}_2 \wedge \mathrm{e}_3, \mathrm{e}_2 \wedge \mathrm{e}_4$ und $\mathrm{e}_3 \wedge \mathrm{e}_4$.

Proposition 9.5.15 (Äußere Potenzen und Dualisieren). *Sei k ein Körper, V ein k-Vektorraum und $r \geq 0$. So existiert genau eine bilineare Abbildung*

$$\bigwedge^r (V^\top) \times \bigwedge^r V \to k$$

mit $((f_1 \wedge \ldots \wedge f_r), (w_1 \wedge \ldots \wedge w_r)) \mapsto \det(f_i(w_j))$, und im Fall $\dim V < \infty$ induziert diese Abbildung einen Isomorphismus

$$\bigwedge^r (V^\top) \xrightarrow{\sim} \left(\bigwedge^r V\right)^\top$$

9.5.16. Im Zweifelsfall interpretieren wir $\bigwedge^r V^\top$ im folgenden als $\bigwedge^r(V^\top)$. Unser kanonischer Isomorphismus $(\bigwedge^r V)^\top \xrightarrow{\sim} \mathrm{Alt}^r(V)$ aus 9.5.3 läßt sich so insbesondere für endlichdimensionales V verlängern zu einem kanonischen Isomorphismus $\bigwedge^r(V^\top) \xrightarrow{\sim} \mathrm{Alt}^r(V)$.

Beweis. Das wurde im wesentlichen bereits im Laufe des Beweises der vorhergehenden Proposition 9.5.12 gezeigt. Die Details bleiben dem Leser überlassen. □

9.5.17 (**Äußere Algebra und alternierende Tensoren**). Gegeben ein Vektorraum V definiert jede Permutation $\sigma \in \mathcal{S}_r$ einen Endomorphismus $[\sigma] : V^{\otimes r} \xrightarrow{\sim} V^{\otimes r}$ durch das "Permutieren der Tensorfaktoren", in Formeln $[\sigma] : v_1 \otimes \ldots \otimes v_r \mapsto v_{\sigma(1)} \otimes \ldots \otimes v_{\sigma(r)}$. Wir schreiben diese Operation auch $[\sigma] : t \mapsto t^\sigma$. Diese Endomorphismen liefern eine Rechtsoperation, in Formeln $t^{\sigma\circ\tau} = (t^\sigma)^\tau$. Um das einzusehen, müssen wir nur das kommutative Diagramm

$$\begin{array}{ccccc} \mathrm{Ens}(\{1,\ldots,n\},V) & \xrightarrow{\sim} & V^n & \longrightarrow & V^{\otimes n} \\ \downarrow{\scriptstyle \circ\sigma} & & & & \downarrow{\scriptstyle [\sigma]} \\ \mathrm{Ens}(\{1,\ldots,n\},V) & \xrightarrow{\sim} & V^n & \longrightarrow & V^{\otimes n} \end{array}$$

betrachten. Unter **alternierenden Tensoren** versteht man diejenigen Elemente von $V^{\otimes r}$, die beim Vertauschen von zwei Tensorfaktoren ihr Vorzeichen wechseln, in Formeln die Elemente des Teilraums

$$(V^{\otimes r})_{\mathrm{sgn}} := \{t \in V^{\otimes r} \mid t^\sigma = (\mathrm{sgn}\,\sigma)t \;\forall \sigma \in \mathcal{S}_r\}$$

Im Fall eines Grundkörpers der Charakteristik Null ist der **Alternator** $\mathrm{alt} : V^{\otimes r} \to (V^{\otimes r})_{\mathrm{sgn}}$ gegeben durch die Abbildungsvorschrift

$$t \mapsto \frac{1}{r!}\sum_{\sigma\in\mathcal{S}_r} \mathrm{sgn}(\sigma)t^\sigma$$

eine Projektion im Sinne von 1.6.5, wir haben also $\mathrm{alt}^2 = \mathrm{alt}$. Nun verschwindet alt auf J_r, folglich faktorisiert alt über $\bigwedge^r V$. Andererseits faktorisiert auch die kanonische Projektion $V^{\otimes r} \twoheadrightarrow \bigwedge^r V$ über alt. Das zeigt $\ker(\mathrm{alt}) = J_r$ und wir können die Identität auf $(V^{\otimes r})_{\mathrm{sgn}}$ darstellen als eine Verknüpfung

$$(V^{\otimes r})_{\mathrm{sgn}} \hookrightarrow V^{\otimes r} \twoheadrightarrow \bigwedge^r V \xrightarrow{\sim} (V^{\otimes r})_{\mathrm{sgn}}$$

wobei die mittlere Abbildung die kanonische Projektion ist und die Komposition der mittleren mit der rechten Abbildung unser Alternator alt. Das zeigt insbesondere, daß im Fall eines Grundkörpers der Charakteristik Null die kanonische Projektion $V^{\otimes r} \twoheadrightarrow \bigwedge^r V$ einen Isomorphismus $(V^{\otimes r})_{\mathrm{sgn}} \xrightarrow{\sim} \bigwedge^r V$ induziert.

Ergänzung 9.5.18. Manche Autoren machen es sich im Fall eines Grundkörpers der Charakteristik Null bei der Definition der äußeren Algebra eines Vektorraums V bequem, setzen schlicht $\bigwedge^r V = (V^{\otimes r})_{\mathrm{sgn}}$ und erklären das äußere Produkt entsprechend durch die Formel $\omega \wedge \eta = \mathrm{alt}(\omega \otimes \eta)$. Das hat allerdings über die Einschränkungen an die Charakteristik hinaus den Nachteil, daß die Assoziativität des äußeren Produkts, die wir sozusagen gratis erhalten haben, dabei durch wenig transparente Rechnungen nachgewiesen werden muß. In der Physik werden Ausdrücke der Gestalt $\mathrm{alt}(v_1 \otimes \ldots \otimes v_n)$ auch **Slater-Determinanten** genannt, da der Alternator bis auf eine Konstante an die Leibniz-Formel für Determinanten erinnert.

Ergänzung 9.5.19. Man beachte, daß sich im Fall eines endlichdimensionalen Vektorraums V mithilfe unserer Proposition 9.5.15 unser Isomorphismus $(\bigwedge^r V)^\top \xrightarrow{\sim} \mathrm{Alt}^r(V)$ aus 9.5.3 zu einem Isomorphismus $\bigwedge^r(V^\top) \xrightarrow{\sim} \mathrm{Alt}^r(V)$ verlängern läßt. Mit den durch diese Isomorphismen gegebenen Vertikalen und dem Dachprodukt in der oberen Horizontalen und dem Dachprodukt, wie wir es im Rahmen des Stokes'schen Satzes in **??** direkt einführen, in der unteren Horizontalen kommutiert dann das Diagramm

$$\begin{array}{ccc} \bigwedge^r V^\top \times \bigwedge^s V^\top & \longrightarrow & \bigwedge^{r+s} V^\top \\ \wr\downarrow & & \wr\downarrow \\ \mathrm{Alt}^r(V) \times \mathrm{Alt}^s(V) & \longrightarrow & \mathrm{Alt}^{r+s}(V) \end{array}$$

Die hier gegebene Konstruktion des Dachprodukts benötigt zwar den größeren begrifflichen Aufwand, scheint mir aber durchsichtiger als die im Rahmen des Beweises von **??** gegebene direkte Konstruktion. Die dort gegebene direkte Konstruktion funktioniert erfreulicherweise ohne alle Einschränkungen an die Charakteristik, liefert aber nur eine direkte Beschreibung für die Graßmann-Algebra des Dualraums eines endlichdimensionalen Vektorraums.

9.5.20 (**Maximale äußere Potenz und Determinante**). Jede lineare Abbildung $f : V \to W$ induziert lineare Abbildungen $f^{\otimes r} : V^{\otimes r} \to W^{\otimes r}$ und durch Übergang zu den Quotienten lineare Abbildungen $\bigwedge^r f : \bigwedge^r V \to \bigwedge^r W$, die in ihrer Gesamtheit einen Ringhomomorphismus

$$\bigwedge f : \bigwedge V \to \bigwedge W$$

liefern. Natürlich gilt auch $\bigwedge(f \circ g) = (\bigwedge f) \circ (\bigwedge g)$ und $\bigwedge(\mathrm{id}) = \mathrm{id}$. Ist speziell $f : V \to V$ ein Endomorphismus eines endlichdimensionalen Vektorraums, so ist $\bigwedge^{\max} f : \bigwedge^{\max} V \to \bigwedge^{\max} V$ ein Endomorphismus eines eindimensionalen Vektorraums alias ein Skalar. Wir zeigen nun, daß dieser Skalar genau die Deter-

minante von f ist, in Formeln

$$\bigwedge^{\max} f = \det f$$

Sei dazu $v_1, \ldots, v_n$ eine Basis von V. Dann ist $v_1 \wedge \ldots \wedge v_n$ nach 9.5.12 eine Basis von $\bigwedge^n V$. Haben wir $f(v_i) = \sum a_{ji} v_j$, so folgt

$$\begin{aligned}
(\textstyle\bigwedge f)(v_1 \wedge \ldots \wedge v_n) &= f(v_1) \wedge \ldots \wedge f(v_n) \\
&= (\textstyle\sum a_{j1} v_j) \wedge \ldots \wedge (\sum a_{ln} v_l) \\
&= \textstyle\sum_{\sigma:\{1,\ldots,n\}\to\{1,\ldots,n\}} a_{\sigma(1)1} v_{\sigma(1)} \wedge \ldots \wedge a_{\sigma(n)n} v_{\sigma(n)} \\
&= \textstyle\sum_{\sigma\in\mathcal{S}_n} \operatorname{sgn}(\sigma) a_{\sigma(1)1} \ldots a_{\sigma(n)n} v_1 \wedge \ldots \wedge v_n \\
&= (\det f) v_1 \wedge \ldots \wedge v_n
\end{aligned}$$

Die Multiplikationsregel für Determinanten folgt mit diesen Erkenntnissen unmittelbar aus der Relation $\bigwedge^{\max}(f \circ g) = (\bigwedge^{\max} f) \circ (\bigwedge^{\max} g)$. Daß die Determinante eines Endomorphismus $f : V \to V$ verschwindet, falls dieser nicht vollen Rang hat, kann man in diesem Formalismus auch wie folgt einsehen: Man schreibt f als Verknüpfung $V \twoheadrightarrow \operatorname{im} f \hookrightarrow V$, und unter der Annahme $d = \dim V > \dim(\operatorname{im} f)$ folgt $\bigwedge^d(\operatorname{im} f) = 0$, womit dann auch die Komposition $\bigwedge^d V \to \bigwedge^d(\operatorname{im} f) \to \bigwedge^d V$ die Nullabbildung sein muß.

Ergänzende Übung 9.5.21. Gegeben eine $(n \times m)$-Matrix A und eine $(m \times n)$-Matrix B kann man die Determinante der $(n \times n)$-Matrix AB bestimmen wie folgt: Für jede n-elementige Teilmenge $I \subset \{1, \ldots m\}$ mit Elementen $i_1 < \ldots < i_n$ möge A_I gerade aus den Spalten von A der Indizes $i_1, \ldots, i_n$ bestehen und B^I aus den Zeilen von B der Indizes $i_1, \ldots, i_n$. So gilt die **Cauchy-Binet-Formel**

$$\det(AB) = \sum_{|I|=n} (\det A_I)(\det B^I)$$

Ergänzung 9.5.22. Für einen k-Vektorraum V endlicher Dimension $\dim V = n$ liefert das Dachprodukt nichtausgeartete Paarungen $\bigwedge^d V \times \bigwedge^{n-d} V \to \bigwedge^n V$, denn wir haben $v_I \wedge v_J = \pm v_1 \wedge \ldots \wedge v_n$, falls I das Komplement von J ist, und Null sonst. Jeder Isomorphismus $\omega : \bigwedge^n V \xrightarrow{\sim} k$ liefert also insbesondere einen Isomorphismus $\hat{\omega} : \bigwedge^{n-1} V \cong V^\top$ gegeben durch $(\hat{\omega}(\eta))(v) = \omega(\eta \wedge v)$.

Weiterführende Übung 9.5.23. Ist $V' \hookrightarrow V \twoheadrightarrow V''$ eine kurze exakte Sequenz endlichdimensionaler Vektorräume, so induziert mit der Notation $d = \dim V''$ das Dachprodukt $\bigwedge^{\max} V' \otimes \bigwedge^d V \to \bigwedge^{\max} V$ einen Isomorphismus, den sogenannten **kanonischen Isomorphismus**

$$\bigwedge^{\max} V' \otimes \bigwedge^{\max} V'' \xrightarrow{\sim} \bigwedge^{\max} V$$

Weiterführende Übung 9.5.24. Sei $L \hookrightarrow V \twoheadrightarrow W$ eine kurze exakte Sequenz von Vektorräumen mit $\dim L = 1$. So faktorisiert für alle $m \geq 1$ das Dachprodukt $L \otimes \bigwedge^{m-1} V \to \bigwedge^m V$ über $L \otimes \bigwedge^{m-1} W$ und wir erhalten so eine kurze exakte Sequenz

$$L \otimes \bigwedge^{m-1} W \hookrightarrow \bigwedge^m V \twoheadrightarrow \bigwedge^m W$$

Hinweis: Man mag mit vollständiger Induktion über m argumentieren.

Weiterführende Übung 9.5.25. Die Determinante einer schiefsymmetrischen Matrix über einem Körper einer von Zwei verschiedenen Charakteristik ist stets Null, wenn die Zahl der Zeilen und Spalten nicht gerade ist, und ist ein Quadrat, wenn die Zahl der Zeilen und Spalten gerade ist. Genauer kann man im Fall der Charakteristik Null die **Pfaff'sche Determinante** einer schiefsymmetrischen $(2n \times 2n)$-Matrix (a_{ij}) erklären, indem man $\omega = \sum_{i<j} a_{ij} \mathrm{e}_i \wedge \mathrm{e}_i$ betrachtet und die Pfaff'sche Determinante erklärt durch die Identität

$$\frac{\omega^n}{n!} = \mathrm{Pf}(a_{ij}) \mathrm{e}_1 \wedge \ldots \wedge \mathrm{e}_{2n}$$

Übung 9.5.26. Sei $f : V \to V$ ein Endomorphismus eines endlichdimensionalen komplexen Vektorraums. Man zeige für den k-ten Koeffizienten a_k des charakteristischen Polynoms die Formel

$$a_k = (-1)^k \operatorname{tr}\left(\bigwedge^k f \,\middle|\, \bigwedge^k V \right)$$

Hinweis: Man ziehe ich auf den Fall einer oberen Dreiecksmatrix zurück. Die Formel gilt auch für beliebige Körper, da mag an sich mit einer Einbettung in einen algebraisch abgeschlossenen Körper behelfen, die nach III.3.7.6 stets existiert.

Ergänzende Übung 9.5.27. Gegeben ein dreidimensionaler reeller Vektorraum V mit einem L-wertigen Skalarprodukt betrachte man die Komposition von Isomorphismen

$$\bigwedge^2 V \xrightarrow{\sim} \mathrm{Hom}\left(V, \bigwedge^3 V\right) \xrightarrow{\sim} V^* \otimes L^{\otimes 3} \otimes \mathrm{or}_{\mathbb{R}}(V) \xrightarrow{\sim} L \otimes \mathrm{or}_{\mathbb{R}}(V) \otimes V$$

wo die erste Abbildung durch $\eta \mapsto \eta\wedge$ gegeben wird, die Zweite von dem Spatprodukt 8.6.10 herkommt, und die Dritte von dem durch das Skalarprodukt gegebenen Isomorphismus $V \xrightarrow{\sim} V^* \otimes L^{\otimes 2}$. Man zeige, daß die Verknüpfung der Abbildung $V \times V \to \bigwedge^2 V$, $(v, w) \mapsto v \wedge w$ mit obiger Identifikation gerade unser Kreuzprodukt aus 8.6.11 ist.

10 Kategorien und Funktoren

10.1 Kategorien

10.1.1. Bereits der linearen Algebra zeigen viele Konstruktionen, wie etwa Dualräume, Tensorpotenzen oder äußere Potenzen, meines Erachtens erst in der Sprache der Kategorientheorie ihre wahre Natur. Es geht bei diesen Konstruktionen ja keineswegs darum, irgendwelche neuen Vektorräume zu erhalten: Wir wissen ja, daß wir zumindest im Fall endlicher Dimension dabei nichts wesentlich Neues finden können. Vielmehr geht es darum, zusammen mit diesen neuen Vektorräumen auch zu jeder linearen Abbildung zwischen den gegebenen Räumen eine lineare Abbildung zwischen den neu konstruierten Räumen zu konstruieren, und erst zusammen mit diesen zusätzlichen Konstruktionen, die zu allem Überfluß meist eher als Nebensache behandelt werden, obwohl sie doch die eigentliche Hauptsache sind, erhält man nützliche und anwendbare Begriffsbildungen.

10.1.2. Die Sprache der Kategorien und Funktoren liefert für derartige Konstruktionen einen formalen Rahmen. Sie ist ähnlich ausdrucksstark, grundlegend und elegant wie die Sprache der Mengenlehre und gehört meines Erachtens in den Rucksack jeder Mathematikerin und jedes Mathematikers. Ich bin sogar der Ansicht, daß die "naive Mengenlehre" aus den Grundvorlesungen am besten durch eine axiomatische Beschreibung der "Kategorie aller Mengen" wie etwa in [LR03] formalisiert wird. So formal will ich bei der hier gegebenen Darstellung jedoch nicht werden und arbeite deshalb weiter auf der Grundlage der naiven Mengenlehre. Eine ausführlichere Behandlung der Kategorientheorie findet man zum Beispiel in [Mac98].

Definition 10.1.3. Eine **Kategorie** $\mathcal{C}$ besteht aus

a. einer Menge von **Objekten** $\operatorname{Ob}\mathcal{C}$;

b. einer Menge $\mathcal{C}(X,Y)$ von **Morphismen** für je zwei Objekte $X, Y \in \operatorname{Ob}\mathcal{C}$;

c. einer Abbildung $\mathcal{C}(X,Y) \times \mathcal{C}(Y,Z) \to \mathcal{C}(X,Z),\ (f,g) \mapsto g \circ f$ für je drei Objekte $X, Y, Z \in \mathcal{C}$, genannt die **Verknüpfung** von Morphismen,

derart, daß folgende Axiome erfüllt sind:

1. Die Morphismenmengen sind paarweise disjunkt;

2. Die Verknüpfung ist **assoziativ**, d.h. es gilt $(f \circ g) \circ h = f \circ (g \circ h)$ für Morphismen f, g und h, wann immer diese Verknüpfungen sinnvoll sind;

3. Für jedes Objekt $X \in \operatorname{Ob}\mathcal{C}$ gibt es einen Morphismus $\mathrm{id}_X \in \mathcal{C}(X,X)$, die **Identität auf** X, so daß gilt $\mathrm{id}_X \circ f = f$ und $g \circ \mathrm{id}_X = g$ für Morphismen f, g, wann immer diese Verknüpfungen sinnvoll sind. Die üblichen Argumente zeigen, daß es für jedes X höchstens einen derartigen Morphismus geben kann, womit auch die Verwendung des bestimmten Artikels gerechtfertigt ist.

Beispiel 10.1.4. Zu jedem Monoid können wir eine Kategorie mit einem einzigen Objekt bilden, dessen Morphismen zu sich selbst eben genau die Elemente von besagtem Monoid sind, mit der Verknüpfung in unserem Monoid als Verknüpfung von Morphismen. Umgekehrt ist für jedes Objekt X einer Kategorie $\mathcal{C}$ die Menge $\mathcal{C}(X,X)$ mit der von der Kategorienstruktur herkommenden Verknüpfung ein Monoid. Die Morphismen von X zu sich selber nennen wir die **Endomorphismen** von X und kürzen sie zukünftig oft ab mit

$$\mathcal{C}(X) := \mathcal{C}(X,X)$$

Beispiel 10.1.5. Als nächstes Beispiel hätte ich gerne die Kategorie $\mathcal{C} = \mathrm{Ens}$ aller Mengen eingeführt. Das ist jedoch nicht ohne weiteres möglich, da die "Gesamtheit aller Mengen" nach I.2.1.21 nicht als Menge angesehen werden darf. Um diese logischen Probleme zu vermeiden, betrachten wir ein Mengensystem alias eine Menge von Mengen $\mathfrak{U}$ und die Kategorie

$$\mathfrak{U}\mathrm{Ens}$$

aller Mengen $X \in \mathfrak{U}$. Ihre Objekte sind beliebige Mengen $X \in \mathfrak{U}$. Für zwei Mengen $X, Y \in \mathfrak{U}$ ist die Morphismenmenge $\mathrm{Ens}(X,Y)$ die Menge aller Abbildungen von X nach Y. Die Verknüpfung ordnet jedem Paar (f,g) von Abbildungen ihre Komposition $g \circ f$ zu, und $\mathrm{id}_X \in \mathrm{Ens}(X,X)$ ist schlicht die identische Abbildung $\mathrm{id}_X(x) = x \; \forall x \in X$.

10.1.6. An dieser Stelle sollte ich vielleicht präzisieren, daß ich mit einer Formalisierung der Mengenlehre arbeite, die ohne "Urelemente" auskommt. Alle Elemente von Mengen sind also wieder Mengen, und ein Mengensystem ist nichts anderes als eine Menge. Zum Beispiel können wir die Menge der natürlichen Zahlen erklären als

$$\mathbb{N} := \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \ldots\}$$

10.1.7. Sei $\mathcal{C}$ eine Kategorie und seien $X, Y \in \operatorname{Ob}\mathcal{C}$ Objekte von $\mathcal{C}$. Statt $f \in \mathcal{C}(X,Y)$ sagen wir auch f **ist ein Morphismus von** X **nach** Y und schreiben kurz

$$f : X \to Y$$

Statt id_X schreiben wir oft nur id. Statt $X \in \operatorname{Ob}\mathcal{C}$ schreiben wir oft kürzer $X \in \mathcal{C}$.

Kategorie	Morphismen	Kürzel
{Mengen}	alle Abbildungen	Ens
{Monoide}	Morphismen von Monoiden	Mon
{Gruppen}	Gruppenhomomorphismen	Grp
{abelsche Gruppen}	Gruppenhomomorphismen	Ab
{topologische Räume}	stetige Abbildungen	Top
{punktierte Mengen}	Abbildungen, die den Basispunkt erhalten	Ens^*
{punktierte Räume}	stetige Abbildungen, die den Basispunkt erhalten	Top^*
{k-Vektorräume}	k-lineare Abbildungen	$k\text{-}\mathrm{Mod}$, Mod_k
{Affine Räume über k}	affine Abbildungen	$k\text{-}\mathrm{Aff}$, Aff_k
{nicht unitäre Ringe}	Rng-Homomorphismen	Rng
{Ringe}	Ringhomomorphismen	Ring
{kommutative Ringe}	Ringhomomorphismen	Kring
{k-Algebren}	k-Algebren-Homomorphismen	$k\text{-}\mathrm{Alg}$, Alg_k
{k-Ringalgebren}	k-Ringalgebren-Homomorphismen	$k\text{-}\mathrm{Ralg}$, Ralg_k

Hier einige Beispiele von Kategorien. Als Verknüpfung von Morphismen ist für die Kategorien dieser Liste stets die Komposition von Abbildungen gemeint. Um logische Abstürze zu vermeiden, müssen wir uns genauer stets ein Mengensystem $\mathfrak{U}$ dazudenken, aus dem die zugrundeliegende Menge der jeweiligen Struktur kommen muß und das wir in der Notation meist unterschlagen. Wenn wir es doch notieren wollen, schreiben wir

$$\mathfrak{U}\mathrm{Kring}$$

und dergleichen. Wir denken es uns meist als ziemlich riesig und fordern zumindest implizit für gewöhnlich, daß es unter dem Bilden von Teilmengen stabil sein möge und die reellen Zahlen enthält. Die Notation Mod_k für Vektorräume über k steht für ihre alternative Bezeichnung als k**-Moduln**.

10.1.8. Unter einer **Unterkategorie** einer Kategorie versteht man ein Paar bestehend aus einer Teilmenge von Objekten nebst Teilmengen der Morphismenräume für je zwei Objekte unserer Teilmenge derart, daß die offensichtlichen Bedingungen erfüllt sind. Eine Unterkategorie heißt **voll** genau dann, wenn die fraglichen Teilmengen der Morphismenräume jeweils aus allen Morphismen in der ursprünglichen Kategorie bestehen.

10.1.9. Morphismen von k-Vektorräumen V, W notiert man statt $\mathrm{Mod}_k(V,W)$ meist $\mathrm{Hom}_k(V,W)$, und für Endomorphismen ist die Notation $\mathrm{Mod}_k(V) = \mathrm{End}_k V$ üblich. Das Symbol "Hom" für Morphismenräume versuche ich jedoch im allgemeinen zu vermeiden: Ich will es reservieren für die sogenannten "internen Hom-Räume", unter denen man Vorschriften versteht, die in gewissen Situationen je zwei Objekten einer Kategorie ein Drittes zuordnen, im Fall der Vektorräume etwa die Morphismenmenge mit ihrer natürlichen Vektorraumstruktur. Das Kürzel "Mod" mit etwelchen oberen und unteren Indizes wird stets für abelsche Gruppen mit Zusatzstrukturen stehen, meist Operationen von Ringen oder Gruppen. Gehen diese Zusatzstrukturen aus dem Kontext hervor, so lassen wir die entsprechenden Indizes auch manchmal weg. Für abelsche Gruppen ohne Zusatzstrukturen benutzen wir stets das Kürzel "Ab".

Beispiel 10.1.10. Jede partiell geordnete Menge $(A, \leq)$ kann als Kategorie aufgefaßt werden wie folgt: Objekte sind die Elemente, Morphismen gibt es jeweils einen von einem Element zu jedem kleineren und zu sich selber, und die Verknüpfung von Morphismen ist die offensichtliche und einzig mögliche.

Beispiel 10.1.11. Für jede Kategorie $\mathcal{C}$ bildet man die **opponierte Kategorie** $\mathcal{C}^{\mathrm{opp}} = \mathcal{C}^{\circ}$ wie folgt: Man setzt

$$\mathrm{Ob}\,\mathcal{C}^{\mathrm{opp}} = \mathrm{Ob}\,\mathcal{C} \qquad \text{und} \qquad \mathcal{C}^{\mathrm{opp}}(X,Y) = \mathcal{C}(Y,X)$$

und erklärt die Verknüpfung von Morphismen in $\mathcal{C}^{\mathrm{opp}}$ in der offensichtlichen Weise.

Beispiel 10.1.12. Gegeben Kategorien $\mathcal{A}, \mathcal{B}$ bildet man ihr **Produkt**, eine weitere Kategorie $\mathcal{A} \times \mathcal{B}$, wie folgt: Man setzt $\mathrm{Ob}(\mathcal{A} \times \mathcal{B}) = \mathrm{Ob}\,\mathcal{A} \times \mathrm{Ob}\,\mathcal{B}$, erklärt Morphismen in der Produktkategorie als Paare von Morphismen in den Ausgangskategorien und erklärt die Verknüpfung von Morphismen in der Produktkategorie in der offensichtlichen Weise.

Definition 10.1.13. 1. Ein Morphismus $f \in \mathcal{C}(X,Y)$ in einer Kategorie heißt ein **Isomorphismus** oder **Iso** und als Adjektiv **iso** genau dann, wenn es einen Morphismus $g \in \mathcal{C}(Y,X)$ gibt mit $f \circ g = \mathrm{id}_Y$ und $g \circ f = \mathrm{id}_X$. Wir notieren die Menge aller Isomorphismen von X nach Y auch $\mathcal{C}^{\times}(X,Y)$ und notieren Isomorphismen oft $f : X \xrightarrow{\sim} Y$.

2. Zwei Objekte X und Y einer Kategorie heißen **isomorph** genau dann, wenn es einen Iso $f : X \xrightarrow{\sim} Y$ gibt. Man schreibt dann auch kurz $X \cong Y$.

Übung 10.1.14. Ein Morphismus $f \in \mathcal{C}(X, Y)$ in einer Kategorie ist ein Isomorphismus genau dann, wenn es Morphismen $g, h \in \mathcal{C}(Y, X)$ gibt mit $f \circ g = \mathrm{id}_Y$ und einen $h \circ f = \mathrm{id}_X$.

Ergänzende Übung 10.1.15. Gegeben in einer Kategorie Morphismen $f \in \mathcal{C}(X, Y)$ und $g \in \mathcal{C}(Y, X)$ derart, daß $f \circ g$ und $g \circ f$ Isomorphismen sind, müssen f und g bereits selbst Isomorphismen sein.

Beispiele 10.1.16. Isomorphismen in der Kategorie der Mengen nennt man Bijektionen, Isomorphismen in der Kategorie der topologischen Räume Homöomorphismen. Kategorien, in denen alle Morphismen Isomorphismen sind, heißen auch **Gruppoide**. Kategorien, in denen es außer den Identitäten keine Morphismen gibt, heißen **diskret**. Natürlich ist jede diskrete Kategorie ein Gruppoid.

10.1.17. Bisher hatten wir an verschiedenen Stellen Isomorphismen abweichend erklärt als bijektive Homomorphismen, zum Beispiel bei Gruppen, Vektorräumen, affinen Räumen etc. In allen diesen Fällen sollte es jedoch klar sein, daß die Umkehrabbildung im Sinne der Mengenlehre auch selbst wieder ein Homomorphismus ist, so daß wir in der Tat auch Isomorphismen im Sinne der Kategorientheorie vor uns haben. Ein typisches Beispiel für eine Kategorie von gewissen "Mengen mit Zusatzstrukturen", in der bijektive Homomorphismen keine Isomorphismen zu sein brauchen, ist die Kategorie der topologischen Räume.

10.1.18. Viele mathematische Fragestellungen lassen sich in der Sprache der Kategorien dahingehend formulieren, daß man einen Überblick über alle Objekte einer Kategorie gewinnen will, wobei man zwischen isomorphen Objekten nicht unterscheidet. Man spricht dann auch von **Isomorphieklassen** von Objekten und nennt Fragestellungen dieser Art **Klassifikationsprobleme**. Zum Beispiel werden die endlich erzeugten k-Vektorräume klassifiziert durch ihre Dimension, die endlich erzeugten abelschen Gruppen durch unsere Sätze 7.4.2 und alternativ 7.4.3, die endlichen Mengen durch ihre Kardinalität I.2.1.8, beliebige Mengen, genauer beliebige Mengen aus unserem Mengensystem $\mathfrak{U}$, ebenfalls durch ihre Kardinalität **??**, und die Liste ließe sich noch lange fortsetzen.

10.1.19. Zu jeder Kategorie $\mathcal{C}$ erklären wir eine Unterkategorie, die **Isomorphismenkategorie** $\mathcal{C}^\times$ **von** $\mathcal{C}^\times$ mit denselben Objekten aber nur den Isomorphismen von $\mathcal{C}$ als Morphismen. Die Menge aller Isomorphismen von einem Objekt X einer Kategorie $\mathcal{C}$ in ein Objekt Y notieren wir folgerichtig $\mathcal{C}^\times(X, Y)$. Die Isomorphismen von einem Objekt X einer Kategorie $\mathcal{C}$ auf sich selber heißen die **Automorphismen** von X. Sie bilden stets eine Gruppe, die **Automorphismengruppe** $\mathcal{C}^\times(X)$ von X. Die Automorphismengruppe $\mathrm{Mod}_k^\times(V)$ eines k-Vektorraums

V hatten wir meist $\mathrm{GL}(V)$ notiert, die Automorphismengruppe $\mathrm{Ens}^\times(X)$ einer Menge X hatten wir die Gruppe der Permutationen von X genannt.

Definition 10.1.20. Ein Objekt F einer Kategorie $\mathcal{C}$ heißt **final** genau dann, wenn es für alle $Y \in \mathcal{C}$ genau einen Morphismus von Y nach F gibt, in Formeln

$$|\mathcal{C}(Y,F)| = 1 \quad \forall Y \in \mathcal{C}$$

Definition 10.1.21. Ein Objekt K einer Kategorie $\mathcal{C}$ heißt **kofinal** genau dann, wenn es für alle $Y \in \mathcal{C}$ genau einen Morphismus von K nach Y gibt, in Formeln

$$|\mathcal{C}(K,Y)| = 1 \quad \forall Y \in \mathcal{C}$$

Beispiele 10.1.22. In einer Kategorie $\mathfrak{U}\mathrm{Ens}$ von Mengen sind die einpunktigen Mengen genau die finalen Objekte und die leere Menge ist das einzige kofinale Objekt, wenn sie denn zu $\mathfrak{U}$ dazugehört.

10.1.23. Zwischen je zwei finalen bzw. kofinalen Objekten gibt es offensichtlich genau einen Isomorphismus. Wir erlauben uns deshalb, etwas lax von *dem* finalen bzw. kofinalen Objekt zu reden, und bezeichnen "das" finale Objekt gerne mit $\mathrm{pt} = \mathrm{pt}(\mathcal{C})$ für "Punkt" und Morphismen dahin mit c für "konstant". Manchmal verwenden wir als Bezeichnung des finalen Objekts auch die kleingeschriebene Bezeichnung der Kategorie, etwa top für den einelementigen topologischen Raum oder ens für die einelementige Menge.

Übung 10.1.24. Man finde finale und kofinale Objekte in den Kategorien der Gruppen, Ringe, topologischen Räume, Vektorräume.

10.2 Funktoren

Definition 10.2.1. Ein **Funktor** $F : \mathcal{A} \to \mathcal{B}$ von einer Kategorie $\mathcal{A}$ in eine Kategorie $\mathcal{B}$ besteht aus

a. einer Abbildung $F : \mathrm{Ob}\,\mathcal{A} \to \mathrm{Ob}\,\mathcal{B}$, $X \mapsto FX$;

b. einer Abbildung $F : \mathcal{A}(X,Y) \to \mathcal{B}(FX,FY)$, $f \mapsto Ff$ für je zwei Objekte $X, Y \in \mathrm{Ob}\,\mathcal{A}$,

derart, daß gilt

1. $F(f \circ g) = (Ff) \circ (Fg)$ für beliebige verknüpfbare Morphismen f und g aus der Kategorie $\mathcal{A}$;

2. $F(\mathrm{id}_X) = \mathrm{id}_{FX}$ für jedes Objekt $X \in \mathcal{A}$.

10.2.2. Man gibt bei einem Funktor F meist nur die Abbildung $X \mapsto FX$ auf den Objekten an in der Hoffnung, daß dadurch schon klar wird, welche Abbildung $f \mapsto Ff$ auf den Morphismen gemeint ist.

Beispiel 10.2.3. Gegeben ein Körper k bezeichne Modfg_k mit fg für "finitely generated" die Kategorie der endlich erzeugten k-Vektorräume. Das Bilden des Dualraums mit dem Bilden der transponierten Abbildung auf dem Niveau der Homomorphismen ist ein Funktor

$$\begin{array}{ccc} \mathrm{Modfg}_k & \to & \mathrm{Modfg}_k^{\mathrm{opp}} \\ V & \mapsto & V^\top \\ f \downarrow & \mapsto & \uparrow f^\top \\ W & \mapsto & W^\top \end{array}$$

von der Kategorie der endlich erzeugten k-Vektorräume in ihre eigene opponierte Kategorie, vergleiche 1.11.10. Genau genommen müssen wir dazu unser Mengensystem $\mathfrak{U}$, das sich stets im Hintergrund halten will, so groß wählen, daß es beim Bilden des Dualraums nicht verlassen wird. Beschränken wir uns wie oben auf endlichdimensionale Räume, so ist das jedoch vergleichsweise unproblematisch. Wollen wir jedoch den Dualraumfunktor auch für Räume unendlicher Dimension erklären, so stoßen wir auf die Schwierigkeit, daß bereits bei unendlichdimensionalen Räumen über dem Körper mit zwei Elementen die "Kardinalität" des Dualraums echt größer sein wird als die Kardinalität des Ausgangsraums. Im folgenden erkläre ich, wie man sich hier mit dem Begriff eines "Universums" 10.2.4 einigermaßen elegant aus der Affäre ziehen kann. Diese Leitplanken zur Vermeidung logischer Abstürze beschreibe ich für eine Formalisierung der Mengenlehre, die ohne "Urelemente" arbeitet, d.h. in der alle Elemente von Mengen auch selbst wieder Mengen sind.

Definition 10.2.4. Ein **Universum** ist eine Menge $\mathfrak{U}$ mit den folgenden Eigenschaften:

1. $x \in M$ und $M \in \mathfrak{U}$ implizieren $x \in \mathfrak{U}$.
2. $x \in \mathfrak{U} \Rightarrow \{x\} \in \mathfrak{U}$.
3. $A \in \mathfrak{U} \Rightarrow \mathcal{P}(A) \in \mathfrak{U}$.
4. Gegeben $I \in \mathfrak{U}$ und eine Abbildung $f : I \to \mathfrak{U}$ gilt $\left(\bigcup_{i\in I} f(i)\right) \in \mathfrak{U}$.

Ergänzung 10.2.5. Diese Definition steht fast genauso bei Grothendieck [Gro72, Exposé I]. Abweichend will Grothendieck nur die leere Menge nicht als Universum zulassen und fordert statt unserer zweiten Bedingung scheinbar stärker $x, y \in \mathfrak{U} \Rightarrow \{x, y\} \in \mathfrak{U}$. Da jedoch für jedes nichtleere Universum gilt $\emptyset \in \mathfrak{U}$, und

folglich $\{\emptyset\} \in \mathfrak{U}$ und $\{\emptyset, \{\emptyset\}\} \in \mathfrak{U}$, ergibt sich das wegen $\{x, y\} = \{x\} \cup \{y\}$ aus dem letzten Axiom, angewandt auf die Abbildung $f : \{\emptyset, \{\emptyset\}\} \to \mathfrak{U}$ mit $f(\emptyset) = \{x\}$ und $f(\{\emptyset\}) = \{y\}$.

10.2.6. Gegeben ein Universum $\mathfrak{U}$ gilt es genau zu unterscheiden zwischen Mengen $x \in \mathfrak{U}$, die also Elemente des Universums sind, und Mengen $M \subset \mathfrak{U}$, die nur Teilmengen des Universums sind. Nach Axiom 3 ist jedes Element eines Universums auch eine Teilmenge besagten Universums, aber das Umgekehrte gilt nicht. Die Formel $M = \{x \in \mathfrak{U} \mid x \notin x\}$ definiert dann eine Teilmenge $M \subset \mathfrak{U}$, die kein Element von $\mathfrak{U}$ zu sein braucht, und die Formel $A = \{M \subset \mathfrak{U} \mid M \notin M\}$ definiert eine Menge A, die nicht Teilmenge von $\mathfrak{U}$ zu sein braucht, so daß keine dieser beiden Formeln unmittelbar auf einen Widerspruch führt.

10.2.7. Wenn wir mit Kuratowski $(x, y) := \{x, \{y\}\}$ setzen, erhalten wir sofort $x, y \in \mathfrak{U} \Rightarrow (x, y) \in \mathfrak{U}$. Das Produkt von je zwei Mengen, die Elemente unseres Universums sind, ist auch selbst Element unseres Universums, zum Beispiel indem wir die Vereinigung erst über alle $x \in X$ und dann über alle $y \in Y$ der Mengen $\{(x, y)\}$ bilden. Weiter ist mit je zwei Mengen $X, Y \in \mathfrak{U}$ auch die Menge der Abbildungen $\mathrm{Ens}(X, Y)$ Element von $\mathfrak{U}$ und dasselbe gilt für jedes Produkt $\prod_{i \in I} X_i$ mit $I \in \mathfrak{U}$ und $X_i \in \mathfrak{U}$ für alle $i \in I$. Ebenso folgt, daß jede Teilmenge eines Elements unseres Universums wieder ein Element unseres Universums ist.

10.2.8. Die Annahme, daß jede Menge Element eines Universums ist, müssen wir der Mengenlehre als zusätzliches Axiom hinzufügen. Es scheint nicht auf Widersprüche zu führen. Insbesondere ist natürlich auch jedes Universum Element eines Universums. Gegeben ein Körper k und ein Universum $\mathfrak{U}$ mit $k \in \mathfrak{U}$ können wir dann auf der Kategorie $k\text{-}\mathfrak{U}\mathrm{Mod}$ der k-Vektorräume aus $\mathfrak{U}$ in der Tat den Dualraumfunktor erklären.

Beispiel 10.2.9. Gegeben ein Körper k bezeichne Modfg_k mit fg für "finitely generated" die Kategorie der endlich erzeugten k-Vektorräume und $\mathrm{Modfg}_k^\times$ die zugehörige Isomorphismenkategorie. Gegeben ein angeordneter Körper k ist das Bilden der Orientierungsmenge nach 3.2.13 ein Funktor

$$\mathrm{or} : \mathrm{Modfg}_k^\times \to \mathrm{Ens}^\times$$

Beispiel 10.2.10. Das Bilden des Homomorphismenraums ist ein Funktor

$$\begin{array}{ccccc}
\mathrm{Mod}_k^{\mathrm{opp}} \times \mathrm{Mod}_k & \to & \mathrm{Mod}_k & & \\
(V, W) & \mapsto & \mathrm{Hom}_k(V, W) & \ni & h \\
(f, g) \downarrow & \mapsto & \downarrow & & \downarrow \\
(V', W') & \mapsto & \mathrm{Hom}_k(V', W') & \ni & g \circ h \circ f
\end{array}$$

wo der ganz rechte vertikale Pfeil eigentlich ein $\mapsto$ sein sollte, was ich aber mit meinem Schreibprogramm nicht hingekriegt habe. Natürlich hätten wir hier statt

$\mathrm{Hom}_k(V,k)$ auch $\mathrm{Mod}_k(V,k)$ schreiben können, aber die Notation Hom betont, daß wir besagte Menge von Morphismen mit ihrer Vektorraumstruktur betrachten wollen.

Ergänzendes Beispiel 10.2.11. Das Bilden des Tensorprodukts ist ein Funktor

$$\begin{array}{ccc} \mathrm{Mod}_k \times \mathrm{Mod}_k & \to & \mathrm{Mod}_k \\ (V,W) & \mapsto & V \otimes W \\ (f,g)\downarrow & \mapsto & \downarrow f \otimes g \\ (V',W') & \mapsto & V' \otimes W' \end{array}$$

Ergänzendes Beispiel 10.2.12. Das Bilden der r-ten Tensorpotenz nach 9.5.1 ist ein Funktor $\mathrm{Mod}_k \to \mathrm{Mod}_k$, $V \mapsto V^{\otimes r}$, $f \mapsto f^{\otimes r}$. Das Bilden der r-ten äußeren Potenz nach 9.5.3 ist ein Funktor $\mathrm{Mod}_k \to \mathrm{Mod}_k$, $V \mapsto \bigwedge^r V$, $f \mapsto \bigwedge^r f$ wie in 9.5.20 erklärt.

Beispiel 10.2.13. Das "Vergessen der Gruppenstruktur" definiert einen Funktor $\mathrm{Grp} \to \mathrm{Ens}$ von den Gruppen in die Mengen. Natürlich gibt es noch viele andere solche **Vergiss-Funktoren**. Ist $\mathcal{C}$ eine Kategorie und $X \in \mathcal{C}$ ein Objekt, so ist die Zuordnung

$$\begin{array}{rccc} \mathcal{C}(X,\ ): & \mathcal{C} & \to & \mathrm{Ens} \\ & Y & \mapsto & \mathcal{C}(X,Y) \end{array}$$

stets ein Funktor. Jeder Funktor $F : \mathcal{A} \to \mathcal{B}$ liefert in offensichtlicher Weise einen Funktor $F : \mathcal{A}^{\mathrm{opp}} \to \mathcal{B}^{\mathrm{opp}}$ zwischen den zugehörigen opponierten Kategorien.

10.2.14. Für jede Kategorie $\mathcal{C}$ haben wir den **Identitätsfunktor** $\mathrm{Id} = \mathrm{Id}_{\mathcal{C}}$ von besagter Kategorie in sich selber. Sind $F : \mathcal{A} \to \mathcal{B}$ und $G : \mathcal{B} \to \mathcal{C}$ Funktoren, so ist auch $G \circ F : \mathcal{A} \to \mathcal{C}$ ein Funktor. In dieser Weise bildet die Gesamtheit aller kleinen Kategorien selbst eine Kategorie Cat, mit den kleinen Kategorien als Objekten und Funktoren als Morphismen. Die Menge aller Funktoren $\mathcal{A} \to \mathcal{B}$ sollten und werden wir insbesondere folgerichtig $\mathrm{Cat}(\mathcal{A},\mathcal{B})$ notieren.

Lemma 10.2.15. *Ein Funktor bildet stets Isomorphismen auf Isomorphismen ab. Insbesondere haben isomorphe Objekte unter einem Funktor stets isomorphe Bilder.*

Beweis. Sei F unser Funktor. Wir schließen:

$$\begin{array}{ll} f \text{ ist Isomorphismus} & \Rightarrow \text{ Es gibt } g \text{ mit } f \circ g = \mathrm{id} \text{ und } g \circ f = \mathrm{id} \\ & \Rightarrow (Ff) \circ (Fg) = \mathrm{id} \text{ und } (Fg) \circ (Ff) = \mathrm{id} \\ & \Rightarrow Ff \text{ ist Isomorphismus.} \end{array}$$ □

Definition 10.2.16. Ein Funktor $F : \mathcal{A} \to \mathcal{B}^{\mathrm{opp}}$ heißt auch ein **kontravarianter Funktor** von $\mathcal{A}$ nach $\mathcal{B}$.

10.2.17. Ausgeschrieben besteht ein kontravarianter Funktor von $\mathcal{A}$ nach $\mathcal{B}$ aus einer Abbildung $F : \operatorname{Ob}\mathcal{A} \to \operatorname{Ob}\mathcal{B}$ sowie für je zwei Objekte $X, Y \in \mathcal{A}$ einer Abbildung $F : \mathcal{A}(X,Y) \to \mathcal{B}(FY, FX)$ derart, daß gilt $F(\mathrm{id}) = \mathrm{id}$ und $F(f \circ g) = Fg \circ Ff$ für alle verknüpfbaren Morphismen f, g.

Beispiel 10.2.18. Die Zuordnung, die jedem Vektorraum über einem festen Körper k seinen Dualraum zuordnet, ist nach 1.11.10 ein kontravarianter Funktor $\mathrm{Mod}_k \to \mathrm{Mod}_k, V \mapsto V^\top, f \mapsto f^\top$.

Beispiel 10.2.19. Gegeben eine Kategorie $\mathcal{C}$ und ein Objekt $X \in \mathcal{C}$ ist die Zuordnung $\mathcal{C}(\ , X) : \mathcal{C} \to \mathrm{Ens}$ stets ein kontravarianter Funktor.

Definition 10.2.20.

1. Ein Funktor $F : \mathcal{A} \to \mathcal{B}$ heißt **treu** genau dann, wenn er Injektionen $F : \mathcal{A}(A, A') \hookrightarrow \mathcal{B}(FA,\ FA')$ auf den Morphismen induziert, für alle $A, A' \in \mathcal{A}$.

2. Ein Funktor $F : \mathcal{A} \to \mathcal{B}$ heißt eine **volltreu** genau dann, wenn er Bijektionen $F : \mathcal{A}(A, A') \xrightarrow{\sim} \mathcal{B}(FA,\ FA')$ auf den Morphismen induziert.

3. Ein Funktor $F : \mathcal{A} \to \mathcal{B}$ heißt eine **Äquivalenz von Kategorien** genau dann, wenn er volltreu ist und zusätzlich eine Surjektion auf Isomorphieklassen von Objekten induziert, wenn es also in Formeln für alle $B \in \mathcal{B}$ ein $A \in \mathcal{A}$ gibt mit $FA \cong B$. Ich notiere Äquivalenzen von Kategorien $\xrightarrow{\approx}$.

4. Ein Funktor $F : \mathcal{A} \to \mathcal{B}$ heißt ein **Isomorphismus von Kategorien** genau dann, wenn er bijektiv ist auf Objekten und auf Morphismen. Ich notiere Isomorphismen von Kategorien $\xrightarrow{\sim}$.

Beispiel 10.2.21. Sei k ein Körper. Wir betrachten die Kategorie Modfg_k aller endlichdimensionalen alias endlich erzeugten alias "finitely generated" k-Vektorräume mit linearen Abbildungen als Morphismen. Weiter betrachten wir, und zwar sogar für einen beliebigen Ring k, die Kategorie $\mathcal{M} = \mathcal{M}_k$ mit Objekten $\operatorname{Ob}\mathcal{M} = \mathbb{N}$ und Matrizen mit Einträgen in k des entsprechenden Formats als Morphismen, in Formeln $\mathcal{M}(m,n) = \mathrm{M}(n \times m; k)$. Die Verknüpfung von Morphismen in $\mathcal{M}$ schließlich sei die Matrixmultiplikation. Im Fall eines Körpers k ist dann der offensichtliche Funktor $n \mapsto k^n$ eine Äquivalenz von Kategorien zwischen unserer **Matrixkategorie** $\mathcal{M}_k$ und der Kategorie der endlich erzeugten k-Vektorräume

$$\mathcal{M}_k \xrightarrow{\approx} \mathrm{Modfg}_k$$

aber natürlich kein Isomorphismus von Kategorien. Diese Aussage faßt eine Vielzahl von Aussagen der linearen Algebra zusammen und illustriert meines Erachtens recht gut die Kraft und Eleganz der Sprache der Kategorientheorie. Wenn unser Ring k selbst durch einen größeren Ausdruck gegeben ist, schreiben wir für unsere Matrixkategorie statt $\mathcal{M}_k$ auch manchmal $\mathcal{M}(k)$.

Übung 10.2.22. Jede Äquivalenz von Kategorien induziert eine Bijektion zwischen den zugehörigen Isomorphieklassen von Objekten. Zum Beispiel werden die endlichdimensionalen k-Vektorräume klassifiziert durch ihre Dimension, alias durch Elemente von $\mathbb{N}$, alias durch Isomorphieklassen der Matrixkategorie.

Übung 10.2.23. Die Verknüpfung von zwei Äquivalenzen von Kategorien ist wieder eine Äquivalenz von Kategorien.

Übung 10.2.24. Bilden wir zu einer Kategorie eine volle Unterkategorie, indem wir aus jeder Isomorphieklasse von Objekten ein Objekt willkürlich auswählen, so ist der Einbettungsfunktor eine Äquivalenz von Kategorien.

Übung 10.2.25. Fassen wir ein Monoid G als eine Kategorie mit nur einem Objekt auf wie in 10.1.4, so ist ein Funktor von dieser Kategorie in die Kategorie der Mengen "dasselbe" wie eine G-Menge, wir haben also einen natürlichen Isomorphismus von Kategorien

$$G\text{-Ens} \xrightarrow{\sim} \mathrm{Cat}(G, \mathrm{Ens})$$

10.3 Transformationen

10.3.1. Bis hierher hat sich unsere Theorie noch in vertrauten Bahnen bewegt: Wir haben nur eine neue Art von Strukturen erklärt, die Kategorien, und dazwischen strukturerhaltende Abbildungen alias Morphismen betrachtet, die Funktoren. Insoweit paßt alles noch in den strukturellen Rahmen, an den man seit der linaren Algebra durch das Studium von Vektorräumen und linearen Abbildungen gewöhnt worden ist. Das Neue bei der Kategorientheorie ist nun, daß es auch "Morphismen von Morphismen" gibt. Sie heißen "Transformationen von Funktoren" und sind das Thema dieses Abschnitts.

Definition 10.3.2. Seien $\mathcal{A}, \mathcal{B}$ Kategorien und $F, G : \mathcal{A} \to \mathcal{B}$ Funktoren. Eine **Transformation** $\tau : F \Rightarrow G$ ist eine Vorschrift, die jedem Objekt $X \in \mathcal{A}$ einen Morphismus $\tau_X \in \mathcal{B}(FX, GX)$ zuordnet derart, daß für jeden Morphismus $f : X \to Y$ in $\mathcal{A}$ das folgende Diagramm in $\mathcal{B}$ kommutiert:

$$\begin{array}{ccc} FX & \xrightarrow{\tau_X} & GX \\ Ff \downarrow & & \downarrow Gf \\ FY & \xrightarrow{\tau_Y} & GY \end{array}$$

In Formeln meint dies "Kommutieren" die Gleichheit $(Gf) \circ \tau_X = \tau_Y \circ (Ff)$ in der Morphismenmenge $\mathcal{B}(FX, GY)$. Ob ein Doppelpfeil eine Transformation von Funktoren oder vielmehr eine Implikation meint, muß der Leser aus dem Kontext erschließen. Sind alle τ_X Isomorphismen, so nenne ich τ eine **Isotransformation**

und notiere sie $\stackrel{\sim}{\Rightarrow}$, aber diese Terminologie ist nicht gebräuchlich. In der Literatur spricht man eher von einem **Isomorphismus** oder auch von einer **Äquivalenz von Funktoren**. Gibt es zwischen zwei Funktoren eine Isotransformation, so heißen sie **isomorph**.

10.3.3. In der Literatur heißen unsere Transformationen meist "natürliche Transformationen". Diese Terminologie schien mir jedoch unnötig umständlich und entspricht auch nicht meinem Sprachempfinden: Ich möchte zum Beispiel unter der "natürlichen" Transformation des Identitätsfunktors auf der Kategorie aller $\mathbb{R}$-Vektorräume in den Bidualraumfunktor gerne die in 10.3.4 gegebene Transformation verstehen, die zwar keineswegs die einzige Transformation zwischen diesen Funktoren ist, aber wohl schon die "natürlichste".

Beispiel 10.3.4. Sei k ein Körper und $B : \mathrm{Mod}_k \to \mathrm{Mod}_k$ der Funktor, der jedem k-Vektorraum V seinen Bidualraum $BV := V^{\top\top}$ zuordnet. So liefern die Evaluationen $\mathrm{ev}_V : V \to V^{\top\top}$, $v \mapsto (f \mapsto f(v))$ eine Transformation $\mathrm{ev} : \mathrm{Id} \Rightarrow B$ und eine Isotransformation zwischen den Restriktionen dieser Funktoren auf die Kategorie der endlichdimensionalen k-Vektorräume, vergleiche 1.11.23.

Beispiel 10.3.5. Sei k ein Körper und $D : \mathrm{Mod}_k \to \mathrm{Mod}_k^{\mathrm{opp}}$ der Funktor, der jedem Raum seinen Dualraum zuordnet. Sei weiter $\mathcal{M} = \mathcal{M}(k)$ die Matrizenkategorie aus 10.2.21 und $T : \mathcal{M} \to \mathcal{M}^{\mathrm{opp}}$ der Funktor, der Matrizen transponiert. Sei schließlich $R : \mathcal{M} \to \mathrm{Mod}_k$ unser "Realisierungsfunktor" $n \mapsto k^n$ aus 10.2.21 und bezeichne R auch den entsprechenden Funktor zwischen den jeweils opponierten Kategorien. So erhalten wir eine Isotransformation

$$\tau : RT \stackrel{\sim}{\Rightarrow} DR$$

indem wir jeder natürlichen Zahl alias jedem Objekt $n \in \mathcal{M}$ den offensichtlichen Isomorphismus $\tau_n : k^n \xrightarrow{\sim} (k^n)^\top$ zuordnen. Es kann hilfreich sein, durch Doppelpfeile in Diagrammen von Kategorien und Funktoren klarzumachen, zwischen welchen Funktoren eine Transformation gemeint ist. So wäre etwa unser τ ein möglicher Doppelpfeil im Diagramm

$$\begin{array}{ccc} \mathcal{M} & \xrightarrow{T} & \mathcal{M}^{\mathrm{opp}} \\ {\scriptstyle R}\downarrow & \swarrow\!\!\swarrow & \downarrow{\scriptstyle R} \\ \mathrm{Mod}_k & \xrightarrow{D} & \mathrm{Mod}_k^{\mathrm{opp}} \end{array}$$

Beispiel 10.3.6. Die natürlichen Abbildungen

$$\mathrm{can} : V^* \otimes_k W \to \mathrm{Hom}_k(V, W)$$

aus 9.4.1 für k-Vektorräume V, W liefern eine Transformation zwischen den durch diese Vorschriften gegebenen Funktoren

$$\mathrm{Mod}_k^{\mathrm{opp}} \times \mathrm{Mod}_k \to \mathrm{Mod}_k$$

Sie liefern sogar eine Isotransformation, wenn wir uns im ersten Faktor auf endlichdimensionale Räume beschränken.

Übung 10.3.7. Man diskutiere, inwiefern die in 9.5.3 für jeden Vektorraum V konstruierten kanonischen Isomorphismen $(\bigwedge^r V)^\top \xrightarrow{\sim} \mathrm{Alt}^r(V)$ eine Isotransformation bilden. Idem für die in 9.5.16 für jeden endlichdimensionalen Vektorraum V konstruierten kanonischen Isomorphismen $\bigwedge^r(V^\top) \xrightarrow{\sim} \mathrm{Alt}^r(V)$.

Ergänzende Übung 10.3.8. Fassen wir ein Monoid G als eine Kategorie mit nur einem Objekt auf wie in 10.1.4 und Funktoren von dieser Kategorie in die Kategorie der Mengen als G-Mengen wie in 10.2.25, so ist eine Transformation zwischen unseren Funktoren "dasselbe" wie eine äquivariante Abbildung. Hierbei heißt eine Abbildung $\phi : X \to Y$ von G-Mengen **äquivariant** genau dann, wenn gilt $\phi(gx) = g\phi(x)$ für alle $g \in G$ und $x \in X$.

Ergänzende Übung 10.3.9. Wir erhalten eine Isotransformation zwischen Funktoren $\mathbb{C}\text{-Mod} \to \mathbb{C}\text{-Mod}$ vermittels der Abbildungen $\mathbb{C} \otimes_{\mathbb{R}} V \xrightarrow{\sim} V \oplus \overline{V}$ gegeben durch $\alpha \otimes v \mapsto (\alpha v, \alpha \bar{v})$ in den Notationen 4.6.14. Die inverse Isotransformation wird beschrieben durch die Abbildungsvorschrift

$$(v, \bar{w}) \mapsto (1/2) \otimes (v + w) - (\mathrm{i}/2) \otimes (\mathrm{i}v - \mathrm{i}w)$$

Ergänzende Übung 10.3.10. Wir erhalten eine Isotransformation zwischen Funktoren $\mathbb{C}\text{-Mod} \to \mathbb{C}\text{-Mod}^{\mathrm{opp}}$ vermittels der Abbildungen $\overline{V^*} \xrightarrow{\sim} \overline{V}^*$ gegeben durch $\bar{\varphi} \mapsto c \circ \varphi$ in den Notationen 4.6.14, mit $c : \mathbb{C} \to \mathbb{C}$ der komplexen Konjugation. Diese Identifikation scheint mir so kanonisch, daß ich auch oft $\bar{\varphi}$ statt $c \circ \varphi$ schreiben werde.

Ergänzung 10.3.11. Gegeben ein komplexer Vektorraum V erklären wir einen natürlichen Isomorphismus

$$\mathrm{res}^{\mathbb{R}}_{\mathbb{C}}(V^*) \xrightarrow{\sim} (\mathrm{res}^{\mathbb{R}}_{\mathbb{C}} V)^*$$

zwischen der Restriktion zu einem reellen Vektorraum seines Dualraums und dem Dualraum seiner Restriktion durch die Vorschrift $\lambda \mapsto 2\,\mathrm{Re}\,\lambda$. Dann kommutiert das Diagramm

$$\begin{array}{ccc} \mathbb{C} \otimes_{\mathbb{R}} (V^*) & \xrightarrow{\sim} & V^* \oplus \overline{V^*} \\ \downarrow \wr & & \downarrow \wr \\ (\mathbb{C} \otimes_{\mathbb{R}} V)^* & \xleftarrow{\sim} & V^* \oplus \overline{V}^* \end{array}$$

wo die Horizontalen von 10.3.9 herkommen, rechts die von 10.3.10 gelieferte Abbildung $(\lambda, \bar{\mu}) \mapsto (\lambda, c \circ \mu)$ gemeint ist mit $c : \mathbb{C} \to \mathbb{C}$ der komplexen Konjugation, und links die Abbildung, die aus obiger Identifikation $\operatorname{res}^{\mathbb{R}}_{\mathbb{C}}(V^*) \xrightarrow{\sim} (\operatorname{res}^{\mathbb{R}}_{\mathbb{C}} V)^*$ zusammen mit der Identifikation $(W^*)_{\mathbb{C}} \xrightarrow{\sim} (W_{\mathbb{C}})^*$ aus 9.3.27 entsteht. Der Faktor Zwei zu Beginn von 10.3.11 scheint mir nicht nur angemessen, da er obiges Diagramm zum Kommutieren bringt, sondern auch, da man allgemeiner für jede endliche separable Körpererweiterung vernünftigerweise einen natürlichen Isomorphismus $\operatorname{res}^k_K(V^*) \xrightarrow{\sim} (\operatorname{res}^k_K V)^*$ erklärt durch die Vorschrift $\lambda \mapsto S^k_K \circ \lambda$ für $S^k_K : K \to k$ die Spur aus **??**.

Ergänzende Übung 10.3.12. Wir erhalten eine Isotransformation von Funktoren $K\text{-Mod} \times K\text{-Mod} \to K\text{-Mod}$ vermittels der durch das Dachprodukt gegebenen Abbildungen

$$\bigoplus_{i+j=k} \bigwedge^i V \otimes \bigwedge^j W \xrightarrow{\sim} \bigwedge^k (V \oplus W)$$

Zusammen mit Übung 10.3.9 erhalten wir insbesondere Isotransformationen von Funktoren $\mathbb{C}\text{-Mod} \to \mathbb{C}\text{-Mod}$ alias für komplexe Vektorräume V kanonische Isomorphismen $\bigoplus_{i+j=k} \bigwedge^i V \otimes \bigwedge^j \overline{V} \xrightarrow{\sim} \bigwedge^k (\mathbb{C} \otimes_{\mathbb{R}} V)$.

Beispiel 10.3.13. Sind $\tau : F \Rightarrow G$ und $\sigma : G \Rightarrow H$ Transformationen, so ist auch $\sigma \circ \tau : F \Rightarrow H$ eine Transformation. Des weiteren gibt es für jeden Funktor die **identische Transformation** id von besagtem Funktor zu sich selber. Sind $\mathcal{A}, \mathcal{B}$ Kategorien, so bilden die Funktoren $\mathcal{A} \to \mathcal{B}$ selbst eine Kategorie, mit Funktoren als Objekten und Transformationen als Morphismen. Ich verwende für diese **Funktorkategorie** die Notation $\mathrm{Cat}(\mathcal{A}, \mathcal{B})$, so daß etwa für Funktoren $F, G : \mathcal{A} \to \mathcal{B}$ die Menge der Transformationen

$$\mathrm{Cat}(\mathcal{A}, \mathcal{B})(F, G)$$

notiert werden kann. Wenn die Kategorien selber durch größere Ausdrücke gegeben werden, sind für die Menge der Transformationen auch abkürzende Notationen wie etwa $\mathrm{Trans}(F, G)$ sinnvoll und üblich.

Beispiel 10.3.14. Seien $F, G : \mathcal{A} \to \mathcal{B}$ Funktoren und $\tau : F \Rightarrow G$ eine Transformation. Gegeben ein weiterer Funktor $H : \mathcal{B} \to \mathcal{C}$ erhalten wir in offensichtlicher Weise eine Transformation $H\tau : HF \Rightarrow HG$. Gegeben ein weiterer Funktor $K : \mathcal{D} \to \mathcal{A}$ erhalten wir in offensichtlicher Weise eine Transformation $\tau K : FK \Rightarrow GK$. Offensichtlich liefern diese Konstruktionen ihrerseits Funktoren $\mathrm{Cat}(\mathcal{A}, \mathcal{B}) \to \mathrm{Cat}(\mathcal{A}, \mathcal{C})$ und $\mathrm{Cat}(\mathcal{A}, \mathcal{B}) \to \mathrm{Cat}(\mathcal{D}, \mathcal{B})$ zwischen den entsprechenden Funktorkategorien, die wir als das **Nachschalten von** H bzw. **Vorschalten von** K bezeichnen.

Ergänzende Übung 10.3.15. Gegeben Funktoren $F, F' : \mathcal{A} \to \mathcal{B}$ und $G, G' : \mathcal{B} \to \mathcal{C}$ sowie Transformationen $\alpha : F \Rightarrow F'$ und $\beta : G \Rightarrow G'$ gilt die Gleichheit $\beta F' \circ G\alpha = G'\alpha \circ \beta F$ von Transformationen $GF \Rightarrow G'F'$. Wir notieren diese Transformation auch $\alpha * \beta : GF \Rightarrow G'F'$ und nennen sie die **Juxtaposition** unserer beiden Transformationen.

Übung 10.3.16. Sind $\mathcal{A}, \mathcal{B}$ Kategorien und ist $K : \mathcal{A}' \xrightarrow{\approx} \mathcal{A}$ eine Äquivalenz von Kategorien, so liefert das Vorschalten von K eine Äquivalenz von Funktorkategorien

$$\mathrm{Cat}(\mathcal{A}, \mathcal{B}) \xrightarrow{\approx} \mathrm{Cat}(\mathcal{A}', \mathcal{B})$$

Ist ähnlich $H : \mathcal{B} \xrightarrow{\approx} \mathcal{B}'$ eine Äquivalenz von Kategorien, so liefert das Nachschalten von H eine Äquivalenz von Funktorkategorien

$$\mathrm{Cat}(\mathcal{A}, \mathcal{B}) \xrightarrow{\approx} \mathrm{Cat}(\mathcal{A}, \mathcal{B}')$$

Ergänzende Übung 10.3.17. Man zeige, daß man für je drei Kategorien $\mathcal{A}, \mathcal{B}, \mathcal{C}$ einen Isomorphismus von Kategorien

$$\mathrm{Cat}(\mathcal{A}, \mathrm{Cat}(\mathcal{B}, \mathcal{C})) \xrightarrow{\sim} \mathrm{Cat}(\mathcal{A} \times \mathcal{B}, \mathcal{C})$$

erhält durch die Vorschrift $F \mapsto \tilde{F}$ mit $\tilde{F}(A, B) = (F(A))(B)$ auf Objekten und eine vom Leser zu spezifizierende Vorschrift auf Morphismen.

10.4 Produkte in Kategorien

Definition 10.4.1. Sei $\mathcal{C}$ eine Kategorie und $(X_i)_{i \in I}$ eine Familie von Objekten von $\mathcal{C}$. Ein **Produkt** der X_i ist ein Datum $(P, (p_i)_{i \in I})$ bestehend aus (1) einem Objekt $P \in \mathcal{C}$ und (2) Morphismen $p_i : P \to X_i$, den sogenannten **Projektionen**, derart daß gilt: Ist $Y \in \mathcal{C}$ ein Objekt und sind $q_i : Y \to X_i$ Morphismen, so gibt es genau einen Morphismus $q : Y \to P$ mit $p_i \circ q = q_i \quad \forall i \in I$. Wir notieren diesen Morphismus dann $q = (q_i)_{i \in I}$.

Beispiele 10.4.2. In der Kategorie der Mengen ist $P = \prod_{i \in I} X_i$ mit p_i den üblichen Projektionsabbildungen ein Produkt der X_i, vergleiche 6.2. Dasselbe gilt in der Kategorie der Vektorräume, vergleiche 6.2.6.

10.4.3. Produkte in Kategorien sind im wesentlichen eindeutig, falls sie existieren. Sind genauer $(P, (p_i))$ und $(\tilde{P}, (\tilde{p}_i))$ zwei mögliche Produkte der Objekte X_i, so gibt es aufgrund der universellen Eigenschaft von P genau ein $\tilde{p} : \tilde{P} \to P$ mit $p_i \circ \tilde{p} = \tilde{p}_i$ und ebenso genau ein $p : P \to \tilde{P}$ mit $\tilde{p}_i \circ p = p_i$. Weiter gibt es auch genau ein $f : P \to P$ mit $p_i \circ f = p_i$, und da sowohl $f = \mathrm{id}$ als auch $f = \tilde{p} \circ p$ diese Bedingung erfüllen, folgt $\tilde{p} \circ p = \mathrm{id}$. Ebenso erhalten wir $p \circ \tilde{p} = \mathrm{id}$, mithin

sind p und $\tilde{p}$ zueinander inverse Isomorphismen. Aufgrund dieser Eindeutigkeit sprechen wir ab jetzt meist von *dem* Produkt und notieren es

$$\left(\prod_{i\in I} X_i, (\mathrm{pr}_i)_{i\in I}\right)$$

oder im Fall endlicher Familien $X_1 \times \ldots \times X_n$ und benutzen für die Projektionen manchmal auch die Notation pr_{X_i}. Morphismen in das Produkt schreiben wir im Fall endlicher Familien auch $(q_1, \ldots, q_n)$. Sind schließlich Morphismen $f : X \to X'$, $g : Y \to Y'$ gegeben und existieren die Produkte $X \times Y$ und $X' \times Y'$, so benutzen wir die Abkürzung $(f \circ \mathrm{pr}_X, g \circ \mathrm{pr}_Y) = f \times g$ und nennen diesen Morphismus den **Produktmorphismus**

$$f \times g : X \times Y \to X' \times Y'$$

Beispiele 10.4.4. Das Produkt über eine leere Familie von Mengen erklärt man als "die" einpunktige Menge, damit das Bilden von Produkten von Mengen "assoziativ" wird in der Weise, daß wir bei einer Familie $(I_j)_{j\in J}$ von Indexmengen mit disjunkter Vereinigung $I = \bigsqcup_j I_j$ stets eine kanonische Bijektion

$$\prod_{i\in I} X_i \xrightarrow{\sim} \prod_{j\in J}\left(\prod_{i\in I_j} X_i\right)$$

haben. Das Produkt über eine leere Familie in einer beliebigen Kategorie $\mathcal{C}$ verstehen wir analog als "das" finale Objekt, da dann die offensichtliche Abbildung auch in diesem Fall Bijektionen $\mathcal{C}(Y, \prod_{i\in I} X_i) \xrightarrow{\sim} \prod_{i\in I} \mathcal{C}(Y, X_i)$ liefert. Wenn wir sagen, eine Kategorie **habe Produkte** oder auch nur endliche Produkte, so fordern wir insbesondere implizit die Existenz eines finalen Objekts.

Übung 10.4.5. Man präzisiere und zeige die "Assoziativität" von Produkten, die die Formel $(X \times Y) \times Z \cong X \times (Y \times Z)$ andeutet.

10.4.6. Produkte in der opponierten Kategorie heißen "Koprodukte". Im folgenden sprechen wir diese Definition explizit aus.

Definition 10.4.7. Sei $\mathcal{C}$ eine Kategorie und $(X_i)_{i\in I}$ eine Familie von Objekten aus $\mathcal{C}$. Ein **Koprodukt** der X_i ist ein Datum $(K, (\mathrm{in}_i)_{i\in I})$ bestehend aus einem Objekt $K \in \mathcal{C}$ und Morphismen $\mathrm{in}_i : X_i \to K$ derart, daß gilt: Ist $Z \in \mathcal{C}$ ein Objekt und sind $f_i : X_i \to Z$ Morphismen, so gibt es genau einen Morphismus $f : K \to Z$ mit $f \circ \mathrm{in}_i = f_i \quad \forall i \in I$. Wir notieren diesen Morphismus dann auch $(f_i)_{i\in I}$ und hoffen, daß der Leser aus dem Kontext erschließen kann, wann damit ein Morphismus aus einem Koprodukt und wann ein Morphismus in ein Produkt gemeint ist. Wir notieren Koprodukte $\bigsqcup_{i\in I} X_i$.

Beispiele 10.4.8. In der Kategorie der Mengen ist das Koprodukt die disjunkte Vereinigung $\bigsqcup_{i\in I} X_i$, vergleiche 6.2.2. In der Kategorie der Vektorräume über einem vorgegebenen Körper ist das Koprodukt die direkte Summe, vergleiche 6.2.6.

Ergänzende Übung 10.4.9. Sei k ein Körper. Man zeige, daß in der Kategorie der k-Kringalgebren das Tensorprodukt ein Koprodukt ist, sofern die Multiplikation auf $A \otimes B$ durch $(a \otimes b)(a' \otimes b') = aa' \otimes bb'$ erklärt wird und die kanonischen Morphismen durch $a \mapsto a \otimes 1$ und $b \mapsto 1 \otimes b$. Man zeige weiter, daß die analoge Aussage in der Kategorie der k-Ringalgebren nicht richtig ist.

Ergänzung 10.4.10. Für die algebraisch Gebildeten unter Ihnen sei bemerkt, daß in der Kategorie Kring der kommutativen Ringe das Tensorprodukt über $\mathbb{Z}$ im Sinne von **??** ein Koprodukt ist, sofern die Multiplikation auf $A \otimes B$ durch $(a \otimes b)(a' \otimes b') = aa' \otimes bb'$ erklärt wird und die kanonischen Morphismen durch $a \mapsto a \otimes 1$ und $b \mapsto 1 \otimes b$.

10.5 Yoneda-Lemma*

10.5.1. Einen Funktor von einer Kategorie $\mathcal{C}$ in eine Kategorie von Mengen nennen wir kurz einen **Mengenfunktor auf** $\mathcal{C}$. Gegeben ein Mengensystem $\mathfrak{U}$ verstehen wir unter einer **$\mathfrak{U}$-Kategorie** eine Kategorie $\mathcal{C}$, bei der für alle Objekte $X, Y \in \mathcal{C}$ die Morphismenmenge zu unserem Mengensystem $\mathfrak{U}$ gehört, in Formeln $\mathcal{C}(X,Y) \in \mathfrak{U}$. Der Bequemlichkeit halber fordern wir gleich mit, daß die Menge der Objekte unserer Kategorie eine Teilmenge von $\mathfrak{U}$ ist, in Formeln $\mathcal{C} \subset \mathfrak{U}$. Das ist unproblematisch, da wir ja andernfalls schlicht unsere Objekte mit ihren Identitätsmorphismen identifizieren können. Gegeben eine $\mathfrak{U}$-Kategorie $\mathcal{C}$ bildet die Menge aller Funktoren $\mathcal{C} \to \mathfrak{U}\mathrm{Ens}$ mit den Transformationen als Morphismen wieder eine Kategorie. Die zur Kategorie dieser "Mengenfunktoren" auf $\mathcal{C}$ opponierte Kategorie

$$\mathcal{C}^\wedge := \mathrm{Cat}(\mathcal{C}, \mathfrak{U}\mathrm{Ens})^{\mathrm{opp}}$$

kann man als eine Art "Vervollständigung" von $\mathcal{C}$ interpretieren, da nämlich, wie das gleich anschließende Yoneda-Lemma 10.5.2 zeigt, die Vorschrift $X \mapsto \mathcal{C}(X, \ )$ einen volltreuen Funktor $\mathcal{C} \to \mathcal{C}^\wedge$ definiert.

Proposition 10.5.2 (Yoneda-Lemma). *Sei $\mathfrak{U}$ ein Mengensystem, $\mathcal{C}$ eine $\mathfrak{U}$-Kategorie, $X \in \mathcal{C}$ ein Objekt und $F : \mathcal{C} \to \mathfrak{U}\mathrm{Ens}$ ein Mengenfunktor auf $\mathcal{C}$. So liefert die Abbildungsvorschrift $\tau \mapsto \tau_X(\mathrm{id}_X)$ eine Bijektion*

$$\mathrm{Trans}(\mathcal{C}(X, \ ), F) \xrightarrow{\sim} F(X)$$

zwischen der Menge der Transformationen $\mathcal{C}(X, \ ) \Rightarrow F$ und der Menge $F(X)$.

Ergänzung 10.5.3. Im Spezialfall einer Kategorie $\mathcal{C}$ mit nur einem Objekt X ist diese Aussage besonders leicht einzusehen: Sie besagt dann im Lichte von 10.3.8, daß die äquivarianten Abbildungen von einem Monoid G in eine beliebige G-Menge F festgelegt und festlegbar sind durch das Bild des neutralen Elements. Im weiteren lassen wir das Mengensystem $\mathfrak{U}$ wieder in den Hintergrund treten und ignorieren es meist in unserer Notation.

Beweis. Wir konstruieren zunächst eine Abbildung in die andere Richtung. Für beliebiges $a \in F(X)$ betrachten wir dazu die Abbildungen

$$\begin{array}{rccc} \tau_Y : & \mathcal{C}(X,Y) & \to & F(Y) \\ & f & \mapsto & (Ff)(a) \end{array}$$

Man prüft ohne Schwierigkeiten, daß sie eine Transformation $\tau : \mathcal{C}(X, \ ) \Rightarrow F$ bilden, die wir mit $\hat{\tau}(a)$ bezeichnen. Jetzt gilt es nur noch zu zeigen, daß die Abbildung $a \mapsto \hat{\tau}(a)$ invers ist zu unserer Abbildung $\tau \mapsto \hat{a}(\tau) = \tau_X(\mathrm{id}_X)$ aus dem Theorem. Dafür müssen wir also prüfen, daß gilt $a = \hat{a}(\hat{\tau}(a))$ für alle $a \in F(X)$ und $\tau = \hat{\tau}(\hat{a}(\tau))$ für alle Transformationen $\tau : \mathcal{C}(X, \ ) \Rightarrow F$. Das überlassen wir dem Leser. □

Übung 10.5.4. Sei k ein endlicher Körper und $\mathcal{M}_k$ die Matrixkategorie aus 10.2.21 und $\mathfrak{U}$ eine Menge derart, daß $\mathcal{M}_k$ eine $\mathfrak{U}$-Kategorie ist. Gilt $X \in \mathfrak{U} \Rightarrow |X| < \infty$, so ist der offensichtliche Funktor eine Äquivalenz

$$\mathcal{M}_k \xrightarrow{\approx} \mathcal{M}_k^\wedge = \mathrm{Cat}(\mathcal{M}_k, \mathfrak{U}\,\mathrm{Ens})^{\mathrm{opp}}$$

Gibt es zwar unendliche, aber keine überabzählbaren Mengen $X \in \mathfrak{U}$, so ist $\mathcal{M}_k^\wedge = \mathrm{Cat}(\mathcal{M}_k, \mathfrak{U}\mathrm{Ens})^{\mathrm{opp}}$ äquivalent zur Kategorie aller abzählbaren k-Vektorräume. Analoge Aussagen gelten für andere Kardinalitäten und mutatis mutandis auch für unendliche Körper.

Definition 10.5.5. Diejenigen Mengenfunktoren auf $\mathcal{C}$, die isomorph sind zu Mengenfunktoren im Bild von $\mathcal{C} \to \mathcal{C}^\wedge$, heißen **darstellbare Funktoren**. Ist ein Mengenfunktor $F : \mathcal{C} \to \mathrm{Ens}$ isomorph zu $\mathcal{C}(X, \ )$ für ein $X \in \mathcal{C}$, so sagen wir, der **Funktor** F **werde dargestellt durch das Objekt** X**.** Ist noch genauer $F : \mathcal{C} \to \mathrm{Ens}$ ein Mengenfunktor und $X \in \mathcal{C}$ ein Objekt und $a \in F(X)$ ein Element, das unter der Bijektion aus dem Yoneda-Lemma einer Isotransformation $\mathcal{C}(X, \ ) \stackrel{\sim}{\Rightarrow} F$ entspricht, so sagen wir, der **Funktor** F **werde strikt dargestellt durch das Paar** (X, a). Oft lassen wir das "strikt" aber auch weg.

Übung 10.5.6. Wird ein Mengenfunktor $F : \mathcal{C} \to \mathrm{Ens}$ strikt dargestellt durch das Paar (X, a) und durch das Paar (Y, b), so gibt es genau einen Isomorphismus $i : X \xrightarrow{\sim} Y$ mit der Eigenschaft $F(i) : a \mapsto b$.

Beispiel 10.5.7. Der Vergißfunktor von den k-Vektorräumen in die Mengen wird dargestellt durch das Paar $(k, 1)$ oder auch durch jeden anderen eindimensionalen Vektorraum mit einem von Null verschiedenen Element.

Beispiel 10.5.8. Der Vergißfunktor von den Gruppen in die Mengen wird dargestellt durch das Paar $(\mathbb{Z}, 1)$ oder auch durch jedes andere Paar (Z, g) bestehend aus einer unendlich zyklischen Gruppe und einem Erzeuger.

Beispiel 10.5.9. Sei k ein Körper und seien V, W zwei k-Vektorräume. Der Funktor der bilinearen Abbildungen $\mathrm{Mod}_k \to \mathrm{Ens}$, $L \mapsto \mathrm{Hom}_k^{(2)}(V \times W, L)$ wird dargestellt durch das Paar $(V \otimes W, \tau)$ mit $\tau : V \times W \to V \otimes W$ der kanonischen bilinearen Abbildung aus 9.3.2. Diese Aussage ist nur eine Umformulierung der universellen Eigenschaft des Tensorprodukts aus 9.3.4.

Übung 10.5.10. Seien k ein Körper, V ein k-Vektorraum, und $U \subset V$ ein Teilraum. Welchen Mengenfunktor stellt der Quotient V/U dar?

Ergänzende Übung 10.5.11. Welchen Mengenfunktor stellt das Produkt im Sinne von 10.5.5 dar?

10.5.12. Dual zu $\mathcal{C}^\wedge$ kann man natürlich für jede Kategorie $\mathcal{C}$ auch die Kategorie $\mathcal{C}^\vee := \mathrm{Cat}(\mathcal{C}, \mathrm{Ens}^{\mathrm{opp}})$ aller kontravarianten Funktoren $\mathcal{C} \to \mathrm{Ens}$ betrachten und erhält mit $X \mapsto \mathcal{C}(\ , X)$ eine volltreue Einbettung $\mathcal{C} \to \mathcal{C}^\vee$.

Übung 10.5.13. Sei k ein Körper und $\mathrm{Id} : \mathrm{Mod}_k \to \mathrm{Mod}_k$ der Identitätsfunktor. Man bestimme alle Transformationen von diesem Funktor zu sich selber. Ebenso bestimme man alle Transformationen von diesem Funktor zum Bidualraumfunktor.

Übung 10.5.14. Sind zwei Funktoren isomorph und ist der Eine eine Äquivalenz von Kategorien, so auch der Andere.

Übung 10.5.15. Man zeige: Genau dann ist ein Funktor $F : \mathcal{A} \to \mathcal{B}$ eine Äquivalenz von Kategorien, wenn es einen Funktor $G : \mathcal{B} \to \mathcal{A}$ gibt derart, daß FG isomorph ist zum Identitätsfunktor auf $\mathcal{B}$ und GF isomorph zum Identitätsfunktor auf $\mathcal{A}$. Ist des weiteren (G, α) ein Paar bestehend aus einem Funktor $G : \mathcal{B} \to \mathcal{A}$ und einer Isotransformation $\alpha : \mathrm{Id} \xRightarrow{\sim} GF$, und ist (G', α') ein weiteres derartiges Paar, so existiert genau eine Isotransformation $\eta : G \xRightarrow{\sim} G'$ mit $\eta F \circ \alpha = \alpha'$. Ein solches Paar (G, α) ist also salopp gesprochen "eindeutig bis auf eindeutigen Isomorphismus". Wir nennen dann den Funktor G oder genauer das Paar Paar (G, α) einen **quasi-inversen Funktor** zu F.

Ergänzung 10.5.16. Ein Zugang zu der von Grothendieck konstruierten Kategorie der **Schemata** ist es, diese Kategorie zu realisieren als volle Unterkategorie der Kategorie $\mathrm{Kring}^\wedge$, die wir erhalten, wenn wir die Kategorie der kommutativen Ringe mit der nötigen Sorgfalt bei Fragen der Mengenlehre in der oben erklärten Weise vervollständigen. Der affine Raum der Dimension n wird dann

zum Beispiel definiert als der Funktor, der jedem kommutativen Ring R die Menge R^n zuordnet, und der projektive Raum der Dimension n als der Funktor, der jedem kommutativen Ring R die Menge derjenigen direkten Summanden D des R-Moduls R^{n+1} zuordnet, die "vom Rang Eins" sind in dem Sinne, daß "bei jedem Primideal $\mathfrak{p} \subset R$ ihre Lokalisierung $D_\mathfrak{p}$ ein freier $R_\mathfrak{p}$-Modul vom Rang Eins ist". Man kann mit Schemata so effizient und geometrisch arbeiten, daß sie mittlerweile zum eigentlichen Arbeitspferd der sogenannten "algebraischen Geometrie" geworden sind.

Kapitel III

Gruppen, Ringe, Körper

Die Abschnitte bis zur Galois-Theorie einschließlich sollten in etwa den Standard-Stoff einer Algebra-Vorlesung für das dritte Semester abdecken. Ich habe mich besonders darum bemüht, die Verwendung des Zorn'schen Lemmas zu vermeiden, um nicht den falschen Eindruck zu erwecken, unsere Sätze über die Auflösbarkeit von polynomialen Gleichungen oder die Bestimmung quadratischer Reste oder die Konstruierbarkeit regelmäßiger Vielecke basierten auf Subtilitäten der Mengenlehre. Insbesondere wird der algebraische Abschluß in den Beweisen nicht verwendet und der Begriff eines maximalen Ideals wird gar nicht erst betrachtet. Ich bedanke mich bei vielen Freiburger Studierenden für Hinweise, die mir geholfen haben, die Darstellung zu klären und zu glätten und Fehler zu beheben. Regina Tammler hat durch ihre fundamentalen didaktischen Anregungen viel zur Lesbarkeit beigetragen.

Inhalt

1 Mehr zu Gruppen

1.1 Die Frage nach der Klassifikation

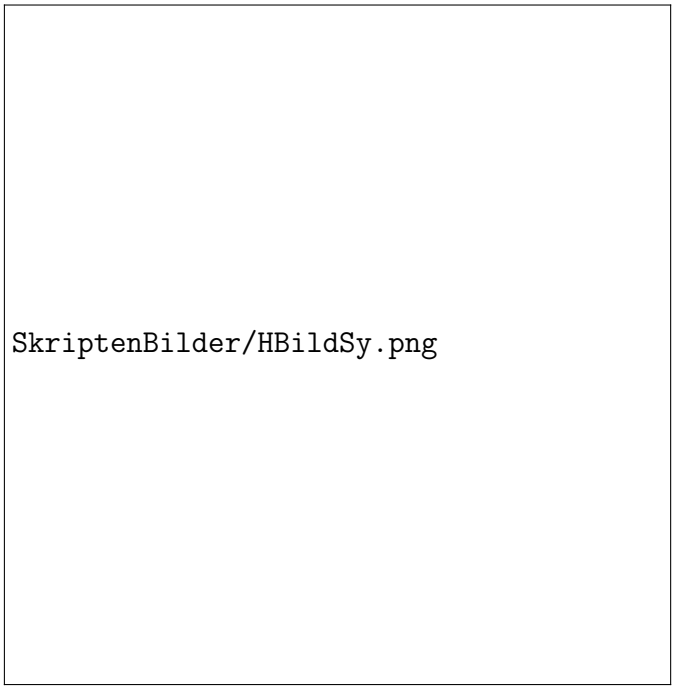
1.1.1. Ich erinnere an die Definition I.3.2.2 einer Gruppe. Wir wollen im Folgenden der Frage nachgehen, welche Gruppen es überhaupt gibt. Präziser nennen wir zwei Gruppen **isomorph** genau dann, wenn es zwischen ihnen einen Isomorphismus im Sinne von I.3.3.8 gibt. Die Frage, welche endlichen Gruppen es überhaupt gibt, können wir dann konkret fassen als die folgende Aufgabe: Man gebe eine Liste von endlichen Gruppen an derart, daß jede beliebige endliche Gruppe isomorph ist zu genau einer Gruppe dieser Liste. In mathematischer Terminologie ist das die Frage nach der **Klassifikation der endlichen Gruppen**.

Beispiel 1.1.2. Für Gruppen mit höchstens 4 Elementen können wir diese Aufgabe noch ohne alle Theorie auf direktem Wege lösen. Eine endliche Menge mit Verknüpfung beschreiben wir dazu durch ihre Verknüpfungstabelle, die im Fall einer Gruppe auch **Gruppentafel** heißt. Zum Beispiel bilden die dritten Einheitswurzeln $1, \zeta = \exp(2\pi\,\mathrm{i}\,/3), \eta = \exp(4\pi\,\mathrm{i}\,/3)$ in $\mathbb{C}$ unter der Multiplikation eine Gruppe mit der Gruppentafel

	1	ζ	η
1	1	ζ	η
ζ	ζ	η	1
η	η	1	ζ

Haben wir eine Gruppentafel vor uns, so muß nach der Kürzungsregel I.3.2.13 in jeder Spalte und in jeder Zeile jedes Element genau einmal vorkommen. Man sieht so recht leicht, daß es bis auf Isomorphismus nur eine Gruppe G gibt mit $|G|$ Elementen für $|G| = 1, 2, 3$, und daß es für $|G| = 4$ bis auf Isomorphismus genau zwei Möglichkeiten gibt, die sich dadurch unterscheiden, ob jedes Element sein eigenes Inverses ist oder nicht: Je nachdem haben wir, bis auf Isomorphismus, die sogenannte **Klein'sche Vierergruppe** $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ oder die zyklische Gruppe $\mathbb{Z}/4\mathbb{Z}$ vor uns.

1.1.3. Warum interessieren wir uns überhaupt für Gruppen? Stellen wir uns doch einmal eine ebene Figur vor, zum Beispiel eine stilisierte Blüte, einen Buchstaben, oder allgemein eine beliebige Teilmenge der Ebene $A \subset \mathbb{R}^2$. Unter einer "Symmetriebewegung" oder kurz **Symmetrie** unserer Figur verstehen wir eine abstandserhaltende Selbstabbildung g der Ebene, die unsere Figur in sich selber überführt, in Formeln $gA = A$. Alle Symmetrien unserer Figur bilden unter der Hintereinanderausführung als Verknüpfung eine Gruppe, die **Symmetriegruppe** der Figur. Bei den meisten Figuren besteht die Symmetriegruppe nur aus einem



Die vier Symmetrien des Buchstabens H und des Sonnenrads, das wohl nicht zuletzt auch wegen seiner Symmetriegruppe so unvermittelt an furchtbare Zeiten der deutschen Geschichte erinnert.

Element, der Identität, aber ein Herz hat schon zwei Symmetrien, die Identität und eine Spiegelung. Der Buchstabe H hat sogar 4 Symmetrien, ebensoviele wie das Sonnenrad, aber die Symmetriegruppen dieser beiden Figuren sind nicht isomorph. In diesem Sinne kann man das Konzept einer Gruppe interpretieren als eine Formalisierung der Idee eines "abstrakten Symmetrietyps".

1.2 Kompositionsreihen

1.2.1. Ich erinnere an Restklassen II.7.1, Normalteiler II.7.2, Gruppenwirkungen II.8.1.1, Bahnformel II.8.2 und Konjugationsklassen II.8.3.

Definition 1.2.2. Eine Gruppe heißt **einfach** genau dann, wenn sie nicht nur aus dem neutralen Element besteht, aber außer dem neutralen Element und der ganzen Gruppe keine weiteren Normalteiler hat.

Beispiele 1.2.3. Beispiele einfacher Gruppen sind die zyklischen Gruppen von Primzahlordnung und die sogenannten **alternierenden Gruppen** $A_r = \ker(\mathrm{sgn} : \mathcal{S}_r \to \{\pm 1\})$ aller geraden Permuationen von $r \geq 5$ Objekten, wie wir als Satz 1.6.2 zeigen werden. Nicht zeigen werden wir, daß die alternierende Gruppe A_5 die kleinste nichtabelsche einfache Gruppe ist. Diese Gruppe ist übrigends genau unsere Ikosaedergruppe aus II.8.4.1 aller Drehsymmetrien eines Ikosaeders, was wir im anschließenden Satz 1.2.5 zeigen.

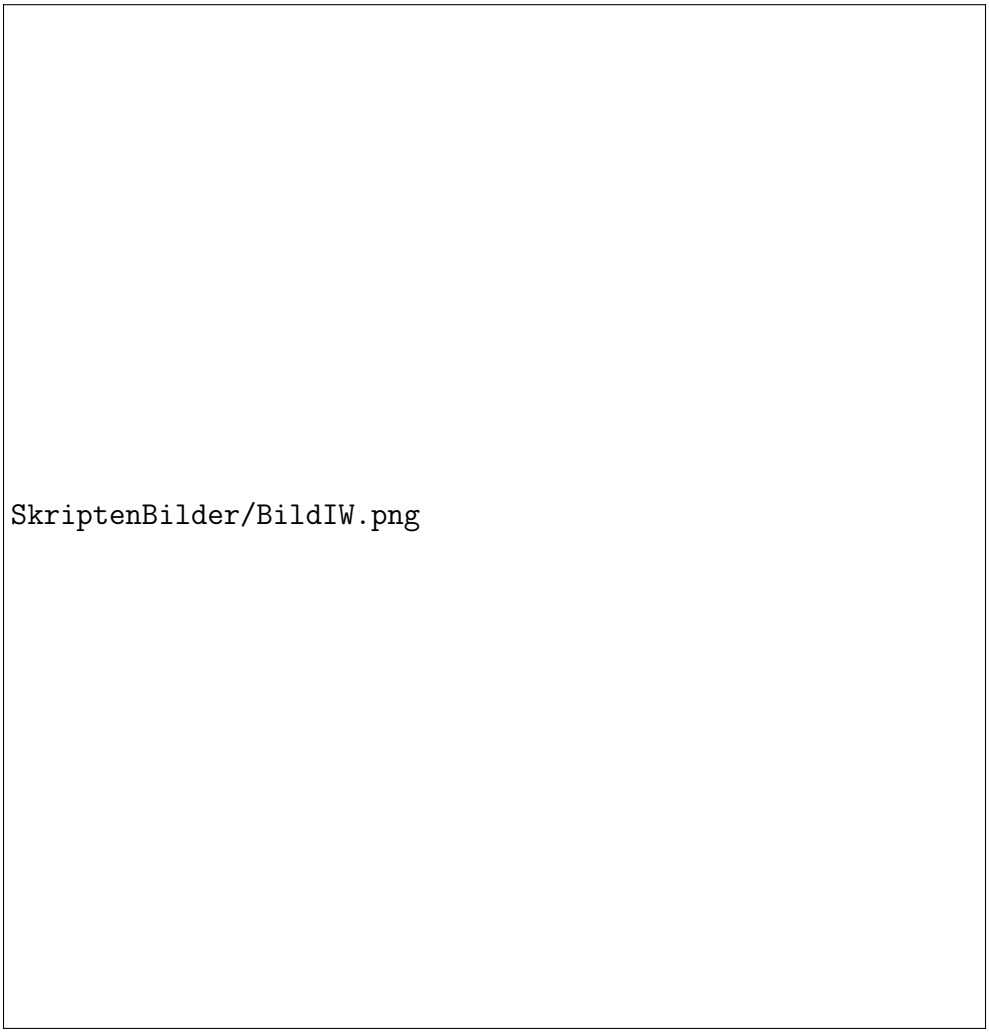
Ergänzung 1.2.4. Alle endlichen einfachen Gruppen sind seit etwa 1980 bekannt, ihre Klassifikation ist jedoch schwierig und man kann nur hoffen, daß zukünftige Forschungen noch substantielle Vereinfachungen der Argumente erlauben. Eine wesentliche Zutat ist ein berühmter Satz von **Feit-Thompson**, nach dem jede endliche einfache nicht abelsche Gruppe gerade Ordnung haben muß.

Satz 1.2.5. *Die Ikosaedergruppe ist einfach und isomorph zur alternierenden Gruppe* A_5.

Beweis. Ein Ikosaeder hat 12 Ecken, 20 Flächen und 30 Kanten. Jedes Paar von gegenüberliegenden Ecken liefert vier Elemente der Ordnung 5 in I, macht 24 Elemente der Ordnung 5. Jedes Paar von gegenüberliegenden Flächen liefert zwei Elemente der Ordnung 3 in I, macht 20 Elemente der Ordnung 3. Jedes Paar von gegenüberliegenden Kanten liefert ein Element der Ordnung 2 in I, macht 15 Elemente der Ordnung 2. Zusammen mit dem neutralen Element haben wir damit alle Gruppenelemente aufgelistet, denn es gilt

$$60 = 1 + 15 + 20 + 24$$

Da je zwei Kanten des Ikosaeders durch eine Drehsymmetrie des Ikosaeders ineinander überführt werden können, bilden die 15 Elemente der Ordnung 2 eine



Einer der fünf eingeschriebenen Würfel eines Dodekaeders, mit gestrichelt eingezeichneten Kanten. Diese Würfel entsprechen im übrigen auch eineindeutig den 2-Sylows unserer Ikosaedergruppe: Diese sind genau die vierelementigen Diedergruppen, die von den drei durch die Flächenmitten eines festen Würfels stechenden Geraden jede in sich überführen. Wenn Sie dieser Anschauung nicht so recht trauen, wofür ich durchaus Sympathie hätte, können Sie auch abstrakt die "Symmetriegruppe der Graphen mit den durchgezogenen Kanten" betrachten. Sie würde den "Dreh- und Spiegelsymmetrien" eines Ikosaeders entsprechen, aber wenn Sie zusätzlich an jeder Ecke auf der Menge der von ihr ausgehenden Kanten in der Terminologie I.2.2.32 die zyklische Anordnung "im Uhrzeigersinn" festlegen, so wird die Gruppe derjenigen Symmetrien unseres Graphen, die diese zyklischen Anordnungen respektieren, genau die Ikosaedergruppe werden.

Konjugationsklasse. Ähnlich sieht man, daß alle 20 Elemente der Ordnung 3 eine Konjugationsklasse bilden. Für die Elemente der Ordnung 5 kann das nicht gelten, denn 24 ist kein Teiler von 60. Mit ähnlichen Überlegungen erkennt man jedoch, daß die 24 Elemente der Ordnung 5 zerfallen in zwei Konjugationsklassen von je 12 Elementen, bestehend aus Drehungen einmal um Winkel $\pm\frac{2\pi}{5}$ und ein andermal $\pm\frac{4\pi}{5}$. Die Kardinalitäten der Konjugationsklassen sind also genau die Summanden auf der rechten Seite der Gleichung

$$60 = 1 + 15 + 20 + 12 + 12$$

Gäbe es nun in I einen echten Normalteiler N, so müßte die Ordnung von N ein Teiler sein von 60 und eine Summe von Kardinalitäten von Konjugationsklassen, darunter die Konjugationsklasse des neutralen Elements. Die einzigen solchen Zahlen sind aber 1 und 60, folglich ist die Ikosaedergruppe I einfach. Man überlegt sich nun anhand der nebenstehenden Zeichnung, daß es genau fünf Möglichkeiten gibt, aus den 20 Ecken eines Dodekaeders, die ja gerade die Flächenmitten eines Ikosaeders bilden, 8 Ecken so auszusuchen, daß sie die Ecken eines Würfels bilden: Auf der Menge dieser 5 einbeschriebenen Würfel operiert unsere Gruppe dann natürlich auch. Wir erhalten so einen Gruppenhomomorphismus

$$\varphi : I \to \mathcal{S}_5$$

Der Kern von $\operatorname{sgn} \circ \varphi : I \to \{+1, -1\}$ ist ein von 1 verschiedener Normalteiler von I, es folgt $\ker(\operatorname{sgn} \circ \varphi) = I$ und φ induziert einen Gruppenhomomorphismus nach $A_5 = \ker(\operatorname{sgn}) \subset \mathcal{S}_5$. Der Kern von $\varphi : I \to \mathcal{S}_5$ ist ein von I verschiedener Normalteiler von I, es folgt $\ker \varphi = 1$, und durch Abzählen folgt dann, daß φ einen Isomorphismus $\varphi : I \xrightarrow{\sim} A_5$ induziert. □

Definition 1.2.6. Eine **Kompositionsreihe** einer Gruppe G ist eine Folge von Untergruppen

$$G = G_r \supset G_{r-1} \supset \ldots \supset G_0 = 1$$

derart, daß jede Gruppe unserer Folge ein Normalteiler in der nächstgrößeren Gruppe ist und daß die sukzessiven Quotienten einfach sind, in Formeln G_i/G_{i-1} einfach ist für $1 \leq \mathrm{i} \leq r$. Die Gruppen G_i/G_{i-1} heißen die **Subquotienten** der Kompositionsreihe.

Satz 1.2.7 (Jordan-Hölder). *Je zwei Kompositionsreihen einer endlichen Gruppe haben dieselbe Länge und bis auf Reihenfolge isomorphe Subquotienten, die man die* **Kompositionsfaktoren** *unserer Gruppe nennt. Ist genauer G eine endliche Gruppe und sind $G = M_r \supset \ldots \supset M_0 = 1$ und $G = N_s \supset \ldots \supset N_0 = 1$ Kompositionsreihen von G, so haben wir $r = s$ und es gibt eine Permutation $\sigma \in \mathcal{S}_r$ mit $N_i/N_{i-1} \cong M_{\sigma(i)}/M_{\sigma(i)-1}$ für alle i.*

Ergänzende Übung 1.2.8. Man zeige die Aussage des Satzes, ohne die Endlichkeit der Gruppe vorauszusetzen. Man zeige auch, daß in einer Gruppe mit Kompositionsreihe eine absteigende Folge von Untergruppen, die jeweils echte Normalteiler in der nächstgrößeren Untergruppe sind, höchstens so lang sein kann wie besagte Kompositionsreihe.

Beispiel 1.2.9. Jede abelsche Gruppe mit n Elementen hat als Kompositionsfaktoren die zyklischen Gruppen $\mathbb{Z}/p_i\mathbb{Z}$ für $n = p_1 \dots p_r$ die Primfaktorzerlegung von n. Jeder endlichdimensionale Vektorraum V über $\mathbb{F}_p$ für eine Primzahl p hat insbesondere als Kompositionsfaktoren $\dim V$ Kopien von $\mathbb{F}_p$. Die Kompositionsfaktoren der symmetrischen Gruppen $\mathcal{S}_r$ werden wird in 1.6.2 und 1.6.3 diskutieren: Ab $r = 5$ ist der Kern des Signums ein einfacher Normalteiler und unsere Gruppe hat folglich nur zwei Kompositionsfaktoren: Diesen Normalteiler und $\mathbb{Z}/2\mathbb{Z}$.

Beweis. Wir zeigen das durch Induktion über die Gruppenordnung. Seien

$$\begin{array}{ccccccc} G & \supset & M & \supset & \dots & \supset & 1 \\ G & \supset & N & \supset & \dots & \supset & 1 \end{array}$$

zwei Kompositionsreihen. Gilt $M = N$, so folgt der Satz per Induktion. Sonst ist das Bild von M in G/N ein von 1 verschiedener Normalteiler, und da G/N einfach ist, liefert die offensichtliche Abbildung notwendig eine Surjektion $M \twoheadrightarrow G/N$ und einen Isomorphismus $M/(M \cap N) \xrightarrow{\sim} G/N$. Ebenso erhalten wir auch $N/(M \cap N) \xrightarrow{\sim} G/M$. Deuten wir mit $(M \cap N) \supset \dots \supset 1$ eine Kompositionsreihe des Schnitts an, so hat die Gruppe G also Kompositionsreihen

$$\begin{array}{ccccccccc} G & \supset & M & \supset & & & \dots & \supset & 1 \\ G & \supset & M & \supset & (M \cap N) & \supset & \dots & \supset & 1 \\ G & \supset & N & \supset & (M \cap N) & \supset & \dots & \supset & 1 \\ G & \supset & N & \supset & & & \dots & \supset & 1 \end{array}$$

und je zwei in dieser Liste benachbarte Kompositionsreihen haben nach Induktionsvoraussetzung und den oben erwähnten Isomorphismen bis auf Reihenfolge dieselben Subquotienten. □

Ergänzende Übung 1.2.10. Man zeige: Sind N und B Gruppen und $\tau : B \to \mathrm{Grp}^\times N$ ein Gruppenhomomorphismus alias eine Operation von B auf N durch Gruppenautomorphismen, notiert $(\tau(a))(n) = ({}^a n)$, so kann man $N \times B$ mit einer Gruppenstruktur versehen vermittels der Vorschrift

$$(m, a)(n, b) = (m\ ({}^a n), ab)$$

Diese Gruppe heißt das oder genauer ein **semidirektes Produkt** von N mit B und wird auch notiert als

$$N \rtimes B = N \rtimes_\tau B$$

Man zeige weiter: Ist $\varphi : G \twoheadrightarrow B$ ein surjektiver Gruppenhomomorphismus, N sein Kern und $\psi : B \to G$ eine Spaltung von φ, so erhalten wir einen Gruppenhomomorphismus $\tau : B \to \mathrm{Grp}^\times N$ durch $(\tau(b))(n) = \psi(b)n\psi(b)^{-1}$ und die Abbildung $(n, b) \mapsto n\psi(b)$ definiert einen Gruppenisomorphismus

$$N \rtimes B \xrightarrow{\sim} G$$

Ergänzung 1.2.11. Ist speziell eine Gruppe N ein Produkt von n Kopien einer festen Gruppe $N = A^n = A \times \ldots \times A$ und operiert eine weitere Gruppe B darauf durch Vertauschung der Faktoren, also in hoffentlich offensichtlicher Weise vermittels eines Gruppenhomomorphismus $B \to \mathcal{S}_n$, so bezeichnet man das zugehörige semidirekte Produkt auch als **Kranzprodukt** und notiert es $N \rtimes B = A \wr B$.

1.3 Symmetrische Gruppen

Definition 1.3.1. Eine **Partition λ einer natürlichen Zahl** $n \in \mathbb{N}$ ist eine monoton fallende Folge von natürlichen Zahlen $\lambda_1 \geq \lambda_2 \geq \ldots$ derart, daß fast alle Folgenglieder verschwinden und die von Null verschiedenen Folgenglieder sich zu n aufsummieren. Die Menge aller Partitionen von n notieren wir $\mathcal{P}_n$.

Beispiel 1.3.2. Die Zahl 5 hat die sieben Partitionen

$$\begin{array}{rcl} 5 & = & 5 \\ 5 & = & 4+1 \\ 5 & = & 3+2 \\ 5 & = & 3+1+1 \\ 5 & = & 2+2+1 \\ 5 & = & 2+1+1+1 \\ 5 & = & 1+1+1+1+1 \end{array}$$

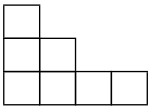
Hier haben wir nur die von Null verschiedenen Folgenglieder aufgeschrieben und sie durch $+$ getrennt. Formal meinen wir zum Beispiel im vierten Fall die Folge $3, 1, 1, 0, 0, \ldots$

Ergänzung 1.3.3. Eine geschickte Art, Partitionen zu veranschaulichen, sind die sogenannten Youngdiagramme. Unter einem **Youngdiagramm** verstehen wir eine endliche Teilmenge $T \subset \mathbb{N} \times \mathbb{N}$ mit der Eigenschaft

$$((i, j) \in T \text{ und } i' \leq i \text{ und } j' \leq j) \quad \Rightarrow \quad (i', j') \in T$$

Die Elemente von T nennen wir die "Kästchen" unseres Youngdiagramms und stellen uns ein Element (i, j) vor als das Kästchen auf einem Rechenpapier, bei

dem die Koordinaten der linken unteren Ecke gerade (i, j) sind. Zum Beispiel stellt das Bild

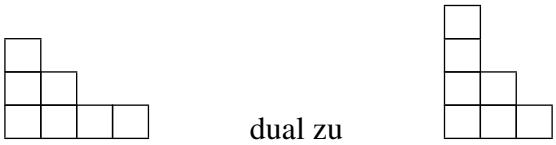


die Menge $\{(0,0),(0,1),(0,2),(1,0),(1,1),(2,0),(3,0)\}$ dar. In der Praxis denke ich bei Youngdiagrammen stets an Bilder dieser Art.

Ergänzung 1.3.4. Jedes Youngdiagramm T mit n Kästchen im Sinne von 1.3.3 liefert zwei Partitionen der Zahl n, die Partition durch die Zeilenlängen $z(T)$ und die Partition durch die Spaltenlängen $s(T)$. Bezeichnet $\mathcal{Y}_n$ die Menge aller Youngdiagramme mit n Kästchen und $\mathcal{P}_n$ die Menge aller Partitionen der Zahl n, so erhalten wir auf diese Weise zwei Bijektionen

$$\mathcal{P}_n \overset{z}{\xleftarrow{\sim}} \mathcal{Y}_n \overset{s}{\xrightarrow{\sim}} \mathcal{P}_n$$

die zusammen eine selbstinverse Bijektion $\mathcal{P}_n \xrightarrow{\sim} \mathcal{P}_n$ liefern. Diese Bijektion notieren wir $\lambda \mapsto \lambda'$ und nennen λ' die **duale Partition zu** λ. Zum Beispiel ist die duale Partition zu $3,2$ die Partition $2,2,1$ und die duale Partition zu $3,2,1,1$ ist $4,2,1$, im Bild also ist



Ergänzende Übung 1.3.5. Gegeben ein n-dimensionaler Vektorraum V bildet für jeden nilpotenten Endomorphismus $N \in \operatorname{End} V$ die Folge der Zahlen $\dim(\operatorname{im} N^r / \operatorname{im} N^{r+1})$ eine Partition von n, und die Fasern der so konstruierten Abbildung

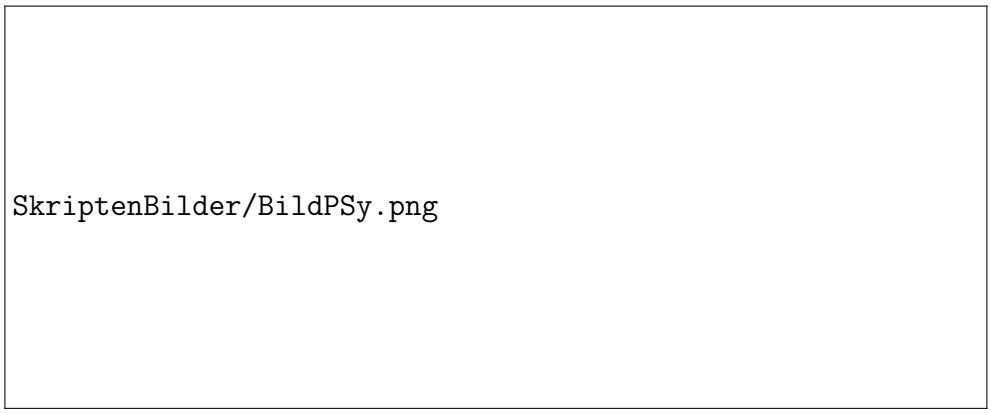
$$\{N \in \operatorname{End} V \mid N \text{ nilpotent}\} \to \mathcal{P}_n$$

sind genau die Bahnen der Operation von $\mathrm{GL}(V)$ durch Konjugation auf der Menge der nilpotenten Endomorphismen von V.

1.3.6. Unter einer **Partition einer Menge** X verstehen wir wie in II.8.1.15 ein System $\mathcal{U} \subset \mathcal{P}(X)$ von paarweise disjunkten nichtleeren Teilmengen, deren Vereinigung ganz X ist. Die Menge aller Partitionen einer gegebenen Menge X notieren wir $\mathcal{P}_X$. Hat X genau n Elemente, so erhalten wir, indem wir die Kardinalitäten der Teilmengen unseres Systems der Größe nach aufführen, eine offensichtliche Surjektion

$$\mathcal{P}_X \twoheadrightarrow \mathcal{P}_n$$

Eine Partition einer Menge mit dreizehn Elementen durch vier Teilmengen. Die im Sinne von 1.3.6 zugehörige Partition der Zahl 13 wäre 13=5+4+3+1.



Eine Permutation $\sigma \in \mathcal{S}_7$, unter der die Bilder der Zahlen $1, 2, 3, 4, 5, 6, 7$ der Reihe nach gerade $2, 5, 3, 4, 1, 7, 6$ sind. Die zugehörige Partition der Menge $\{1, 2, 3, 4, 5, 6, 7\}$ ist durch die gestrichelten Linien angedeutet und wäre in Formeln die Zerlegung $\{1, 2, 3, 4, 5, 6, 7\} = \{1, 2, 5\} \cup \{6, 7\} \cup \{3\} \cup \{4\}$. Die zugehörige Partition der Zahl 7 ist $7 = 3 + 2 + 1 + 1$.

1.3.7. Jede Permutation $\sigma \in \mathrm{Ens}^\times(X)$ einer Menge X liefert eine Partition von X, nämlich die Partition in die Bahnen der von σ erzeugten Untergruppe $\langle\sigma\rangle = \{\sigma^r \mid r \in \mathbb{Z}\}$. Im Fall $|X| = n < \infty$ erhalten wir durch Verknüpfung dieser Abbildung $\mathrm{Ens}^\times(X) \to \mathcal{P}_X$ mit der in 1.3.6 diskutierten Abbildung $\mathcal{P}_X \twoheadrightarrow \mathcal{P}_n$ die sogenannte **Zykellängenabbildung** $\mathrm{Ens}^\times(X) \to \mathcal{P}_n$. Im Fall $X = \{1, \ldots, n\}$ ist das eine Abbildung $\mathcal{S}_n \to \mathcal{P}_n$.

1.3.8. Ich erinnere an die Operation durch Konjugation einer Gruppe auf sich selber aus II.8.3.1 und an ihre Bahnen, die Konjugationsklassen.

Satz 1.3.9 (Konjugationsklassen in den symmetrischen Gruppen). *Ist X eine endliche Menge mit $|X| = n$ Elementen, so sind die Fasern der Zykellängenabbildung*

$$\mathrm{Ens}^\times(X) \to \mathcal{P}_n$$

genau die Konjugationsklassen in der Permutationsgruppe $\mathrm{Ens}^\times(X)$.

Ergänzung 1.3.10. Eine analoge Aussage gilt mit demselben Beweis auch für eine beliebige Menge X.

Beweis. Seien Permutationen $\sigma, \tau \in \mathrm{Ens}^\times(X)$ gegeben. Ist $X = X_1 \cup \ldots \cup X_r$ die Partition von X in die Bahnen von $\langle\sigma\rangle$, so ist

$$X = \tau(X_1) \cup \ldots \cup \tau(X_r)$$

die Partition in die Bahnen von $\langle\tau\sigma\tau^{-1}\rangle$, folglich ist die Zykellängenabbildung konstant auf Konjugationsklassen. Die Zykellängenabbildung ist auch offensichtlich surjektiv. Um schließlich zu zeigen, daß je zwei Permutationen mit denselben Zykellängen konjugiert sind, seien etwa $\sigma, \kappa \in \mathrm{Ens}^\times(X)$ unsere beiden Permutationen und

$$\begin{aligned} X &= X_1 \cup \ldots \cup X_r \\ X &= Y_1 \cup \ldots \cup Y_r \end{aligned}$$

die Zerlegungen in Bahnen unter $\langle\sigma\rangle$ und $\langle\kappa\rangle$ mit $|X_i| = |Y_i| = r_i$. Gegeben $z \in X_i$ und $u \in Y_i$ haben wir dann

$$\begin{aligned} X_i &= \{z, \sigma(z), \sigma^2(z), \ldots, \sigma^{r_i}(z) = z\} \\ Y_i &= \{u, \kappa(u), \kappa^2(u), \ldots, \kappa^{r_i}(u) = u\} \end{aligned}$$

Definieren wir also $\tau : X_i \xrightarrow{\sim} Y_i$ durch $\tau(\sigma^\nu(z)) = \kappa^\nu(u)$, so kommutiert das Diagramm

$$\begin{array}{ccc} X_i & \xrightarrow{\sigma} & X_i \\ {\scriptstyle\tau}\downarrow & & \downarrow{\scriptstyle\tau} \\ Y_i & \xrightarrow{\kappa} & Y_i \end{array}$$

Setzen wir dann alle diese $\tau : X_i \xrightarrow{\sim} Y_i$ zusammen zu $\tau : X \xrightarrow{\sim} X$, so gilt ebenso $\kappa\tau = \tau\sigma$ alias $\kappa = \tau\sigma\tau^{-1}$. □

Übung 1.3.11. Man zeige, daß die symmetrische Gruppe $\mathcal{S}_5$ genau sieben Konjugationsklassen besitzt.

Definition 1.3.12. Hat $\langle\sigma\rangle$ außer einer p-elementigen Bahn nur einelementige Bahnen, so nennt man σ einen **p-Zykel**. Die Zweizykel heißen auch **Transpositionen**.

Ergänzende Übung 1.3.13. Man zeige, daß das Signum eines p-Zykels stets $(-1)^{p+1}$ ist.

1.3.14. Eine Möglichkeit, Permutationen zu notieren, besteht darin, unter jedes Element sein Bild zu schreiben, also etwa

$$\tau = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 2 & 3 & 5 & 1 \end{bmatrix}$$

Eine andere Möglichkeit ist die Notation als Produkt paarweise disjunkter Zykel. Ein p-Zykel σ wird notiert in der Form $\sigma = (z, \sigma(z), \sigma^2(z), \ldots, \sigma^{p-1}(z))$ wobei $\sigma^p(z) = z$ zu verstehen ist. In Zykelschreibweise hätten wir für unsere Permutation τ von eben etwa

$$\tau = (1,6)(2,4,3)(5)$$

und das ist so zu verstehen, daß jedes Element auf das dahinterstehende abgebildet wird, außer wenn es direkt vor einer Klammer steht: Dann wird es auf das erste Element innerhalb seiner Klammer abgebildet. Oft werden Fixpunkte nicht mit notiert, so daß wir also auch schreiben könnten

$$\tau = (1,6)(2,4,3)$$

Das ist übrigends auch das Produkt der Transposition $\kappa = (1,6)$ mit den Dreizykel $\rho = (2,4,3)$ und wir haben $\tau = \kappa\rho = \rho\kappa$, was die Sinnhaftigkeit unserer Notation zeigt. Zwei Zykel heißen **disjunkt** genau dann, wenn jedes Element von einem der beiden festgehalten wird. Ganz allgemein kommutieren disjunkte Zykel, so gilt etwa $(1,6)(2,3,4) = (2,3,4)(1,6)$ in $\mathcal{S}_6$.

Übung 1.3.15. Man zeige unabhängig von unseren geometrischen Betrachtungen zur Ikosaedergruppe 1.2.5, daß es in der alternierenden Gruppe A_5 genau 5 Konjugationsklassen gibt, die die Kardinalitäten 20, 15, 12, 12 und 1 haben. Man folgere, daß die alternierende Gruppe A_5 einfach ist.

Zwei Permutationen $\sigma, \sigma' \in \mathcal{S}_5$, die dieselbe Partition $5 = 3 + 2$ liefern, und eine Permutation τ, die sie ineinander konjugiert.

1.4 p-Gruppen

Definition 1.4.1. Das **Zentrum** einer Gruppe G ist die Menge

$$Z(G) = \{x \in G \mid xg = gx \quad \forall g \in G\}$$

derjenigen Elemente, die mit allen anderen Gruppenelementen kommutieren.

1.4.2. Offensichtlich ist das Zentrum ein Normalteiler, was im Übrigen auch die alternative Beschreibung $Z(G) = \ker(\mathrm{int} : G \to \mathrm{Grp}^\times(G))$ in den Notationen aus II.8.3 als Kern eines Gruppenhomomorphismus sofort zeigt.

Ergänzende Übung 1.4.3. Man bestimme das Zentrum der Gruppe $\mathrm{GL}(n;k)$ für $n \in \mathbb{N}$ und k ein Körper. Man bestimme das Zentrum der Symmetriegruppe eines Quadrats.

Definition 1.4.4. Die Standgruppe von $g \in G$ unter der Operation von G auf sich selbst durch Konjugation heißt der **Zentralisator** $Z_G(g)$ von g, in Formeln

$$Z_G(g) = \{x \in G \mid xgx^{-1} = g\}$$

1.4.5. Ist G eine endliche Gruppe, $G = C_1 \sqcup \ldots \sqcup C_r$ ihre Zerlegung in Konjugationsklassen und $g_i \in C_i$ jeweils ein Element, so liefert die Bahnformel II.8.2.2 die sogenannte **Klassengleichung**

$$\begin{aligned} |G| &= |C_1| + \ldots + |C_r| \\ &= |G|/|Z_G(g_1)| + \ldots + |G|/|Z_G(g_r)| \end{aligned}$$

Die einelementigen Konjugationsklassen sind natürlich genau die Elemente des Zentrums.

Definition 1.4.6. Sei p eine Primzahl. Eine **p-Gruppe** ist eine endliche Gruppe, deren Ordnung eine Potenz von p ist. Wir lassen hier insbesondere auch die triviale Gruppe zu.

1.4.7. Gegeben eine Primzahl p hatten wir eine p-Gruppe definiert als eine endliche Gruppe, deren Ordnung eine p-Potenz ist. Die triviale Gruppe hat p^0 Elemente und ist damit eine p-Gruppe für jede Primzahl p.

Proposition 1.4.8. *Jede nichttriviale p-Gruppe hat nichttriviales Zentrum.*

Beweis. Zerlegen wir unsere Gruppe in Konjugationsklassen $G = C_1 \sqcup \ldots \sqcup C_r$, so sind alle $|C_i|$ nach der Bahnformel Teiler von $|G|$, also p-Potenzen. Die einelementigen Konjugationsklassen gehören aber genau zu den Elementen des Zentrums von G und wir folgern

$$|G| \equiv |Z(G)| \pmod{p}$$

Da nun das Zentrum stets mindestens ein Element hat, nämlich das neutrale Element, muss es im Fall einer nichttrivialen p-Gruppe sogar mindestens p Elemente haben. □

Korollar 1.4.9. *Ist die Ordnung einer Gruppe das Quadrat einer Primzahl, so ist die besagte Gruppe abelsch, in Formeln:*

$$|G| = p^2 \;\Rightarrow\; Z(G) = G$$

Beweis. Sei p die fragliche Primzahl. Nach der vorhergehenden Proposition 1.4.8 hat das Zentrum unserer Gruppe mindestens p Elemente. Gäbe es nun außerhalb des Zentrums noch ein Element unserer Gruppe, so müßte dieses Element zusammen mit dem Zentrum eine kommutative Untergruppe mit mehr als p Elementen erzeugen, und diese wäre wegen dem Satz von Lagrange II.7.1.5 notwendig bereits die ganze Gruppe. □

Satz 1.4.10 (Struktur von p-Gruppen). *Ist G eine p-Gruppe, so gibt es in G eine Kette $G = G_r \supset G_{r-1} \supset \ldots \supset G_0 = 1$ von Normalteilern von G mit $G_i/G_{i-1} \cong \mathbb{Z}/p\mathbb{Z}$ für alle i.*

Beweis. Wir führen den Beweis durch Induktion über die Gruppenordnung. Ist G nicht trivial, in Formeln $G \neq 1$, so hat G nach 1.4.8 ein nichttrivales Zentrum $Z(G) \neq 1$. Indem wir von irgendeinem nichttrivialen Element des Zentrums eine geeignete Potenz nehmen, finden wir im Zentrum sogar ein Element x der Ordnung p. Die von x erzeugte Untergruppe $G_1 = \langle x \rangle$ ist also isomorph zu $\mathbb{Z}/p\mathbb{Z}$, und da x im Zentrum liegt, ist G_1 ein Normalteiler in G. Nach Induktion finden wir nun im Quotienten $\overline{G} = G/G_1$ eine Kette $\overline{G} = \overline{G}_l \supset \ldots \supset \overline{G}_1 \supset \overline{G}_0 = 1$ wie gewünscht. Dann nehmen wir $G_i = \mathrm{can}^{-1}(\overline{G}_{i-1})$ für $\mathrm{can} : G \twoheadrightarrow \overline{G}$ die Projektion. Wegen II.7.2.3 erhalten wir so eine Kette von Normalteilern von G. Wegen II.7.1.6 haben wir $|G_i| = p|\overline{G}_{i-1}| = p^i$. Damit hat G_i/G_{i-1} genau p Elemente und ist folglich zyklisch. □

Definition 1.4.11. Eine Gruppe G heißt **auflösbar** (engl. **solvable**, franz. **soluble**) genau dann, wenn es eine Folge von Untergruppen $G = G_r \supset G_{r-1} \supset G_{r-2} \supset \ldots \supset G_0 = 1$ gibt mit G_{i-1} normal in G_i und G_i/G_{i-1} abelsch für $1 \leq i \leq r$.

1.4.12. Die Terminologie "auflösbar" kommt von der Beziehung dieses Begriffs zum Auflösen von Gleichungen her und wird erst im Licht von Satz 4.7.19 verständlich. Satz 1.4.10 zeigt, daß jede p-Gruppe auflösbar ist, und Bemerkung 1.6.3 zeigt, daß die symmetrische Gruppe $\mathcal{S}_4$ auflösbar ist.

Ergänzung 1.4.13. Stärker heißt eine Gruppe G **überauflösbar** genau dann, wenn es eine Folge $G = G_r \supset G_{r-1} \supset G_{r-2} \supset \ldots \supset G_0 = 1$ von Normalteilern von G gibt mit G_i/G_{i-1} zyklisch für $1 \leq i \leq r$. Wir haben oben demnach sogar gezeigt, daß jede endliche p-Gruppe überauflösbar ist.

Übung 1.4.14. Jede Untergruppe einer auflösbaren Gruppe ist auflösbar. Gegeben $G \supset N$ eine Gruppe mit Normalteiler ist die ganze Gruppe G auflösbar genau dann, wenn N und G/N auflösbar sind.

1.5 Die Sätze von Sylow

Definition 1.5.1. Sei G eine endliche Gruppe und p eine Primzahl. Eine Untergruppe $P \subset G$ heißt eine **p-Sylowuntergruppe** oder kurz **p-Sylow** von G genau dann, wenn ihre Kardinalität $|P|$ die höchste p-Potenz ist, die die Gruppenordnung $|G|$ teilt.

Beispiel 1.5.2. Eine 2-Sylow in der Gruppe der 24 Drehsymmetrien eines Würfels ist per definitionem eine Untergruppe mit 8 Elementen. Zum Beispiel wäre jede Untergruppe, die die Achse durch die Mittelpunkte zweier gegenüberliegender Flächen stabilisiert, eine solche 2-Sylow. Die einzige 5-Sylow in derselben Gruppe wäre in unserer Terminologie die einelementige Untergruppe. Viele Autoren verstehen aber auch abweichend unter Sylowuntergruppen nur diejenigen Untergruppen, die wir in unserer Terminologie als "nichttriviale Sylowuntergruppen" ansprechen würden.

Satz 1.5.3 (Sätze von Sylow). *Sei G eine endliche Gruppe, p eine Primzahl und p^r die größte p-Potenz, die die Gruppenordnung $|G|$ teilt. So gilt:*

1. *Die Gruppe G besitzt Untergruppen der Ordnung p^r alias p-Sylows.*
2. *Je zwei p-Sylows von G sind zueinander konjugiert.*
3. *Jede Untergruppe von G, deren Ordnung eine p-Potenz ist, liegt in einer p-Sylow von G.*
4. *Die Zahl der p-Sylows von G ist ein Teiler von $|G|/p^r$ und kongruent zu 1 modulo p.*

1.5.4. Ist G eine endliche abelsche Gruppe, so gibt es insbesondere genau eine p-Sylow für alle p. Wir kennen diese Untergruppe schon aus Proposition II.7.3.23, es ist genau unsere Untergruppe $G(p)$ aller Elemente von G, deren Ordnung eine p-Potenz ist.

1.5.5. Im Fall der Gruppe der 24 Drehsymmetrien eines Würfels liefern die drei Paare gegenüberliegender Flächen drei paarweise verschiedene 2-Sylows, bestehend aus allen Drehsymmetrien, die das jeweilige Paar in sich überführen. Das müssen dann auch bereits alle 2-Sylows alias alle 8-elementigen Untergruppen dieser Gruppe sein, wie man unschwer aus Teil 2 oder auch aus Teil 4 des vorhergehenden Satzes folgern kann.

Beweis. 1. Wir argumentieren durch Induktion über $|G|$. Ohne Beschränkung der Allgemeinheit dürfen wir annehmen, daß p die Ordnung unserer Gruppe teilt. Besitzt G eine echte Untergruppe $H \subsetneq G$ mit $p \nmid |G/H|$, so folgt die Aussage aus der Induktionsannahme. Teilt sonst p den Index $|G/H|$ jeder echten Untergruppe H von G, so ist die Kardinalität jeder Konjugationsklasse mit mehr als einem Element teilbar durch p. Aus der Klassengleichung 1.4.5 folgt damit $|G| \equiv |Z(G)| \pmod p$ und p teilt die Ordnung des Zentrums $Z(G)$. Dann gibt es nach II.7.3.24 in $Z(G)$ ein Element g der Ordnung p. Nach der Induktionsannahme finden wir nun eine p-Sylow von $G/\langle g\rangle$, und deren Urbild in G ist notwendig eine p-Sylow von G.

2–4. Bezeichne $\mathcal{S}$ die Menge aller p-Sylows von G. Sicher operiert G auf $\mathcal{S}$ vermittels Konjugation. Wir vereinbaren zur Notation im weiteren Verlauf des Beweises die folgenden Konventionen: Bezeichnen wir eine Sylow durch einen kleinen Buchstaben, so fassen wir sie primär als ein Element $x \in \mathcal{S}$ auf und schreiben die mit $g \in G$ konjugierte Sylow gx. Bezeichnen wir eine Sylow jedoch durch einen großen Buchstaben, so fassen wir sie primär als eine Teilmenge $P \subset G$ auf und schreiben die mit $g \in G$ konjugierte Sylow gPg^{-1}. Sei nun eine Sylow $P = x$ gegeben. Für ihre Isotropiegruppe G_x gilt $G_x \supset P$, also ist nach der Bahnformel II.8.2.2 die Kardinalität $|Gx|$ der Bahn $Gx \subset \mathcal{S}$ von x teilerfremd zu p. Sei nun weiter $H \subset G$ eine Untergruppe von p-Potenzordnung. Sicher zerfällt Gx in Bahnen unter H, und die Ordnung jeder solchen Bahn muß eine p-Potenz sein. Folglich gibt es in Gx einen Fixpunkt y von H. Dies $y = gx$ ist nun aber in der Großbuchstabennotation gerade die zu P konjugierte Sylowuntergruppe $Q = gPg^{-1}$, und die Fixpunkteigenschaft besagt $hQh^{-1} = Q \quad \forall h \in H$. Mithin ist $HQ = QH$ eine Untergruppe von G. Ihre Ordnung ist $|QH| = |QH/H| \cdot |H|$ und QH/H ist unter Q eine einzige Bahn und damit ist $|QH/H|$ eine p-Potenz. Da aber auch $|H|$ eine p-Potenz ist, muß QH eine p-Gruppe sein. Es folgt $QH = Q$, also $Q \supset H$ und 2 und 3 sind bewiesen. Unser Argument zeigt aber insbesondere auch, daß es nur eine einpunktige Bahn unserer Sylow P auf der Menge aller p-Sylows $\mathcal{S}$ gibt, nämlich die Bahn von P selber. Alle anderen P-Bahnen in $\mathcal{S}$ haben als Kardinalität eine echte p-Potenz, und das zeigt $|\mathcal{S}| \equiv 1 \pmod p$. Die Isotropiegruppe G_x von $P \in \mathcal{S}$ umfaßt schließlich unsere Sylow P, und da je zwei p-Sylows konjugiert sind alias ganz $\mathcal{S}$ ein homogener G-Raum ist, folgt auch, daß $|\mathcal{S}| = |G/G_x|$ ein Teiler ist von $|G/P|$. □

Korollar 1.5.6 (Satz von Cauchy). *Jeder Primfaktor der Ordung einer endlichen Gruppe tritt auch als Ordnung eines Elements besagter Gruppe auf.*

1.5.7. Man beachte, daß wir diese Aussage für abelsche Gruppen bereits in II.7.3.24 bewiesen hatten, und daß wir sie in diesem Fall ihrerseits beim Beweis der Sylowsätze verwendet haben.

Beweis. Sei p unser Primfaktor. Man findet zunächst nach 1.5.3 in unserer Gruppe eine p-Sylow und dann darin das leicht das gesuchte Element der Ordnung p als geeignete Potenz eines beliebigen vom neutralen Element verschiedenen Elements. □

Proposition 1.5.8. *Jede Gruppe mit genau sechs Elementen ist entweder zyklisch oder isomorph zur symmetrischen Gruppe $\mathcal{S}_3$.*

Beweis. Sei G unsere Gruppe der Ordnung $|G| = 6$. Wir finden nach dem Satz von Cauchy 1.5.6 Elemente $a, b \in G$ der Ordnungen 2 und 3. Nach Übung II.2.2.5 zum Satz von Lagrange gilt $\langle a\rangle \cap \langle b\rangle = 1$, also definiert die Multiplikation eine Bijektion

$$\langle a\rangle \times \langle b\rangle \xrightarrow{\sim} G$$

Sicher kann unter diesen Umständen ba weder eine Potenz von a noch eine Potenz von b sein. Gilt $ba = ab$, so ist unsere Gruppe kommutativ und folglich isomorph zu $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$. Gilt $ba = ab^2$, so legt diese Gleichung schon die ganze Gruppenstruktur fest und wir haben die $\mathcal{S}_3$ vor uns. □

Korollar 1.5.9. *Jede Gruppe der Ordnung 15 ist zyklisch.*

Beweis. Die Zahl der 3-Sylows teilt 5 und ist kongruent zu 1 modulo 3. Es gibt also genau eine 3-Sylow und damit genau zwei Elemente der Ordnung 3. Ähnlich gibt es genau eine 5-Sylow und damit genau 4 Elemente der Ordnung 5. Zusammen mit dem neutralen Element sind das nur 7 Elemente. Die übrigen 8 Elemente haben notwendig die Ordnung 15. □

Ergänzende Übung 1.5.10. Sind $p > q$ Primzahlen und ist q kein Teiler von $p-1$, so ist jede Gruppe der Ordnung pq zyklisch. Hinweis: 1.5.9.

Ergänzung 1.5.11 (**Gruppen mit höchstens 15 Elementen**). Mit den folgenden Übungen können Sie die Klassifikation der Gruppen mit höchstens 15 Elementen zu Ende bringen. Gruppen mit $2, 3, 5, 7, 11$ oder 13 Elementen sind ja zyklisch nach II.7.3.5. Gruppen mit 4 oder 9 Elementen sind abelsch nach 1.4.9 und werden damit durch II.7.4.3 klassifiziert. Gruppen mit 6 Elementen hatten wir in 1.5.8 diskutiert. Für Gruppen mit 10 oder 14 Elementen funktioniert dieselbe Argumentation, wie Sie als Übung 1.5.12 ausarbeiten dürfen. Gruppen mit 8 Elementen klassifizieren wir in 1.5.15, Gruppen mit 12 Elementen klassifizieren Sie in 1.5.14, und jede Gruppe mit 15 Elementen ist zyklisch nach 1.5.9. Bei Gruppen mit 16 Elementen fängt es aber an, unübersichtlich zu werden, es gibt von ihnen bereits 14 Isomorphieklassen.

Ergänzende Übung 1.5.12. Für jede Primzahl p gibt es bis auf Isomorphismus genau zwei Gruppen der Ordnung $2p$, eine zyklische Gruppe und eine Diedergruppe. Hinweis: Man erinnere die Argumentation im Fall $p = 3$ und interessiere sich für die Anzahl der 2-Sylows.

Ergänzende Übung 1.5.13 (**Funktorialität semidirekter Produkte**). Seien A, M, B, N Gruppen und $\kappa : A \to \mathrm{Grp}^\times M$ sowie $\tau : B \to \mathrm{Grp}^\times N$ Gruppenhomomorphismen. Seien weiter $\psi : A \to B$ und $\varphi : M \to N$ Gruppenhomomorphismen mit ${}^{\psi(a)}\varphi(m) = \varphi({}^a m)$ für alle $a \in A$ und alle $m \in M$ alias $\tau(\psi(a)) \circ \varphi = \varphi \circ \kappa(a)$ für alle $a \in A$. So ist $\varphi \times \psi$ ein Homomorphismus der semidirekten Produkte

$$(\varphi \times \psi) : M \rtimes A \to N \rtimes B$$

Speziell haben wir$N \rtimes_\tau B \cong N \rtimes_\kappa B$ im Fall $\kappa = (\mathrm{int}\,\varphi) \circ \tau$ für einen Automorphismus $\varphi \in \mathrm{Grp}^\times N$ der Gruppe N.

Ergänzende Übung 1.5.14 (**Gruppen mit 12 Elementen**). In dieser Übung sollen Sie zeigen, daß es bis auf Isomorphismus genau 5 Gruppen der Ordnung 12 gibt: Die beiden abelschen Gruppen $(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/3\mathbb{Z}$ und $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, die Diedergruppe D_6, die alternierende Gruppe A_4 und ein semidirektes Produkt $\mathbb{Z}/4\mathbb{Z} \ltimes \mathbb{Z}/3\mathbb{Z}$, für das mir keine konkrete Interpretation eingefallen ist. Ich rate, der Reihe nach folgendes zu zeigen:

1. In einer Gruppe mit 12 Elementen gibt es entweder nur eine 2-Sylow oder nur eine 3-Sylow. Hinweis: Mehr Platz ist nicht vorhanden.

2. Schreiben wir im folgenden $\rtimes$ nur für semidirekte Produkte, die nicht gewöhnliche Produkte sind, so gehört jede Gruppe mit 12 Elementen zu einer der sechs Typen

$$\begin{array}{lll} (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/3\mathbb{Z} & (\mathbb{Z}/2\mathbb{Z})^2 \ltimes \mathbb{Z}/3\mathbb{Z} & (\mathbb{Z}/2\mathbb{Z})^2 \rtimes \mathbb{Z}/3\mathbb{Z} \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \mathbb{Z}/4\mathbb{Z} \ltimes \mathbb{Z}/3\mathbb{Z} & \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z} \end{array}$$

3. Vom letzten dieser Typen existiert keine Gruppe, von jedem anderen Typ existiert bis auf Isomorphismus genau eine, und diese fünf Gruppen sind paarweise nicht isomorph. Hinweis: Man beachte 1.5.13 und beachte auch, daß für den Fall, in dem es von beiden Typen von Sylow nur eine gibt, die Gruppe kommutativ sein muß: Sind H, K die beiden Sylows, so gilt dann ja $hkh^{-1}k^{-1} \in H \cap K$ für alle $h \in H, k \in K$.

Ergänzung 1.5.15 (**Gruppen mit 8 Elementen**). Es gibt 5 Isomorphieklassen von Gruppen der Ordnung acht, nämlich die drei abelschen Gruppen $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ und $(\mathbb{Z}/2\mathbb{Z})^3$, die Diedergruppe der Ordnung acht sowie die **Quaternionengruppe** der acht Quaternionen $\{\pm 1, \pm \mathrm{i}, \pm \mathrm{j}, \pm \mathrm{k}\}$ nach II.2.9.4. Um das einzusehen, kann man argumentieren wie folgt: Jede nichtabelsche Gruppe der Ordnung acht besitzt nach II.1.4.34 Elemente der Ordnung vier, also nach II.7.2.4 einen zyklischen Normalteiler der Ordnung vier. Gibt es eine Involution außerhalb dieses Normalteilers, so sehen wir schnell, daß unsere Gruppe ein semidirektes Produkt

$(\mathbb{Z}/4\mathbb{Z}) \rtimes (\mathbb{Z}/2\mathbb{Z})$ sein muß für die einzige nichttriviale Operation, so daß wir eine Diedergruppe vor uns haben. Sonst haben alle Elemente außerhalb unseres Normalteilers die Ordnung vier und in unserer Gruppe bleibt nur noch Platz für ein einziges Element der Ordnung zwei. Unsere Gruppe ist also die Vereinigung von drei zyklischen Gruppen der Ordnung vier, und der Schnitt dieser Gruppen ist auch der Schnitt von je zweien unter ihnen und ist zyklisch von der Ordnung zwei und zentral. Bezeichne 1 das neutrale Element und -1 das andere Element dieses Schnitts. Wählen wir i und j Erzeuger von zwei verschiedenen zyklischen Untergruppen der Ordnung vier, so müssen $\mathrm{i}\,\mathrm{j}$ und auch $\mathrm{k} := (-1)\,\mathrm{i}\,\mathrm{j}$ die dritte zyklische Untergruppe der Ordnung vier erzeugen, denn diese Elemente sind weder eine Potenz von i noch eine Potenz von j. Von hier aus ist leicht zu sehen, daß wir gerade die Quaternionengruppe vor uns haben.

Ergänzende Übung 1.5.16. Teilt eine Primzahlpotenz die Ordnung einer Gruppe, so gibt es eine Untergruppe mit besagter Primzahlpotenz als Ordnung. In der symmetrischen Gruppe $\mathcal{S}_5$ gibt es keine Untergruppe mit 15 Elementen.

Ergänzung 1.5.17. Jede Gruppe der Ordnung 18 ist auflösbar. In der Tat gibt es nur eine 3-Sylow, die ist notwendig normal, und wir sind fertig.

Ergänzende Übung 1.5.18. Man zeige, daß die 2-Sylow in der symmetrischen Gruppe $\mathcal{S}_4$ der Drehsymmetrien eines Würfels isomorph ist zur Diedergruppe der Ordnung 8.

Ergänzende Übung 1.5.19. Gegeben in einer endlichen Gruppe G zwei Sylow-Untergruppen P, Q gilt stets $\{p \in P \mid pQp^{-1} = Q\} = P \cap Q$. Hinweis: Die Lösung ist im Beweis der Sylowsätze versteckt.

1.6 Alternierende Gruppen*

1.6.1. Die Abbildung sgn, die jeder Permutation $\tau \in \mathcal{S}_r$ ihr Signum zuordnet, ist ein Gruppenhomomorphismus $\mathrm{sgn} : \mathcal{S}_r \to \{1, -1\}$. Der Kern dieses Gruppenhomomorphismus, d.h. die Gruppe aller geraden Permutationen von r Objekten, heißt die r-te **alternierende Gruppe** und wird notiert als

$$A_r = \ker(\mathrm{sgn} : \mathcal{S}_r \to \{1, -1\})$$

Satz 1.6.2. *Die alternierenden Gruppen A_r sind einfach für $r \geq 5$.*

1.6.3. In der alternierenden Gruppe A_4 bilden die drei Doppeltranspositionen zusammen mit dem neutralen Element einen Normalteiler, der isomorph ist zur Klein'schen Vierergruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Insbesondere ist A_4 nicht einfach. Die Gruppen A_1 und A_2 sind trivial, $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ ist jedoch auch noch einfach. Daß A_5 einfach ist, kann man wie beim Beweis der Einfachkeit der Ikosaedergruppe unmittelbar einsehen, indem man die Kardinalitäten der Konjugationsklassen

berechnet. Dem Beweis des Satzes im allgemeinen schicken wir zwei Lemmata voraus.

1.6.4. Hat das Erzeugnis $\langle\sigma\rangle$ einer Permutation σ genau zwei zweielementige und sonst nur einelementige Bahnen, so heißt σ eine **Doppeltransposition**. Hat $\langle\sigma\rangle$ genau zwei dreielementige und sonst nur einelementige Bahnen, so nennen wir σ einen **Doppeldreizykel**.

Lemma 1.6.5. *Die symmetrischen Gruppen $\mathcal{S}_r$ werden von den Transpositionen erzeugt, die alternierenden Gruppen A_r von den Dreizykeln.*

Beweis. Die erste Aussage war Übung II.2.10.8. Die Zweite folgt daraus, daß man jede Doppeltransposition als Produkt von zwei Dreizykeln schreiben kann, $(ab)(cd) = (abc)(bcd)$, und daß das Produkt von zwei nicht kommutierenden Transpositionen ein Dreizykel ist, $(ab)(ac) = (acb)$. Jedes Produkt einer geraden Zahl von Transpositionen läßt sich demnach auch als ein Produkt von Dreizykeln darstellen. □

Lemma 1.6.6. *Für $r \geq 5$ wird die alternierende Gruppe A_r nicht nur erzeugt von den Dreizykeln, sondern auch von den Doppeltranspositionen. Des weiteren sind für $r \geq 5$ je zwei Doppeltranspositionen und je zwei Dreizykel auch schon in A_r konjugiert.*

Beweis. Jeder Dreizykel kann als Verknüpfung von zwei Transpositionen seiner drei Elemente dargestellt werden. Haben wir noch zwei weitere Elemente zur Verfügung, so können wir diese beiden Transpositionen durch das Verknüpfen mit der Vertauschung dieser beiden Elemente zu Doppeltranspositionen machen. Das zeigt die erste Aussage. Zwei Doppeltranspositionen $(ab)(cd)$ und $(a'b')(c'd')$ sind konjugiert unter jeder Permutation τ mit $a \mapsto a', \ldots, d \mapsto d'$ und auch unter $\tau \circ (ab)$. Entweder τ oder $\tau \circ (ab)$ ist aber stets gerade. Zwei Dreizykel (abc) und $(a'b'c')$ sind konjugiert unter jeder Permutation τ mit $a \mapsto a', \ldots, c \mapsto c'$ und insbesondere auch unter $\tau \circ (de)$ für (de) disjunkt von (abc). Entweder τ oder $\tau \circ (de)$ ist aber stets gerade. Das zeigt die zweite Aussage. □

Beweis von 1.6.2. Sei ab jetzt r beliebig und $N \subset A_r$ ein nichttrivialer Normalteiler. Nach dem vorhergehenden Lemma 1.6.6 reicht es zu zeigen, daß es in N entweder eine Doppeltransposition oder einen Dreizykel gibt. Dazu zeigen wir, wie man zu jedem nichttrivialen Element $g \in N$, das weder eine Doppeltransposition noch ein Dreizykel ist, ein anderes nichttriviales Element $\tilde{g} \in N$ mit noch mehr Fixpunkten konstruieren kann. Indem wir zu Potenzen von g übergehen, können wir g von Primzahlordnung annehmen.

Ist $\operatorname{ord} g \geq 5$, so wählen wir einen Zykel von g und betrachten einen Dreizykel h, der von einem festen Ausgangspunkt auf dem Zykel von g zwei Schritte

Die durchgezogenen Pfeile stellen eine Permutation g der Ordnung ≥ 5 auf der Menge der fetten Punkte dar, die gestrichelten Pfeile den im Beweis beschriebenen Dreizykel h, der umrandete Punkt unseren “Ausgangspunkt”.

mitläuft um dann wieder zum Ausgangspunkt zurückzukehren. Dann ist unser Ausgangspunkt ein Fixpunkt von $\tilde{g} = h^{-1}g^{-1}hg$ und wir haben ein nichttriviales $\tilde{g} \in N$ gefunden, das mehr Fixpunkte hat als g.

Ist $\operatorname{ord} g = 3$ und ist g kein Dreizykel, so muß g ein Produkt sein von mindestens zwei disjunkten Dreizykeln. Dann stimmen die Konjugationsklassen von g in A_r und in $\mathcal{S}_r$ überein, da es nämlich eine ungerade Permutation gibt, die mit g kommutiert, zum Beispiel eine geeignete "Dreifachtransposition zwischen zwei Dreizykeln von g". Es ist nun ein Leichtes, in $\mathcal{S}_6$ zwei Doppeldreizykel zu finden derart, daß ihr Produkt nicht trivial ist und dennoch einen Fixpunkt hat. Wenn wir also einen Doppeldreizykel von g auf der zugehörigen 6-elementigen Menge konjugieren zu einem geeigneten anderen Doppeldreizykel, so erhalten wir ein $h \in N$ derart, daß hg nicht trivial ist und mehr Fixpunkte hat als g.

Ist schließlich $\operatorname{ord} g = 2$ und g keine Doppeltransposition, so muß g ein Produkt sein von mindestens zwei disjunkten Doppeltranspositionen. Wieder stimmen dann die Konjugationsklassen von g in A_r und in $\mathcal{S}_r$ überein, da es eine ungerade Permutation gibt, die mit g kommutiert, zum Beispiel eine "Transposition aus einer Doppeltransposition von g". Wir finden also $h \in N$ derart, daß h auf einer vierelementigen Teilmenge eine andere Doppeltransposition ist als g und außerhalb dieser vierelementigen Teilmenge mit g übereinstimmt. Dann ist hg die dritte Doppeltransposition auf unserer vierelementigen Teilmenge und die Identität außerhalb, ist also einerseits nicht trivial und hat andererseits mehr Fixpunkte als g. □

Ergänzende Übung 1.6.7. Man zeige für $r \geq 5$, daß A_r der einzige nichttriviale echte Normalteiler von $\mathcal{S}_r$ ist. Man bestimme alle Kompositionsreihen aller symmetrischen Gruppen.

1.6.8. Nach der vorhergehenden Übung ist für $r \geq 5$ jeder Gruppenhomomorphismus von der symmetrischen Gruppe $\mathcal{S}_r$ in eine weitere Gruppe entweder injektiv oder konstant oder hat denselben Kern wie das Signum. Salopp gesprochen "kann es also keine feinere Invariante als das Signum geben".

Ergänzende Übung 1.6.9. In dieser Übung sollen Sie zeigen, daß die Gruppe $\mathrm{SL}(2;\mathbb{F}_5)$ genau fünf 2-Sylows besitzt und daß die Operation dieser Gruppe auf der Menge ihrer 2-Sylows einen Isomorphismus

$$\mathrm{SL}(2;\mathbb{F}_5)/\{\pm \mathrm{id}\} \xrightarrow{\sim} A_5$$

mit der sogenannten "alternierenden Gruppe" aller geraden Permutationen einer fünfelementigen Menge induziert. Den Quotienten auf der linken Seite notiert man auch $\mathrm{PSL}(2;\mathbb{F}_5)$, er liegt als Untergruppe vom Index 2 in der Gruppe $\mathrm{PGL}(2;\mathbb{F}_5)$ aller von invertierbaren Matrizen induzierten Automorphismen der projektiven Gerade alias dem Quotienten von $\mathrm{GL}(2;\mathbb{F}_5)$ nach der Gruppe der vier darin enthaltenen Diagonalmatrizen. Ich rate, der Reihe nach folgendes zu zeigen:

Die durchgezogenen Pfeile stellen einen Doppeldreizykel g auf der Menge der fetten Punkte dar, die gestrichelten Pfeile den im Beweis beschriebenen dazu konjugierten Doppeldreizykel h, der umrandete Punkt einen Fixpunkt von hg.

1. Jedes Element der Ordnung 4 in $\mathrm{SL}(2;\mathbb{F}_5)$ ist diagonalisierbar und der Normalisator seines Erzeugnisses ist eine 2-Sylow. Jede 2-Sylow enthält 6 Elemente der Ordnung 4.

2. Es gibt in $\mathrm{SL}(2;\mathbb{F}_5)$ genau dreißig Elemente der Ordnung 4 und fünf 2-Sylows, und der Schnitt von je zwei verschiedenen 2-Sylows besteht nur aus $\pm\mathrm{id}$.

3. Jede 2-Sylow von $\mathrm{PSL}(2;\mathbb{F}_5)$ ist eine Klein'sche Vierergruppe und operiert nach 1.5.19 frei auf der Menge der vier anderen 2-Sylows. Vom Bild unseres Homomorphismus $\mathrm{PSL}(2;\mathbb{F}_5) \to \mathcal{S}_5$ wissen wir damit, daß es alle Doppeltranspositionen enthält und aus höchstens 60 Elementen besteht. Nach 1.6.6 muß dieses Bild folglich die A_5 sein.

2 Mehr zu Ringen

2.1 Restklassenringe und Teilringe

2.1.1. Wir erinnern die grundlegenden Definitionen aus II.2.4. Die Stärke der Ringtheorie liegt unter anderem darin begründet, daß es sehr viele Vefahren gibt, die zu einem gegebenen Ring einen weiteren Ring konstruieren, und daß man auf diese neuen Ringe dann wieder alle bereits bekannten Sätze anwenden kann. Einige Beispiele dafür haben wir bereits in II.2.4.4 gesehen, weitere Beispiele sind das Bilden von Polynomringen II.2.5.2, II.2.5.32 und Potenzreihenringen II.2.5.33. Wir besprechen im folgenden noch eine weitere wichtige Konstruktion, das Bilden von Restklassenringen.

Definition 2.1.2. Sei R ein Ring. Ein **Ideal** von R ist eine Teilmenge $I \subset R$ mit der Eigenschaft, daß I eine Untergruppe ist von $(R,+)$ und daß zusätzlich gilt $RI \subset I$ und $IR \subset I$.

Beispiele 2.1.3. Ein Ideal von $\mathbb{Z}$ ist dasselbe wie eine Untergruppe von $\mathbb{Z}$, die Ideale von $\mathbb{Z}$ sind also nach II.2.2.16 genau die Teilmengen der Gestalt $\mathbb{Z}m$ für $m \in \mathbb{N}$. Für ein beliebiges Element a in einem kommutativen Ring R ist die Menge Ra aller Vielfachen von a ein Ideal. Der ganze Ring R und $\{0\}$ sind stets Ideale.

2.1.4. Ist $\varphi : R \to S$ ein Ringhomomorphismus, so ist $\ker \varphi$ ein Ideal von R. Allgemeiner ist das Urbild von einem Ideal unter einem Ringhomomorphismus stets wieder ein Ideal, und desgleichen das Bild eines Ideals unter einem *surjektiven* Ringhomomorphismus.

2.1.5. Ganz allgemein ist ein Schnitt von Idealen eines Rings R stets wieder ein Ideal. Gegeben eine Teilmenge $T \subset R$ bezeichen wir mit $\langle T\rangle_R \subset R$ das kleinste Ideal von R, das T umfaßt, und nennen es das **von** T **erzeugte Ideal**. Meist schreiben wir kürzer $\langle T\rangle$ in der Hoffnung, daß der Leser aus dem Kontext erschließen kann, daß damit nicht die von T erzeugte Untergruppe sondern eben das von T erzeugte Ideal gemeint ist. Wir können $\langle T\rangle$ entweder beschreiben als den Schnitt aller Ideale, die T umfassen, oder als die Menge aller endlichen Ausdrücke

$$\langle T\rangle = \{a_1t_1b_1 + \ldots a_nt_nb_n \mid n \geq 0,\ a_i, b_i \in R,\ t_i \in T\}$$

Hierbei ist der leere Ausdruck mit $n = 0$ wie üblich als die Null von R zu verstehen. Ist $T = \{t_1, \ldots, t_r\}$ eine endliche Menge, so schreiben wir auch $\langle T\rangle = \langle t_1, \ldots, t_r\rangle$. Insbesondere gilt für einen kommutativen Ring R zum Beispiel $\langle a\rangle = Ra$ für alle $a \in R$. Wollen wir betonen, daß das Symbol zwischen den Spitzklammern für eine Menge von Erzeugern und nicht für einen einzigen Erzeuger steht, so schreiben wir $\langle T\rangle = \langle\!| T\rangle$. Ideale, die von einem einzigen Element erzeugt

werden können, heißen **Hauptideale**. Insbesondere ist nach II.2.2.16 jedes Ideal in $\mathbb{Z}$ ein Hauptideal.

2.1.6. Gegeben ein Kring R und Elemente $a, b \in R$ ist a ein Teiler von b genau dann, wenn gilt $\langle a\rangle \ni b$ oder gleichbedeutend $\langle a\rangle \supset \langle b\rangle$. Gegeben ein Kring R und ein Element $u \in R$ ist u eine Einheit genau dann, wenn gilt $\langle u\rangle = R$. Gegeben ein kommutativer Integritätsbereich folgt aus $\langle a\rangle = \langle b\rangle$, daß es eine Einheit u gibt mit $au = b$.

Proposition 2.1.7 (Restklassenringe und universelle Eigenschaft). *Sei R ein Ring und $I \subset R$ ein Ideal.*

1. *Es gibt genau eine Verknüpfung "Multiplikation" auf der Restklassengruppe R/I derart, daß die kanonische Abbildung*

$$\mathrm{can} = \mathrm{can}_{\mathrm{q}} : R \twoheadrightarrow R/I$$

   mit den Multiplikationen verträglich ist, d.h. $\mathrm{can}(a \cdot b) = (\mathrm{can}\, a) \cdot (\mathrm{can}\, b)$.

2. *Mit dieser Multiplikation wird R/I ein Ring.*

3. *Jeder Ringhomomorphismus $\varphi : R \to R'$ mit $\varphi(I) = \{0\}$ faktorisiert eindeutig über R/I, es gibt also in Formeln für solch ein φ genau einen Ringhomomorphismus $\tilde{\varphi} : R/I \to R'$ mit $\varphi = \tilde{\varphi} \circ \mathrm{can}$.*

2.1.8. Die Nebenklasse $a + I = \mathrm{can}(a)$ von a bezeichnet man auch oft mit $\mathrm{can}(a) = \bar{a}$. Den Spezialfall der Restklassenringe $\mathbb{Z}/m\mathbb{Z}$ kennen wir bereits aus II.2.4.7.

Beweis. Auf der Potenzmenge von R betrachten wir die Verknüpfung

$$(A, B) \mapsto A \odot B := AB + I = \{ab + t \mid a \in A, b \in B, t \in I\}$$

Wenn I ein Ideal ist, so gilt $(a + I) \odot (b + I) = ab + I$. Folglich induziert unsere Verknüpfung auf $\mathcal{P}(R)$ eine Verknüpfung auf R/I, und das ist die gesuchte Multiplikation auf R/I. Es ist leicht zu sehen, daß diese Multiplikation R/I zu einem Ring macht. Für die dritte Aussage muß nur gezeigt werden, daß das aus der Gruppentheorie bereits bekannte $\tilde{\varphi}$ mit den Multiplikationen verträglich ist und die Eins auf die Eins wirft. Das bleibe dem Leser überlassen. □

Übung 2.1.9. Gegeben ein Körper k und ein Polynom $P \in k[X]$ vom Grad $\mathrm{grad}\, P = d \geq 1$ bilden die Nebenklassen der Monome $1, X, X^2, \ldots, X^{d-1}$ eine k-Basis des Restklassenrings $k[X]/\langle P\rangle$.

Definition 2.1.10. Eine Teilmenge eines Rings heißt ein **Teilring** genau dann, wenn sie so mit der Struktur eines Rings versehen werden kann, daß die Einbettung ein Ringhomomorphismus wird. Gleichbedeutend und expliziter ist das eine Teilmenge eines Rings, die sein Einselement enthält, die abgeschlossen ist unter Addition und Multiplikation, und die mit diesen Verknüpfungen zu einem Ring wird.

2.1.11. Die in II.2.4.3 bereits angesprochene Begriffsverwirrung setzt sich hier fort: Autoren, deren Ringe kein Einselement zu enthalten brauchen, fordern von ihren Teilringen zwar dem Wortlaut nach dasselbe wie wir im ersten Satz der Definition. Es bedeutet dann aber in unserer Terminologie nur noch, daß unsere Teilmenge unter Addition und Multiplikation abgeschlossen ist und mit diesen Verknüpfungen zu einem Rng wird. Wir nennen eine derartige Teilmenge einen **Teilrng**. Jedes Ideal eines Rings ist ein Teilrng, aber das einzige Ideal, das ein Teilring ist, ist der ganze Ring selber. Es ist im übrigen auch durchaus möglich, daß ein Teilrng eine Rings selbst wieder ein Ring ist, ohne aber in unserem Sinne ein Teilring zu sein: Der Nullring etwa ist ein Teilrng aber kein Teilring von $\mathbb{Q}$ und der Ring $\mathbb{Z} \times 0$ ist ein Teilrng aber kein Teilring von $\mathbb{Z} \times \mathbb{Z}$.

2.1.12. Jeder Schnitt von Teilringen ist selbst ein Teilring. Den kleinsten Teilring eines Ringes R, der eine gegebene Teilmenge $T \subset R$ umfaßt, heißt der **von** T **erzeugte Teilring**. Gegeben $S \supset R$ ein Kring mit einem Teilring und Elemente $a_1, \ldots, a_n \in S$ bezeichnet man mit

$$R[a_1, \ldots, a_n] \subset S$$

den Teilring von S, der von R und den a_i erzeugt wird, in anderen Worten den kleinsten Teilring von S, der R umfaßt und alle a_i enthält.

2.1.13. Die Notation aus 2.1.10 führt leicht zu Verwechslungen mit Polynomringen. Viele Autoren verwenden die Konvention, nach der die "freien" oder "unabhängigen" Variablen in Polynomringen mit großen Buchstaben vom Ende des Alphabets geschrieben werden, die "abhängigen" Erzeuger eines Teilrings in einem bereits gegebenen Ring dahingegen mit kleinen Buchstaben. Nebenbei bemerkt kann man $R[a_1, \ldots, a_n]$ auch beschreiben als das Bild des Einsetzungshomomorphismus $R[X_1, \ldots, X_n] \to S$ mit $X_i \mapsto a_i$. Ist dieser Einsetzungshomomorphismus injektiv, also ein Isomorphismus auf sein Bild, so heißen die Elemente a_i **algebraisch unabhängig über** R. Wollen wir besonders betonen, daß wir mit freien Veränderlichen arbeiten, so setzen wir ein kleines "Freiheitsstrichlein" vorne in die Klammer und schreiben $R[' X_1, \ldots, X_n]$. Diese Notation gibt es jedoch bis jetzt nur in diesem Skriptum.

2.1.14. Gegeben ein Ringhomomorphismus $\varphi : R \to S$ ist nach 2.1.4 der Kern $\ker \varphi$ ein Ideal von R und das Bild $\operatorname{im} \varphi$ offensichtlich ein Teilring von S. Nach

2.1.7 und dem Isomorphiesatz II.7.2.12 faktorisiert φ dann über einen Ringisomorphismus

$$R \twoheadrightarrow R/(\ker \varphi) \xrightarrow{\sim} \operatorname{im} \varphi \hookrightarrow S$$

2.1.15. Gegeben sei ein Ring R mit einem Ideal I. Bezeichnet $I[X] \subset R[X]$ das von unserem Ideal I im Polynomring erzeugte Ideal, so induziert der offensichtliche Ringhomomorphismus $R[X] \twoheadrightarrow (R/I)[X]$ aus II.2.5.6 offensichtlich einen Isomorphismus

$$R[X]/I[X] \xrightarrow{\sim} (R/I)[X]$$

Ergänzende Übung 2.1.16. Seien $K \subset L$ Körper, $I \subset K[X_1, \ldots, X_n]$ ein Ideal. Bezeichne $\langle IL[X_1, \ldots, X_n]\rangle$ das von I im Polynomring über L erzeugte Ideal. So gilt

$$I = K[X_1, \ldots, X_n] \cap \langle IL[X_1, \ldots, X_n]\rangle$$

Hinweis: Jedes Element von $\langle IL[X_1, \ldots, X_n]\rangle$ hat die Gestalt $c_1 f_1 + \ldots + c_r f_r$ mit $f_\nu \in I$ und $c_\nu \in L$ linear unabhängig über K.

Übung 2.1.17. Das Einsetzen von i für X im Sinne von II.2.5.4 liefert mithilfe der universellen Eigenschaft des Quotienten 2.1.7 Isomorphismen von Ringen $\mathbb{R}[X]/\langle X^2 + 1\rangle \xrightarrow{\sim} \mathbb{C}$ und $\mathbb{Z}[X]/\langle X^2 + 1\rangle \xrightarrow{\sim} \mathbb{Z}[\mathrm{i}]$. Hinweis: Die Existenz der fraglichen Ringhomomorphismen folgt aus den universellen Eigenschaften. Um zu sehen, daß sie Isomorphismen sind, muß allerdings noch mehr argumentiert werden, etwa mit 2.1.14. $\mathbb{Z}[\mathrm{i}]$ ist hier im Sinne von 2.1.10 zu verstehen als der Ring aller komplexen Zahlen mit ganzzahligem Real- und Imaginärteil.

Ergänzende Übung 2.1.18. Man zeige: Ist V ein Vektorraum über einem Körper k, so induziert der durch unsere Konstruktion der äußeren Algebra in II.9.5.5 gegebene Homomorphismus von Ringalgebren $\mathrm{T}_k V \twoheadrightarrow \bigwedge V$ von der Tensoralgebra aus II.9.5.9 auf die äußere Algebra einen Isomorphismus

$$\mathrm{T}_k V/\langle v \otimes w + w \otimes v\rangle \xrightarrow{\sim} \bigwedge V$$

der äußeren Algebra mit dem Quotienten der Tensoralgebra nach dem von allen $v \otimes w + w \otimes v$ mit $v, w \in V$ erzeugten Ideal.

Ergänzende Übung 2.1.19. Ist V ein Vektorraum über einem Körper k, so erklärt man die **symmetrische Algebra über** V als den Quotienten

$$\mathrm{S}_k V := \mathrm{T}_k V/\langle v \otimes w - w \otimes v\rangle$$

der Tensoralgebra aus II.9.5.9 nach dem von allen $v \otimes w - w \otimes v$ mit $v, w \in V$ erzeugten Ideal. Wenn sich der Grundkörper von selbst versteht, schreiben wir auch kürzer $\mathrm{S}V$. Man zeige: Ist $v_1, \ldots, v_n$ eine Basis von V, so erhalten wir einen Isomorphismus von k-Ringalgebren

$$k[X_1, \ldots, X_n] \xrightarrow{\sim} \mathrm{S}_k V$$

durch die Vorschrift $X_i \mapsto v_i$. Des weiteren zeige man für die symmetrische Algebra mit der offensichtlichen k-linearen Abbildung $\mathrm{can} : V \hookrightarrow \mathrm{S}_k V$, daß sie die zu II.9.5.9 analoge **universelle Eigenschaft** für Ringalgebrenhomomorphismen in kommutative Ringalgebren hat: Ist genauer A eine kommutative k-Ringalgebra und $\varphi : V \to A$ eine k-lineare Abbildung, so gibt es genau einen Homomorphismus von k-Ringalgebren $\hat{\varphi} : \mathrm{S}_k V \to A$ mit $\varphi = \hat{\varphi} \circ \mathrm{can}$, im Diagramm

$$\begin{array}{ccc} V & \xrightarrow{\mathrm{can}} & \mathrm{S}_k V \\ & \searrow^{\varphi} & \downarrow{\scriptstyle \hat{\varphi}} \\ & & A \end{array}$$

Die universelle Eigenschaft liefert einen Homomorphismus $\mathrm{S}_k V \to \mathrm{Ens}(V^\top, k)$ von k-Ringalgebren in die Ringalgebra aller k-wertigen Funktionen auf dem Dualraum von V. Ist k ein unendlicher Körper, so ist dieser Homomorphismus injektiv und induziert einen Isomorphismus von $\mathrm{S}_k V$ mit derjenigen Unterringalgebra von $\mathrm{Ens}(V^\top, k)$, die von allen Auswertungen an Vektoren $v \in V$ erzeugt wird. Ist speziell V endlichdimensional und k unendlich, so erhalten wir auf diese Weise einen Isomorphismus von $\mathrm{S}_k(V^\top)$ mit der von allen Linearformen erzeugten Unterringalgebra von $\mathrm{Ens}(V, k)$.

Ergänzende Übung 2.1.20. Bezeichnet $\mathrm{S}^r V$ das Bild von $V^{\otimes r} \subset \mathrm{T}V$ in $\mathrm{S}V$, so haben wir eine Zerlegung

$$\mathrm{S}V = \bigoplus_{r \geq 0} \mathrm{S}^r V$$

und das Produkt eines Elements von $\mathrm{S}^r V$ mit einem Element von $\mathrm{S}^p V$ liegt in $\mathrm{S}^{r+p} V$. Hier heißt $\mathrm{S}^r V$ die **homogene Komponente vom Grad** r der symmetrischen Algebra $\mathrm{S}V$.

Ergänzung 2.1.21. Meines Erachtens ist die allgemein übliche Bezeichnung von $\mathrm{S}V$ als "symmetrische Algebra" nicht besonders glücklich. Ich würde dazu lieber die "universelle Kringalgebra über V" sagen. Die allgemein übliche Bezeichnung hat den folgenden Ursprung: Natürlich operiert die symmetrische Gruppe $\mathcal{S}^r$ durch Vertauschung der Tensorfaktoren auf $V^{\otimes r}$. Die Invarianten $(V^{\otimes r})^{\mathcal{S}^r}$ unter dieser Operation heißen die **symmetrischen Tensoren** der Stufe r. In Charakteristik Null liefert nun eben für jedes $r \geq 0$ die Projektion $V^{\otimes r} \twoheadrightarrow \mathrm{S}^r V$ einen Isomorphismus $(V^{\otimes r})^{\mathcal{S}^r} \xrightarrow{\sim} \mathrm{S}^r V$ vom Raum der symmetrischen Tensoren der Stufe r mit der homogenen Komponente $\mathrm{S}^r V$ der Algebra $\mathrm{S}V$, deshalb die Bezeichnung als "symmetrische Algebra". Das Inverse dieses Isomorphismus heißt die **Symmetrisierung** und wird gegeben durch die Formel

$$v_1 \ldots v_r \mapsto \frac{1}{r!} \sum_{\sigma \in \mathcal{S}_r} v_{\sigma(1)} \otimes \ldots \otimes v_{\sigma(r)}$$

Genauer kann man im Fall eines Grundkörpers der Charakteristik Null den **Symmetrisator** $\mathrm{sym} : V^{\otimes r} \to (V^{\otimes r})^{\mathcal{S}_r}$ erklären durch die Abbildungsvorschrift

$$t \mapsto \frac{1}{r!} \sum_{\sigma \in \mathcal{S}_r} t^\sigma$$

Er ist eine Projektion im Sinne von II.1.6.5, wir haben also $\mathrm{sym}^2 = \mathrm{sym}$. Nun verschwindet sym auf $I_r := \langle v \otimes w - w \otimes v \rangle \cap V^{\otimes r}$, folglich faktorisiert sym über eine wohlbestimmte Abbildung $\mathrm{S}^r V \to (V^{\otimes r})^{\mathcal{S}_r}$. Andererseits faktorisiert auch die kanonische Projektion $V^{\otimes r} \twoheadrightarrow \mathrm{S}^r V$ über sym. Das zeigt $\ker(\mathrm{sym}) = I_r$ und wir können die Identität auf $(V^{\otimes r})^{\mathcal{S}_r}$ darstellen als eine Verknüpfung

$$(V^{\otimes r})^{\mathcal{S}_r} \hookrightarrow V^{\otimes r} \twoheadrightarrow \mathrm{S}^r V \xrightarrow{\sim} (V^{\otimes r})^{\mathcal{S}_r}$$

wobei die mittlere Abbildung die kanonische Projektion ist und die Komposition der mittleren mit der rechten Abbildung unser Symmetrisator sym . Das zeigt dann, daß im Fall eines Grundkörpers der Charakteristik Null die kanonische Projektion $V^{\otimes r} \twoheadrightarrow \mathrm{S}^r V$ in der Tat einen Isomorphismus $(V^{\otimes r})^{\mathcal{S}_r} \xrightarrow{\sim} \mathrm{S}^r V$ induziert.

Ergänzung 2.1.22. Ich will hier den Begriff des maximalen Ideals vermeiden, da er mir für die Ziele dieser Vorlesung ein Umweg scheint. Ich zeige in 2.3.27 nur, daß der Restklassenring eines Hauptidealrings nach dem von einem irreduziblen Element erzeugten Hauptideal stets ein Körper ist. Die Erkenntnis, daß das allgemeiner für beliebige Restklassenringe zu maximalen Idealen gilt, erkläre ich erst in **??**.

2.2 Der abstrakte chinesische Restsatz

Definition 2.2.1. Gegeben Ringe $R_1, \ldots, R_s$ bilden wir den **Produktring** $R_1 \times \ldots \times R_s$ mit komponentenweiser Addition und Multiplikation. Gegeben ein weiterer Ring R und Ringhomomorphismen $f_i : R \to R_i$ erhalten wir natürlich einen Ringhomomorphismus

$$\begin{array}{rccc} (f_1, \ldots, f_s) : & R & \to & R_1 \times \ldots \times R_s \\ & r & \mapsto & (f_1(r), \ldots, f_s(r)) \end{array}$$

Definition 2.2.2. Gegeben Ideale $\mathfrak{a}, \mathfrak{b}$ in einem Ring R ist auch ihre **Summe** $\mathfrak{a} + \mathfrak{b} = \{a+b \mid a \in \mathfrak{a},\ b \in \mathfrak{b}\}$ ein Ideal, und wir nennen ihr **Produkt** und bezeichnen mit $\langle \mathfrak{a}\mathfrak{b} \rangle$ dasjenige Ideal oder gleichbedeutend diejenige additive Untergruppe von R, das bzw. die von allen Produkten ab mit $a \in \mathfrak{a}$ und $b \in \mathfrak{b}$ erzeugt wird. Analog notieren wir auch Produkte von mehr als zwei Idealen.

2.2.3. Für das Produkt zweier Ideale ist eigentlich die Notation $\mathfrak{a}\mathfrak{b}$ gebräuchlich, die wir aber bereits für die von der Multiplikation eines Rings auf seiner Potenzmenge induzierte Verknüpfung vergeben haben.

Satz 2.2.4 (Abstrakter chinesischer Restsatz). *Seien R ein Ring und $\mathfrak{a}_1, \ldots, \mathfrak{a}_s \subset R$ Ideale. Gilt $\mathfrak{a}_i + \mathfrak{a}_j = R$ für $i \neq j$, so ist die offensichtliche Abbildung*

$$\varphi : R \to R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_s$$

eine Surjektion mit dem Schnitt der $\mathfrak{a}_i$ als Kern. Für einen kommutativen Ring R fällt dieser Schnitt auch zusammen mit dem Produktideal $\langle \mathfrak{a}_1 \ldots \mathfrak{a}_s \rangle$ und wir erhalten einen Ringisomorphismus

$$R/\langle \mathfrak{a}_1 \ldots \mathfrak{a}_s \rangle \quad \tilde{\to} \quad R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_s$$

Beispiel 2.2.5. Der Name dieses Satzes rührt von seiner Bedeutung im Ring der ganzen Zahlen her, die wir bereits in II.7.3.19 besprochen hatten.

Beweis. Für die Surjektivität reicht es nachzuweisen, daß alle nur in einem Eintrag von Null verschiedenen Tupel im Bild liegen. Ohne Beschränkung der Allgemeinheit reicht es also zu zeigen, daß für alle $r \in R$ das Tupel $(\bar{r}, 0, \ldots, 0)$ im Bild liegt. Es reicht sogar, wenn wir das für $r = 1$ zeigen, denn aus $\varphi(x) = (\bar{1}, 0, \ldots, 0)$ folgt $\varphi(rx) = \varphi(r)\varphi(x) = (\bar{r}, 0, \ldots, 0)$. Nach Annahme gilt für $i \neq 1$ jedoch $\mathfrak{a}_i + \mathfrak{a}_1 = R$, wir finden für $i \neq 1$ also eine Darstellung $a_i + b_i = 1$ mit $a_i \in \mathfrak{a}_i$ und $b_i \in \mathfrak{a}_1$. Für das Ringelement $a_i = 1 - b_i$ hat $\varphi(a_i)$ dann natürlich die Gestalt

$$\varphi(a_i) = (1, *, \ldots, *, 0, *, \ldots *)$$

mit einer Null an der i-ten Stelle. Für das Bild des Produkts der a_i folgt dann $\varphi(a_2 a_3 \ldots a_s) = (1, 0, \ldots, 0)$ und die Surjektivität ist gezeigt. Der Kern dieser Surjektion ist offensichtlich genau der Schnitt der $\mathfrak{a}_i$, und wir müssen nur noch zeigen, daß er für kommutatives R mit dem Produktideal zusammenfällt. Im Fall $s = 2$ impliziert $\mathfrak{a} + \mathfrak{b} = R$ schon mal $\mathfrak{a} \cap \mathfrak{b} = \langle \mathfrak{a}\mathfrak{b} \rangle$, denn schreiben wir $1 = a + b$ mit $a \in \mathfrak{a}$ und $b \in \mathfrak{b}$, so gilt $x = xa + xb$ auch für alle $x \in \mathfrak{a} \cap \mathfrak{b}$. Im allgemeinen beachten wir, daß das Aufmultiplizieren unserer Identitäten $a_i + b_i = 1$ von eben für $2 \leq i \leq n$ sogar zeigt $\mathfrak{a}_1 + \langle \mathfrak{a}_2 \ldots \mathfrak{a}_s \rangle = R$. Mit vollständiger Induktion erhalten wir dann $\mathfrak{a}_1 \cap (\mathfrak{a}_2 \cap \ldots \cap \mathfrak{a}_s) = \mathfrak{a}_1 \cap \langle \mathfrak{a}_2 \ldots \mathfrak{a}_s \rangle = \langle \mathfrak{a}_1 \langle \mathfrak{a}_2 \ldots \mathfrak{a}_s \rangle \rangle = \langle \mathfrak{a}_1 \mathfrak{a}_2 \ldots \mathfrak{a}_s \rangle$. □

2.2.6. Wir schreiben auch $\langle I^n \rangle$ für das n-fache Produkt eines Ideals mit sich selbst. Betrachten wir zum Beispiel $R = k[X, Y]$ für einen Körper k und darin das Ideal $I = \langle X, Y \rangle$, so gilt $\langle I^2 \rangle = \langle X^2, XY, Y^2 \rangle$, $\langle I^3 \rangle = \langle X^3, X^2Y, XY^2, Y^3 \rangle$ und so weiter.

Korollar 2.2.7 (Interpolation durch Polynome). *Sei k ein Körper und $n \in \mathbb{N}$. Wir finden stets ein Polynom $P \in k[X_1, \ldots, X_n]$, das an endlich vielen vorgegebenen Stellen des k^n vorgegebene Werte annimmt und sogar eine beliebig vorgegebene "Taylorentwicklung bis zu einem festen endlichen Grad" hat.*

Eine Interpolation in einer Variablen mit vorgegebenen Werten an zwei Punkten und vorgegebenem Wert und Wert der Ableitung an einem weiteren Punkt

Beweis. Für einen Punkt $p \in k^n$ bezeichne $I(p)$ das Ideal aller Polynome, die bei p verschwinden. Mit der vagen Formulierung "die Taylorentwicklung bei p eines Polynoms $P \in k[X_1, \ldots, X_n]$ bis zum Grad $m-1$ vorzugeben" meinen wir, seine Nebenklasse in $k[X_1, \ldots, X_n]/\langle I(p)^m \rangle$ vorzugeben. Damit wir den abstrakten chinesischen Restsatz anwenden können, müssen wir nur noch zeigen $\langle I(p)^m \rangle + \langle I(q)^m \rangle = \langle 1 \rangle$ falls $p \neq q$. Offensichtlich gilt $I(p) + I(q) = \langle 1 \rangle$, denn p und q unterscheiden sich in mindestens einer Koordinate, sagen wir $p_i \neq q_i$, und dann ist $(X_i - p_i) + (q_i - X_i)$ eine Einheit im Polynomring. Schreiben wir nun $1 = a + b$ mit $a \in I(p)$ und $b \in I(q)$ und nehmen von dieser Gleichung die $2m$-te Potenz, so folgt $1 \in \langle I(p)^m \rangle + \langle I(q)^m \rangle$ wie gewünscht. □

Ergänzung 2.2.8. Unter dem **Zentrum** $Z(R)$ eines Rings R verstehen wir die Menge derjenigen Elemente von R, die mit allen anderen Elementen kommutieren, in Formeln

$$Z(R) = \{z \in R \mid za = az \ \ \forall a \in R\}$$

Das Zentrum ist stets ein kommutativer Teilring von R.

Ergänzung 2.2.9. Für jede Zerlegung $A = A_1 \oplus \ldots \oplus A_n$ eines Rings in eine Summe zweiseitiger Ideale sind die Summanden A_i unter der induzierten Multiplikation selber Ringe mit Eins-Element 1_r für $1 = 1_1 + \ldots + 1_n$ die unserer Zerlegung entsprechende Zerlegung der Eins des Rings A. Des weiteren liefert dann das Aufaddieren auch einen Ringisomorphismus

$$A_1 \times \ldots \times A_n \xrightarrow{\sim} A$$

und die 1_i liegen im Zentrum von A und haben die Eigenschaft $1_i 1_j = \delta_{ij} 1_i$. Haben wir umgekehrt eine Darstellung $1 = 1_1 + \ldots + 1_n$ mit 1_i zentral und $1_i 1_j = \delta_{ij} 1_i$, so zerfällt A in das Produkt der Ideale $A_i = \langle 1_i \rangle$. Wir nennen eine solche Darstellung eine **Zerlegung der Eins in paarweise orthogonale zentrale Idempotente**. Fassen wir in einer derartigen Zerlegung einige Summanden zusammen, so sprechen wir von einer **Vergröberung** unserer Zerlegung. Natürlich haben je zwei derartige Zerlegungen eine gemeinsame Verfeinerung, bestehend aus allen Produkten von einem Idempotenten der einen Zerlegung und einem Idempotenten der anderen Zerlegung. Existiert eine feinste Zerlegung mit von Null verschiedenen Summanden, so ist sie demnach eindeutig. Die zugehörige Zerlegung des Rings heißt dann seine **Block-Zerlegung** $A = A_1 \times \ldots \times A_n$ und die zugehörigen Faktoren A_i heißen die **Blöcke** des Rings A. Rückblickend können wir festhalten, daß bei einem Ring, der eine Zerlegung in eine endliche direkte Summe ihrerseits nicht weiter zerlegbarer zweisetiger Ideale besitzt, die Summanden wohlbestimmt sind und dann eben die Blöcke unseres Rings heißen.

2.3 Euklidische Ringe und Primfaktorzerlegung

2.3.1. Die folgende schematische Übersicht soll die Struktur dieses Abschnitts und die Beziehungen der darin neu eingeführten Begriffe untereinander verdeutlichen:

Interessante Ringe, etwa $\mathbb{Z}$, $\mathbb{Z}[\mathrm{i}]$, oder der Ring $k[X]$ für einen Körper k;
$\cap$
Euklidische Ringe, in denen es eine "Division mit Rest" gibt;
$\cap$
Hauptidealringe, in denen jedes Ideal von einem Element erzeugt wird;
$\cap$
Faktorielle Ringe, d.h. Ringe mit "eindeutiger Primfaktorzerlegung".

Wir arbeiten nun unser Schema von unten nach oben ab und beginnen mit faktoriellen Ringen.

Definition 2.3.2. Ein Element a eines Krings R heißt **irreduzibel** oder genauer **irreduzibel in** R genau dann, wenn gilt:

1. a ist keine Einheit, in Formeln $a \notin R^\times$;
2. In jeder Darstellung von a als Produkt von zwei Ringelementen ist einer der beiden Faktoren eine Einheit, in Formeln $a = bc \Rightarrow b \in R^\times$ oder $c \in R^\times$.

Beispiele 2.3.3. Die Null ist nie irreduzibel: Im Nullring ist sie eine Einheit, in anderen Kringen das Produkt der zwei Nichteinheiten $0 = 0 \cdot 0$. Eine ganze Zahl $n \in \mathbb{Z}$ ist irreduzibel in $\mathbb{Z}$ genau dann, wenn ihr Betrag $|n|$ eine Primzahl ist. In einem Körper gibt es überhaupt keine irreduziblen Elemente, insbesondere ist auch keine ganze Zahl n irreduzibel in $\mathbb{Q}$.

2.3.4. Ein Element a eines Krings ist irreduzibel genau dann, wenn das von ihm erzeugte Hauptideal nicht Null und nicht der ganze Kring ist, jedes echt größere Hauptideal aber der ganze Kring ist, in Formeln ausgedrückt: Wenn gilt $0 \neq \langle a \rangle \neq R$ und $(\langle a \rangle \subsetneq \langle b \rangle \Rightarrow \langle b \rangle = R)$.

Definition 2.3.5. Ein Ring R heißt **faktoriell** genau dann, wenn R ein kommutativer Integritätsbereich ist und wenn zusätzlich gilt:

1. Jedes $a \in R \backslash 0$ läßt sich darstellen als ein Produkt von irreduziblen Elementen und einer Einheit, in Formeln $a = up_1 \ldots p_n$ mit $u \in R^\times$, p_i irreduzibel und $n \geq 0$.
2. Diese Darstellung ist eindeutig bis auf Einheiten und die Reihenfolge der Faktoren. Ist genauer $a = u'p'_1 \ldots p'_{n'}$ eine zweite Darstellung wie eben, so gilt $n = n'$ und es gibt eine Permutation $\sigma \in \mathcal{S}_n$ von n sowie Einheiten $u_i \in R^\times$ mit $p'_i = u_i p_{\sigma(i)}$ für $1 \leq i \leq n$.

Übung 2.3.6. Der Quotient eines faktoriellen Rings R nach einem Hauptideal $\langle a\rangle$ ist genau dann ein Integritätsbereich, wenn gilt $a = 0$ oder a irreduzibel.

Ergänzung 2.3.7. Gegeben ein Integritätsbereich bilden die von Null verschiedenen Elemente ein Monoid, und die Definition eines faktoriellen Rings 2.3.5 ist äquivalent zu einer Forderung an die Struktur dieses Monoids: Ein Ring ist faktoriell genau dann, wenn er ein Integritätsbereich ist und das multiplikative Monoid seiner von Null verschiedenen Elemente isomorph ist zum Produkt einer kommutativen Gruppe mit dem Monoid aller fast überall verschwindenden Abbildungen von einer Menge in das additive Monoid $\mathbb{N}$.

Beispiele 2.3.8. Unsere einzigen Beispiele für faktorielle Ringe sind bisher $\mathbb{Z}$ und alle Körper. Im folgenden werden wir viele weitere Beispiele für faktorielle Ringe kennenlernen. Insbesondere zeigen wir, daß Polynomringe über Körpern stets faktoriell sind. Als Beispiel für einen nicht faktoriellen Integritätsbereich betrachten wir den Teilring $\mathbb{Z}[\sqrt{-5}]$ der komplexen Zahlen, der gegeben wird durch

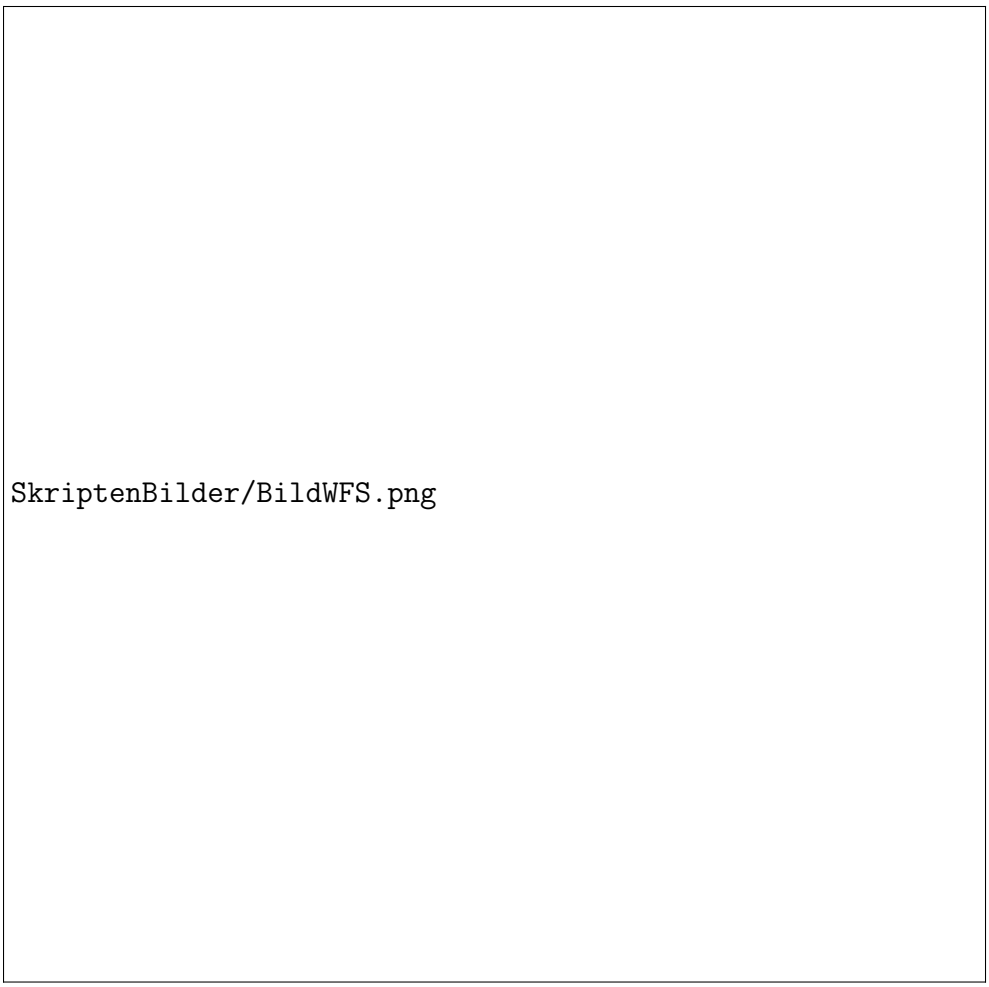
$$\mathbb{Z}[\sqrt{-5}] = \{a + b\,\mathrm{i}\,\sqrt{5} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

Ich behaupte, daß $6 = 2\cdot 3 = (1+\sqrt{-5})\cdot(1-\sqrt{-5})$ zwei Zerlegungen in irreduzible Faktoren sind, die sich nicht nur um Einheiten und Reihenfolge unterscheiden. Das folgt leicht unter Verwendung der Multiplikativität der Norm $|zw| = |z||w|$ für $z, w \in \mathbb{C}$ aus der anschließenden Tabelle, in der alle Elemente $z \in \mathbb{Z}[\sqrt{-5}]$ der Quadratlänge $|z|^2 \leq 9$ aufgelistet sind.

$\lvert z\rvert^2$	mögliche $z \in \mathbb{Z}[\sqrt{-5}]$
0	0
1	± 1
4	± 2
5	$\pm\sqrt{-5}$
6	$(\pm 1) + (\pm\sqrt{-5})$
9	± 3, $(\pm 2) + (\pm\sqrt{-5})$

Definition 2.3.9. Ein Ring R heißt ein **Hauptidealring** genau dann, wenn R ein kommutativer Integritätsbereich ist und jedes Ideal von R ein Hauptideal ist, d.h. von einem einzigen Element erzeugt wird.

2.3.10. Für meinen Geschmack ist diese Definition überfrachtet. Ich hätte lieber einen Hauptidealring als einen Ring definiert, in dem eben jedes Ideal ein Hauptideal ist. Diese Konvention ist nun jedoch wohl leider nicht mehr zu ändern.



Einige Elemente des Rings $\mathbb{Z}[\sqrt{-5}]$ als Punkte in der Gauß'schen Zahlenebene

Beispiel 2.3.11. Nach II.2.2.16 ist der Ring $\mathbb{Z}$ der ganzen Zahlen ein Hauptidealring. Der Polynomring in zwei Variablen $\mathbb{C}[X,Y]$ ist kein Hauptidealring, denn das Ideal aller beim Ursprung von $\mathbb{C}^2$ verschwindenden Polynome ist kein Hauptideal: Jedes Polynom, das am Ursprung verschwindet, verschwindet auch sonst noch irgendwo, und dasselbe gilt für alle Polynome des von ihm erzeugten Hauptideals.

Satz 2.3.12. *Jeder Hauptidealring ist faktoriell.*

Beweis. Wir zeigen als erstes, daß sich in einem Hauptidealring jedes Element $a \in R\backslash 0$ zerlegen läßt als Produkt einer Einheit mit endlich vielen irreduziblen Elementen. Wir bemerken dazu, daß in einem Integritätsbereich R die Gleichheit $\langle a\rangle = \langle b\rangle$ von Hauptidealen äquivalent ist zu $a = ub$ mit $u \in R^\times$. Jetzt argumentieren wir durch Widerspruch. Gäbe es $a \in R\backslash 0$, das sich nicht in ein Produkt einer Einheit mit höchstens endlich vielen Irreduziblen zerlegen läßt, so wäre insbesondere a selbst weder eine Einheit noch irreduzibel, also von der Gestalt $a = a_1b_1$ mit $a_1, b_1 \notin R^\times$. Hier können nicht sowohl a_1 als auch b_1 eine Zerlegung in ein Produkt von Irreduziblen besitzen. Wir dürfen ohne Beschränkung der Allgemeinheit annehmen, a_1 habe keine Zerlegung in Irreduzible, und können schreiben $a_1 = a_2b_2$ mit $a_2, b_2 \notin R^\times$ und a_2 ohne Zerlegung in Irreduzible. Indem wir so weitermachen, finden wir in R eine unendliche echt aufsteigende Folge von Hauptidealen

$$\langle a\rangle \subset \langle a_1\rangle \subset \langle a_2\rangle \subset \dots$$

Die Vereinigung über alle diese Hauptideale ist auch ein Ideal, also ein Hauptideal $\langle h\rangle$. Andererseits ist diese Vereinigung aber auch das Erzeugnis $\langle h\rangle = \langle a, a_1, a_2, \dots\rangle$ der a_i. Es folgt eine Relation der Gestalt $h = ra + r_1a_1 + \dots + r_na_n$ und damit $\langle h\rangle = \langle a_n\rangle$ im Widerspruch zu $\langle a_n\rangle \neq \langle a_{n+1}\rangle$. Dieser Wiederspruch zeigt die Existenz der Zerlegung. Jetzt zeigen wir die Eindeutigkeit. Dazu vereinbaren wir folgende Definition.

Definition 2.3.13. Sei R ein kommutativer Ring. Ein Element $p \in R$ heißt ein **Primelement** oder kurz **prim**, falls es (1) weder Null noch eine Einheit ist und falls (2) aus $p|ab$ folgt $p|a$ oder $p|b$.

2.3.14. Mir scheint diese Terminologie eine unglückliche Wahl, aber sie ist nun einmal historisch gewachsen. Einerseits sind nun zwar die positiven Primelemente des Rings der ganzen Zahlen $\mathbb{Z}$ genau unsere Primzahlen, aber das ist bereits ein nichttrivialer Satz: Von ihrer ursprünglichen Definition her versteht man unter Primzahlen ja viel eher die positiven irreduziblen Elemente dieses Rings. Andererseits wäre es auch natürlich, in einem beliebigen kommutativen Ring diejenigen Elemente als Primelemente zu bezeichnen, die im Sinne von **??** “ein Primideal

erzeugen", aber dann müßten wir in der obigen Definition auch die Null als Primelement zulassen. So gesehen sitzt man mit der obigen allgemein gebräuchlichen Definition eines Primelements leider zwischen allen Stühlen.

2.3.15. Primelemente in Integritätsbereichen sind offensichtlich stets irreduzibel, aber irreduzible Elemente müssen auch in Integritätsbereichen im allgemeinen nicht prim sein. In einem faktoriellen Ring sind die Primelemente genau die irreduziblen Elemente. Um allerdings zu beweisen, daß ein Hauptidealring faktoriell ist, brauchen wir ein weiteres Lemma.

Lemma 2.3.16. *In einem Hauptidealring sind die Primelemente genau die irreduziblen Elemente.*

Beweis. Wir müssen nur zeigen, daß jedes irreduzible Element ein Primelement ist. Sei also R unser Hauptidealring und sei $p \in R$ irreduzibel. Seien $a, b \in R$ gegeben mit $p|ab$. Wir nehmen an $p \nmid a$ und folgern $p|b$. Denn sei $\langle a, p\rangle$ das von a und p erzeugte Ideal. Es ist nach Annahme ein Hauptideal, sagen wir $\langle a, p\rangle = \langle d\rangle$. Da p irreduzibel ist, liegt nach 2.3.4 über dem von p erzeugten Hauptideal als einziges weiteres Hauptideal der ganze Ring, in Formeln gilt also $\langle d\rangle = \langle p\rangle$ oder $\langle d\rangle = \langle 1\rangle$. Da p nicht a teilt, folgt $\langle d\rangle \neq \langle p\rangle$, also $\langle d\rangle = R$. Mithin können wir schreiben $1 = ax + py$ für geeignete $x, y \in R$. Es folgt $b = abx + pby$ und aus $p|ab$ erhalten wir wie gewünscht $p|b$. □

Damit sind also alle irreduziblen Elemente in unserem Hauptidealring R Primelemente. Ist nun p_1' ein Faktor unserer alternativen Zerlegung von a, so gibt es ein i mit $p_1'|p_i$ und damit $p_1' = u_1 p_i$ für eine Einheit u_1. Wir setzen $i = \sigma(1)$, kürzen in beiden Produkten, und beenden den Beweis mit Induktion. □

Ergänzende Übung 2.3.17. Man zeige: Gegeben ein Körper k ist der Ring $k[\![X]\!]$ der formalen Potenzreihen mit Koeffizienten aus k aus II.2.5.33 ein Hauptidealring, und die Ideale dieses Rings sind das Nullideal sowie die Ideale $X^n k[\![X]\!]$ für $n \in \mathbb{N}$. Man bespreche die Primfaktorzerlegung in diesem Hauptidealring.

Definition 2.3.18. Ein **euklidischer Ring** ist ein kommutativer Integritätsbereich mit einer Abbildung $\sigma : R\backslash 0 \to \mathbb{N}$ derart, daß man für alle $a, b \in R$ mit $a \neq 0$ Elemente $p, q \in R$ finden kann mit $b = aq + r$ und $r = 0$ oder $\sigma(r) < \sigma(a)$.

2.3.19. Grob gesagt ist also ein euklidischer Ring ein Integritätsbereich, in dem man "teilen kann mit Rest", wobei der Rest in einer präzisen, durch σ spezifizierten Weise "kleiner" sein soll als der Teiler. Alle unsere Argumente funktionieren auch noch, wenn σ allgemeiner Werte in einer beliebigen "wohlgeordneten" Menge annimmt, als da heißt einer angeordneten Menge, in der jede nichtleere Teilmenge ein kleinstes Element besitzt.

Beispiele 2.3.20. 1. $R = \mathbb{Z}$ mit $\sigma(n) = |n|$.

2. $R = k[X]$ für einen Körper k und $\sigma(P) = \operatorname{grad} P$, siehe II.2.5.15.

3. $R = \mathbb{Z}[\mathrm{i}] = \{x + y\,\mathrm{i} \mid x, y \in \mathbb{Z}\}$, $\sigma(x + y\,\mathrm{i}) = x^2 + y^2$. Dieser Ring der sogenannten **Gauß'schen Zahlen** ist als Teilring von $\mathbb{C}$ zu verstehen. Wir werden dies Beispiel in 2.4 noch ausführlich besprechen.

Satz 2.3.21. *Jeder euklidische Ring ist ein Hauptidealring und damit insbesondere faktoriell.*

Beweis. Sei $I \subset R$ ein Ideal. Ist $I = 0$, so ist $I = \langle 0\rangle$ ein Hauptideal. Sonst finden wir $a \in I\backslash 0$ mit $\sigma(a)$ kleinstmöglich. Wir behaupten $I = \langle a\rangle$. Gäbe es nämlich $b \in I\backslash\langle a\rangle$, so könnten wir schreiben $b = aq + r$ mit $r \neq 0$ und $\sigma(r) < \sigma(a)$. Dann gilt aber auch $r = b - aq \in I$, und das steht im Widerspruch zur Wahl von a. □

Bemerkung 2.3.22. Der vorhergehende Satz 2.3.21 und sein Beweis sind unmittelbare Verallgemeinerungen unseres Satzes II.2.2.16 über die Untergruppen von $\mathbb{Z}$ und des dort gegebenen Beweises.

Korollar 2.3.23. *Der Polynomring in einer Veränderlichen mit Koeffizienten einem Körper ist stets ein Hauptidealring und ist insbesondere stets faktoriell.*

Beweis. Wie in 2.3.20 ausgeführt wird, ist unser Polynomring ein euklidischer Ring. Das Korollar folgt damit aus 2.3.21. □

2.3.24. Die irreduziblen Elemente des Polynomrings $k[X]$ mit Koeffizienten in einem Körper k nennt man **irreduzible Polynome**. In Zusammenhängen, in denen man mit mehreren Körpern gleichzeitig arbeitet, werden wir manchmal präziser von **k-irreduziblen** Polynomen reden, da dieser Begriff ganz entscheidend von k abhängt. Zum Beispiel ist das Polynom $X^2 + 1$ zwar $\mathbb{R}$-irreduzibel, aber keineswegs $\mathbb{C}$-irreduzibel.

Beispiel 2.3.25. Die irreduziblen Polynome in $\mathbb{C}[X]$ sind nach II.2.5.26 genau die Polynome vom Grad Eins. Die irreduziblen Polynome in $\mathbb{R}[X]$ sind nach II.2.5.28 genau die Polynome vom Grad Eins sowie die Polynome vom Grad Zwei ohne reelle Nullstelle. Die irreduziblen Polynome in $\mathbb{Q}[X]$ zu bestimmen, ist dahingegen ziemlich schwierig.

Übung 2.3.26. Sei k ein Körper. Man zeige: (1) Alle Polynome vom Grad 1 sind irreduzibel in $k[X]$. (2) Ist $P \in k[X]$ irreduzibel und $\operatorname{grad} P > 1$, so hat P keine Nullstelle in k. (3) Ist $P \in k[X] \setminus k$ vom Grad $\operatorname{grad} P \leq 3$ und hat P keine Nullstelle in k, so ist P irreduzibel in $k[X]$. (4) Ist k algebraisch abgeschlossen, so sind die irreduziblen Polynome in $k[X]$ genau die Polynome vom Grad 1.

Satz 2.3.27 (Quotienten von Hauptidealringen). *Für den Quotienten eines Hauptidealrings nach einem von Null verschiedenen Ideal sind gleichbedeutend:*

1. *Unser Quotient ist ein Körper;*

2. *Ein und jeder Erzeuger unseres Ideals ist ein irreduzibles Element.*

Ergänzung 2.3.28. In **??** werden wir lernen, daß ein Quotient eines kommutativen Rings nach einem Ideal genau dann ein Körper ist, wenn unser Ideal ein "maximales Ideal" ist. In diesem Licht sind also die maximalen Ideale eines Hauptidealrings, der nicht bereits ein Körper ist, genau die von seinen irreduziblen Elementen erzeugten Hauptideale.

Beispiel 2.3.29. $\mathbb{Z}/p\mathbb{Z}$ ist genau dann ein Körper, wenn p oder $-p$ eine Primzahl ist.

Beispiel 2.3.30. $\mathbb{R}[X]/\langle X^2+1\rangle$ ist ein Körper, genauer induziert das Einsetzen von i für X einen Isomorphismus dieses Körpers mit $\mathbb{C}$.

Beispiel 2.3.31. $\mathbb{R}[X]/\langle X^2+2\rangle$ ist ein Körper, genauer induziert das Einsetzen von $\mathrm{i}\sqrt{2}$ für X einen Isomorphismus dieses Körpers mit $\mathbb{C}$.

Beispiel 2.3.32. $\mathbb{R}[X]/\langle X+1\rangle$ ist ein Körper, genauer induziert das Einsetzen von -1 für X einen Isomorphismus dieses Körpers mit $\mathbb{R}$.

Beispiel 2.3.33. $\mathbb{R}[X]/\langle X^2-1\rangle$ ist *kein* Körper, vielmehr liefert der chinesische Restsatz in Verbindung mit dem vorhergehenden Beispiel einen Ringisomorphismus $\mathbb{R}[X]/\langle X^2-1\rangle \xrightarrow{\sim} \mathbb{R}\times\mathbb{R}$, und $\mathbb{R}\times\mathbb{R}$ besitzt Nullteiler: Es gilt darin ja etwa $(1,0)(0,1)=(0,0)$.

Beweis. Sei R unser Hauptidealring und $I=\langle a\rangle$ unser von Null verschiedenes Ideal. Ist a nicht irreduzibel, so gibt es eine Zerlegung $a=bc$ mit $b,c\notin R^\times$. Daraus folgt $c,b\notin\langle a\rangle$ und damit sind die Nebenklassen $\bar b,\bar c\in R/I$ von Null verschiedene Nullteiler und unser Quotient ist kein Körper. Ist dahingegen a irreduzibel und $b\notin\langle a\rangle$, so ist jeder Erzeuger d des Ideals $\langle a,b\rangle$ Teiler von a aber kein Vielfaches von a und damit eine Einheit. Es folgt $\langle a,b\rangle=R$ und damit gibt es $x,y\in R$ mit $ax+by=1$. Dann aber ist die Nebenklasse $\bar y$ in R/I ein Inverses zu $\bar b$, und da in dieser Weise jedes von Null verschiedene Element dieses Quotienten ein Inverses besitzt, ist besagter Quotient ein Körper. □

Ergänzende Übung 2.3.34. In einem Polynomring in mindestens einer Variablen über einem Körper gibt es stets unendlich viele normierte irreduzible Polynome. Hinweis: Man multipliziere sonst alle zusammen und ziehe 1 ab.

2.4 Irreduzible im Ring der Gauß'schen Zahlen

Lemma 2.4.1. *Der Ring $\mathbb{Z}[\mathrm{i}]$ der Gauß'schen Zahlen ist euklidisch und damit auch faktoriell.*

Einige Punkte des Gitters der Vielfachen von $1 + 3\,\mathrm{i}$ als fette Punkte im Ring der Gauß'schen Zahlen, von dem ich einige andere Elemente durch kleine Punkte angedeutet habe.

Beweis. Im Ring $\mathbb{Z}[\mathrm{i}]$ der Gauß'schen Zahlen bilden die Vielfachen eines festen von Null verschiedenen Elements $0 \neq a = x + \mathrm{i}\,y \in \mathbb{Z}[\mathrm{i}]$ die Ecken eines quadratischen Rasters auf der komplexen Zahlenebene, mit $|a| = \sqrt{x^2 + y^2}$ der Seitenlänge der Quadrate. Jedes $b \in \mathbb{Z}[\mathrm{i}]$ liegt in einem dieser Quadrate und hat von einer der Ecken einen Abstand $\leq \sqrt{2}|a|/2 < |a|$. Folglich ist unser Ring euklidisch mit $\sigma(a) = |a|^2$. □

2.4.2. Von nun an wird in diesem Abschnitt der Begriff "Quadrat" nicht mehr in seiner geometrischen Bedeutung verwendet, sondern in seiner algebraischen Bedeutung als Abkürzung für "Quadratzahl". Die ersten Quadrate in $\mathbb{Z}$ sind also $0, 1, 4, 9, 16, 25, \ldots$

2.4.3. Der Ring der Gauß'schen Zahlen besitzt genau vier Einheiten, als da sind $1, -1, \mathrm{i}$, und $-\mathrm{i}$. Die irreduziblen Elemente von $\mathbb{Z}[\mathrm{i}]$ bestimmt der folgende Satz. Man beachte, daß jede Gauß'sche Zahl ungleich Null durch Multiplikation mit einer Einheit auf genau eine Gauß'sche Zahl in der Vereinigung des offenen ersten Quadranten mit der positiven reellen Achse abgebildet werden kann.

Satz 2.4.4 (Irreduzible im Ring der Gauß'schen Zahlen). *1. Die irreduziblen Elemente im Ring $\mathbb{Z}[\mathrm{i}]$ der Gauß'schen Zahlen, die im offenen ersten Quadranten liegen, sind genau die $x + \mathrm{i}\,y$ für $x, y \in \mathbb{N}$ mit $x^2 + y^2$ prim in $\mathbb{Z}$.*

2. *Die irreduziblen Elemente im Ring $\mathbb{Z}[\mathrm{i}]$ der Gauß'schen Zahlen, die auf der positiven reellen Achse liegen, sind genau die Primzahlen $p \in \mathbb{N}$ mit $p \equiv 3 \pmod 4$.*

3. *Umgekehrt gibt es für Primzahlen $p \in \mathbb{N}$ mit $p \equiv 3 \pmod 4$ nie eine ganzzahlige Lösung der Gleichung $x^2 + y^2 = p$, und für Primzahlen $p \in \mathbb{N}$ mit $p \not\equiv 3 \pmod 4$ gibt es bis auf Reihenfolge stets genau eine Lösung der Gleichung $x^2 + y^2 = p$ mit $x, y \in \mathbb{N}$.*

Beispiele 2.4.5. $2 = 1^2 + 1^2$, $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, $17 = 1^2 + 4^2$, $\ldots$

2.4.6. Eine mögliche Zerlegung einer Primzahl $p \in \mathbb{N}$ in ein Produkt irreduzibler Elemente von $\mathbb{Z}[\mathrm{i}]$ hat nach unserem Satz folgende Gestalt:

$$\begin{array}{ll} p \equiv 3 \pmod 4 & p = p; \\ p \not\equiv 3 \pmod 4 & p = (x + \mathrm{i}\,y)(x - \mathrm{i}\,y) \text{ für } x^2 + y^2 = p. \end{array}$$

Beschränken wir uns auf die irreduziblen Elemente von Teil 1 des Satzes, so müssen wir die Faktorisierung von p im zweiten Fall etwas unübersichtlicher schreiben als $p = -\mathrm{i}(x + \mathrm{i}\,y)(y + \mathrm{i}\,x)$. Man beachte, daß die Primzahl 2 insofern eine Sonderrolle spielt, als bei ihr und nur bei ihr ein irreduzibler Faktor bis auf Einheiten doppelt vorkommt: Wir haben nämlich $2 = -\mathrm{i}(1 + \mathrm{i})^2$.

Beweis. Wir behaupten zunächst für $\pi = x + \mathrm{i}\,y \in \mathbb{Z}[\mathrm{i}]$ weder reell noch rein imaginär die Äquivalenz

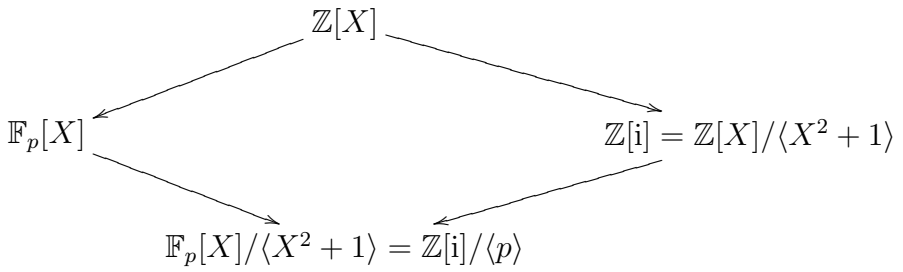
$$\pi \text{ ist prim in } \mathbb{Z}[\mathrm{i}] \quad \Leftrightarrow \quad \pi\bar{\pi} = x^2 + y^2 \text{ ist prim in } \mathbb{Z}$$

Ist in der Tat π prim in $\mathbb{Z}[\mathrm{i}]$, so ist $\pi\bar{\pi} = x^2 + y^2$ prim in $\mathbb{Z}$ aufgrund der Eindeutigkeit der Zerlegung in irreduzible Faktoren in $\mathbb{Z}[\mathrm{i}]$. Ist umgekehrt π nicht prim in $\mathbb{Z}[\mathrm{i}]$, sagen wir $\pi = ab$ mit $|a| > 1$ und $|b| > 1$, so gilt $\pi\bar{\pi} = (a\bar{a})(b\bar{b})$, und das ist nicht prim in $\mathbb{Z}$. Damit ist Teil 1 gezeigt. Die Eindeutigkeit der Darstellung einer Primzahl p als Summe von zwei Quadraten in Teil 3 folgt sofort mit Teil 1 aus der Eindeutigkeit der Zerlegung in irreduzible Faktoren im Ring der Gauß'schen Zahlen. Die restlichen Behauptungen des Satzes folgen unmittelbar aus der anschließenden Proposition. □

Proposition 2.4.7. *Für eine Primzahl $p \in \mathbb{N}$ sind gleichbedeutend:*

1. *p bleibt nicht prim im Ring $\mathbb{Z}[\mathrm{i}]$ der Gauß'schen Zahlen;*
2. *p ist Summe von zwei Quadraten, in Formeln $p = x^2 + y^2$;*
3. *p läßt beim Teilen durch Vier den Rest Eins oder Zwei, in Formeln $p \equiv 1 \pmod 4$ oder $p = 2$;*
4. *Das Polynom $(X^2 + 1)$ ist nicht irreduzibel in $\mathbb{F}_p[X]$;*
5. *(-1) ist ein Quadrat in $\mathbb{F}_p$.*

Beweis. Ist $\pi = x + \mathrm{i}\,y$ ein irreduzibler Faktor echt kleinerer Länge von p, so ist $\pi\bar{\pi} = x^2 + y^2$ ein Primfaktor echt kleinerer Länge von p^2, also $x^2 + y^2 = p$. Das zeigt 1⇒2. Aus $p = x^2 + y^2$ folgt umgekehrt $p = (x + \mathrm{i}\,y)(x - \mathrm{i}\,y)$, also haben wir auch 2⇒1. Die Implikation 2⇒3 folgt daraus, daß jedes Quadrat kongruent ist zu Null oder Eins modulo Vier, da nämlich gilt $\{x^2 \mid x \in \mathbb{Z}/4\mathbb{Z}\} = \{\bar{0}, \bar{1}\}$. 1⇔4 folgert man durch die Betrachtung des Diagramms von Ringen



Alle vier Morphismen sind Quotienten nach geeigneten Hauptidealen. Nach 2.3.27 sind also sowohl 1 als auch 4 gleichbedeutend dazu, daß $\mathbb{F}_p[X]/\langle X^2 + 1\rangle$ kein

Körper ist, und damit sind sie auch untereinander äquivalent. 4⇔5 ist evident. Schließlich zeigen wir noch 3⇒5: Sicher ist nämlich -1 ein Quadrat in $\mathbb{F}_2$, und unter der Vorausetzung $p \equiv 1 \pmod 4$ gilt dasselbe in $\mathbb{F}_p$: Dann gibt es nämlich in $\mathbb{F}_p^\times/\{\pm 1\}$ nach II.7.3.24 ein Element der Ordnung zwei, und jedes Urbild $x \in \mathbb{F}_p^\times$ dieses Elements hat die Ordnung vier und löst folglich die Gleichung $x^2 = -1$ in $\mathbb{F}_p^\times$. □

2.4.8. Formal geht unser kommutatives Diagramm auf den Noether'schen Isomorphiesatz zurück: Sind $I, J \subset R$ Ideale in einem Ring, so liefert dieser Satz Isomorphismen $(R/I)/((I+J)/I) \xrightarrow{\sim} R/(I+J) \xrightarrow{\sim} (R/J)/((I+J)/J)$. Das wenden wir an auf den Ring $R = \mathbb{Z}[X]$ mit seinen Idealen $I = \langle X^2+1\rangle$ und $J = \langle p\rangle[X]$, wo wir das $[X]$ nur dazuschreiben, um zu betonen, daß wir das von p in $\mathbb{Z}[X]$ erzeugte Ideal meinen. Unterwegs verwenden wir dann zusätzlich auch noch den kanonischen Isomorphismus $\mathbb{Z}[X]/\langle p\rangle[X] \xrightarrow{\sim} (\mathbb{Z}/\langle p\rangle)[X]$ nach 2.1.15.

Korollar 2.4.9 (Summen von zwei Quadraten). *Eine positive natürliche Zahl ist Summe von zwei Quadratzahlen genau dann, wenn in ihrer Primfaktorzerlegung alle diejenigen Primfaktoren, die modulo vier kongruent sind zu drei, in geraden Potenzen auftreten.*

Beweis. Genau dann ist $n \in \mathbb{Z}$ Summe von zwei Quadratzahlen, wenn es $a \in \mathbb{Z}[\mathrm{i}]$ gibt mit $n = a\bar{a}$. Ist $n \neq 0$ und $a = \varepsilon\pi_1\pi_2\ldots\pi_r$ eine Darstellung als Produkt einer Einheit ε mit Primelementen, von denen wir $\pi_1, \ldots, \pi_s$ weder reell noch rein imaginär annehmen und $\pi_{s+1}, \ldots, \pi_r$ aus $\mathbb{N}$, so muß

$$n = (\varepsilon\bar{\varepsilon})(\pi_1\bar{\pi}_1)\ldots(\pi_s\bar{\pi}_s)\pi_{s+1}\pi_{s+1}\ldots\pi_r\pi_r$$

die Primfaktorzerlegung in $\mathbb{N}$ sein. Damit folgt das Korollar aus unserer Beschreibung 2.4.4 der Primelemente im Ring der Gauß'schen Zahlen. □

Übung 2.4.10. Man bestimme sämtliche Zerlegungen von 1000000 in eine Summe von zwei Quadratzahlen.

2.5 Primfaktorzerlegung in Polynomringen

Definition 2.5.1. Sei R ein faktorieller Ring. Ein Polynom $\sum_{i=0}^r a_i X^i$ aus dem Polynomring $R[X]$ heißt **primitiv** genau dann, wenn es kein irreduzibles Element von R gibt, das alle seine Koeffizienten teilt. Ein Polynom mit Koeffizienten im Quotientenkörper $P \in (\operatorname{Quot} R)[X]$ nennen wir **primitiv** oder genauer **R-primitiv** genau dann, wenn es bereits in $R[X]$ liegt und dort primitiv ist.

Beispiele 2.5.2. Die Polynome $X^2+2X+10$ und $3X^2+20X+150$ sind primitiv in $\mathbb{Z}[X]$. Das Polynom $10x^2+6X+8$ ist nicht primitiv in $\mathbb{Z}[X]$.

2.5.3. Ich bin etwas unglücklich darüber, daß mit dieser Definition auch alle Einheiten von R primitive Polynome in $R[X]$ sind. An primitive Polynome aber noch zusätzliche Bedingungen zu stellen, schien mir ein größeres Übel.

Lemma 2.5.4 (von Gauss). *Gegeben primitive Polynome mit Koeffizienten in einem faktoriellen Ring ist auch ihr Produkt primitiv.*

Beweis. Sei R unser faktorieller Ring und seien $P, Q \in R[X]$ primitive Polynome. Wäre PQ nicht primitiv, so gäbe es ein irreduzibles Element $p \in R$ mit $\overline{PQ} = \bar{P}\bar{Q} = 0$ in $(R/\langle p\rangle)[X]$. Nach 2.3.6 wären aber $R/\langle p\rangle$ und damit auch $(R/\langle p\rangle)[X]$ Integritätsbereiche, und aus $\bar{P}\bar{Q} = 0$ folgte $\bar{P} = 0$ oder $\bar{Q} = 0$, im Widerspruch zu unserer Annahme P, Q primitiv. □

2.5.5. Gegeben ein faktorieller Ring R mit Quotientenkörper $\operatorname{Quot} R = K$ und ein von Null verschiedenes Polynom $P \in K[X]$ gibt es sicher ein $a \in K^\times$ mit aP primitiv. Es scheint mir auch offensichtlich, daß a wohlbestimmt ist bis auf die Multiplikation mit einer Einheit $u \in R^\times$. Ordnen wir jedem von Null verschiedenen Polynom das Inverse a^{-1} dieses Elements zu, so erhalten wir mithin eine wohlbestimmte Abbildung

$$\operatorname{cont} : K[X]\backslash 0 \;\to\; K^\times/R^\times$$

in besagte Restklassengruppe. Für $P \in \mathbb{Z}[X]\backslash 0$ etwa ist $\operatorname{cont}(P)$ der größte gemeinsame Teiler der Koeffizienten von P oder genauer dessen Bild in $\mathbb{Q}^\times/\mathbb{Z}^\times$. Ich nenne $\operatorname{cont}(P)$ den **Primfaktorgehalt** des Polynoms P, die Notation steht für englisch **content**. Für $P = c \in K^\times$ ist per definitionem $\operatorname{cont}(c) = [c]$ gerade die Nebenklasse von c. Das Urbild des neutralen Elements unter cont besteht per definitionem genau aus den primitiven Polynomen von $K[X]$, und für $P \in K[X]\backslash 0$ ist $\operatorname{cont}(P) \in (R\backslash 0)/R^\times$ gleichbedeutend zu $P \in R[X]$. Das Lemma von Gauss 2.5.4 impliziert, daß cont ein Homomorphismus von Monoiden ist, in Formeln $\operatorname{cont}(1) = 1$ und

$$\operatorname{cont}(PQ) = (\operatorname{cont} P)(\operatorname{cont} Q)$$

Beispiel 2.5.6. Die Einbettung liefert sicher eine Bijektion $\mathbb{Q}_{>0} \xrightarrow{\sim} \mathbb{Q}^\times/\mathbb{Z}^\times$, vermittels derer wir unseren Primfaktorgehalt im Spezialfall $R = \mathbb{Z}$ als Abbildung $\operatorname{cont} : (\mathbb{Q}[X])\backslash 0 \;\to\; \mathbb{Q}_{>0}$ auffassen können. Zum Beispiel hätten wir $\operatorname{cont}(9X^2 + 18X + 90) = 9$ und $\operatorname{cont}((9/5)X^2 + 12X + 90) = 3/5$.

2.5.7. Ist R ein faktorieller Ring mit Quotientenkörper K und sind $P, Q \in R[X]$ primitive Polynome und gibt es $A \in K[X]$ mit $P = AQ$, so folgt bereits $A \in R[X]$ und sogar A primitiv. In der Tat liefert $\operatorname{cont}(P) = (\operatorname{cont} A)(\operatorname{cont} Q)$ dann unmittelbar $\operatorname{cont}(A) = 1$.

Übung 2.5.8. Ist R ein faktorieller Ring mit Quotientenkörper K und sind $P, Q \in K[X]$ normierte Polynome mit $PQ \in R[X]$, so folgt bereits $P, Q \in R[X]$.

Satz 2.5.9 (Polynomringe über faktoriellen Ringen). *Ist R ein faktorieller Ring, so ist auch der Polynomring $R[X]$ ein faktorieller Ring und die irreduziblen Elemente von $R[X]$ sind genau:*

1. *alle irreduziblen Elemente von R;*
2. *alle primitiven Polynome aus $R[X]$, die irreduzibel sind in $(\operatorname{Quot} R)[X]$.*

Beweis. Man sieht leicht, daß die unter 1 und 2 aufgeführten Elemente irreduzibel sind. Wir nennen sie für den Moment kurz die 1&2-Irreduziblen von $R[X]$. Wir vereinbaren für das weitere die Notation $\operatorname{Quot} R = K$. Gegeben $P \in R[X]$ zerlegen wir $P = Q_1 \dots Q_n$ als Produkt von irreduziblen Polynomen in $K[X]$ und schreiben $Q_i = c_i \tilde{Q}_i$ mit $c_i \in K^\times$ und $\tilde{Q}_i$ primitiv. So erhalten wir eine Zerlegung $P = c\tilde{Q}_1 \dots \tilde{Q}_n$ mit $\tilde{Q}_i$ primitiv und irreduzibel in $K[X]$ sowie $c \in K^\times$. Da nun das Produkt $\tilde{Q}_1 \dots \tilde{Q}_n$ primitiv ist nach dem Lemma von Gauss 2.5.4, folgt $c \in R$. Wir können also c faktorisieren in $c = up_1 \dots p_r$ mit $u \in R^\times$, $p_i \in R$ irreduzibel, und folgern so die Existenz einer Zerlegung von P in ein Produkt einer Einheit mit 1&2-Irreduziblen. Das zeigt insbesondere, daß wir unter 1 und 2 in der Tat alle irreduziblen Elemente von R aufgelistet haben. Ist $P = u'p'_1 \dots p'_{r'} S_1 \dots S_{n'}$ eine weitere Zerlegung von P in ein Produkt einer Einheit mit irreduziblen Elementen, sagen wir $u' \in R^\times$, $p'_i \in R$ irreduzibel und $S_j \in R[X]$ primitiv und irreduzibel in $K[X]$, so liefert die Eindeutigkeit der Primfaktorzerlegung in $K[X]$ zunächst $n = n'$ und $S_i = q_i \tilde{Q}_{\sigma(i)}$ für geeignetes $\sigma \in \mathcal{S}_n$ und $q_i \in K^\times$. Dann folgt $q_i \in R^\times$, und schließlich aus der Faktorialität von R die Gleichheit $r = r'$ sowie die Existenz einer Permutation $\tau \in \mathcal{S}_r$ und von Einheiten $u_i \in R^\times$ mit $p'_i = u_i p_{\tau(i)}$. □

2.5.10. Unser Satz enthält insbesondere die Aussage, daß gegeben ein faktorieller Ring R jedes nicht konstante irreduzibles Polynom $P \in R[X]$ auch als Element von $(\operatorname{Quot} R)[X]$ irreduzibel bleibt. Das Argument ist im Beweis versteckt: Wäre $P = Q_1 Q_2$ eine Faktorisierung von P in $(\operatorname{Quot} R)[X]$ in zwei nichtkonstante Polynome, so könnten wir $Q_1 = c_1 \tilde{Q}_1$ und $Q_2 = c_2 \tilde{Q}_2$ schreiben mit $c_1, c_2 \in \operatorname{Quot} R$ und $\tilde{Q}_i$ primitiv, also insbesondere $\tilde{Q}_i \in R[X]$. Aus dem Lemma von Gauß 2.5.4 folgte $\tilde{Q}_1 \tilde{Q}_2$ primitiv und die Identität $P = (c_1 c_2) \tilde{Q}_1 \tilde{Q}_2$ zeigt durch Anwenden von cont sofort $(c_1 c_2) \in R$, im Widerspruch zur Irreduzibilität von P in $R[X]$.

Ergänzung 2.5.11. Die Zerlegung eines Polynoms aus $\mathbb{Z}[X]$ in irreduzible Faktoren kann im Prinzip durch Ausprobieren in endlicher Zeit bestimmt werden. Genauer wissen wir aus II.2.5.9, wie die Beträge der der Koeffizienten eines komplexen Polynoms die Beträge der Wurzeln beschränken und umgekehrt die Beträge der Wurzeln die Beträge der Koeffizienten. Zusammen liefert das eine obere Abschätzung für die Beträge der Koeffizienten der Teiler eines gegebenen Polynoms aus $\mathbb{Z}[X]$.

Korollar 2.5.12. *Für jeden Körper k ist der Polynomring $k[X_1, \ldots, X_n]$ faktoriell. Sogar $\mathbb{Z}[X_1, \ldots, X_n]$ ist ein faktorieller Ring.*

Ergänzende Übung 2.5.13. Seien k ein Körper und $0 < n(1) < n(2) < \ldots < n(r) < n$ natürliche Zahlen, $r \geq 0$. Man zeige, daß das Polynom

$$T^n + a_r T^{n(r)} + \ldots + a_1 T^{n(1)} + a_0$$

irreduzibel ist in $K[T]$, für $K = \operatorname{Quot} k[' a_0, \ldots, a_r]$ der Funktionenkörper. Hinweis: Jede Zerlegung käme nach 2.5.9 notwendig von einer Zerlegung im Polynomring $k[a_0, \ldots, a_r, T]$ her und müßte unter dem Einsetzen $a_1 = \ldots = a_r = 0$ zu einer Zerlegung von $T^n + a_0$ in $k[a_0, T]$ führen.

Korollar 2.5.14. *Ist k ein Körper und sind $f, g \in k[X, Y]$ teilerfremde Polynome, so haben f und g höchstens endlich viele gemeinsame Nullstellen in k^2.*

2.5.15. In 2.8.2 werden wir genauer die "Schranke von Bezout" für die maximal mögliche Zahl gemeinsamer Nullstellen herleiten.

Beweis. Unsere Polynome haben wegen 2.5.9 außer Einheiten erst recht keine gemeinsamen Teiler im Ring $k(X)[Y]$. Da dieser Ring nach 2.3.23 ein Hauptidealring ist, und da jeder Erzeuger des von unseren beiden Polynomen darin erzeugten Ideals ein gemeinsamer Teiler ist, gibt es notwendig $p, q \in k(X)[Y]$ mit $1 = pf + qg$. Nach Multiplikation mit dem Hauptnenner h von p und q erhalten wir eine Identität der Gestalt

$$h = \tilde{p}f + \tilde{q}g$$

mit $0 \neq h \in k[X]$ und $\tilde{p}, \tilde{q} \in k[X, Y]$. Die endlich vielen Nullstellen von h sind dann die einzigen x-Koordinaten, die für gemeinsame Nullstellen von f und g in Frage kommen. Ebenso kommen auch nur endlich viele y-Koordinaten für gemeinsame Nullstellen in Frage, und das Korollar folgt. □

Übung 2.5.16. Sei k ein Körper. Gibt es für ein Polynom P aus dem Polynomring $P \in k[X_1, \ldots, X_n]$ ein Element $Q \in k(X_1, \ldots, X_n)$ aus dem Quotientenkörper mit $Q^2 = P$, so ist Q bereits selbst ein Polynom, in Formeln $Q \in k[X_1, \ldots, X_n]$.

2.6 Kreisteilungspolynome

2.6.1. Besonders interessant wird für uns die Zerlegung der Polynome $X^n - 1$ in irreduzible Faktoren in $\mathbb{Z}[X]$ sein. Die komplexen Nullstellen von $X^n - 1$ heißen die **komplexen n-ten Einheitswurzeln**. Sie bilden in der komplexen Zahlenebene die Ecken eines in den Einheitskreis eingeschriebenen regelmäßigen n-Ecks. In $\mathbb{C}[X]$ gilt natürlich

$$X^n - 1 = \prod_{\zeta^n = 1} (X - \zeta)$$

Die Nullstellenmengen zweier Polynome $f, g \in \mathbb{R}[X, Y]$ ohne gemeinsamen nichtkonstanten Teiler als durchgezogener Kreis und gestrichelter Umriß eines auf dem Rücken liegenden Kamels. Hierfür ist die Papierebene vermittels eines Koordinatensystems mit dem $\mathbb{R}^2$ zu identifizieren. Legen wir etwa den Ursprung ins Zentrum des durgezogenen Kreises, so würden wir $f(X, Y) = X^2 + Y^2 - 1$ und $g(X, Y) = X^4 - 2X^2 + \frac{3}{2} - Y$ in etwa die skizzierten Nullstellenmengen besitzen.

Bilden wir in $\mathbb{C}[X]$ die Polynome

$$\Phi_d(X) = \prod_{\operatorname{ord}\zeta = d} (X - \zeta)$$

so gilt offensichtlich

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

Daraus folgt durch Teilen mit Rest und Induktion erst $\Phi_n(X) \in \mathbb{Q}[X]$ für alle $n \geq 1$ und mit 2.5.7 und erneuter Induktion sogar $\Phi_n(X) \in \mathbb{Z}[X]$ für alle $n \geq 1$. Dies Polynom Φ_n heißt das **n-te Kreisteilungspolynom** oder bei griechisch Gebildeten das **n-te zyklotomische Polynom**. Natürlich gilt $\operatorname{grad}(\Phi_n) = \varphi(n)$, der Grad des n-ten Kreisteilungspolynoms ist also genau der Wert der Euler'schen φ-Funktion an der Stelle n, und das macht auch die Notation plausibel. Wir werden in 4.5.2 zeigen, daß alle Kreisteilungspolynome irreduzibel sind in $\mathbb{Q}[X]$, so daß wir das n-te Kreisteilungspolynom auch und vielleicht eher noch besser charakterisieren können als das eindeutig bestimmte normierte in $\mathbb{Q}[X]$ irreduzible Polynom, das die n-te Einheitswurzel $\exp(2\pi\mathrm{i}/n)$ als Nullstelle hat. Natürlich haben wir für $p > 1$ stets die Zerlegung $X^p - 1 = (X-1)(X^{p-1} + X^{p-2} \ldots + X + 1)$, also ist für p prim der zweite Faktor das p-te Kreisteilungspolynom Φ_p. In diesem Fall können wir die Irreduzibilität mithilfe des gleich folgenden "Eisensteinkriteriums" bereits hier zeigen.

Satz 2.6.2 (Eisensteinkriterium). *Sei $P = a_n X^n + \ldots + a_0 \in \mathbb{Z}[X]$ ein Polynom mit ganzzahligen Koeffizienten und p eine Primzahl. Gilt $p \nmid a_n$, $p|a_{n-1}, \ldots, p|a_0$ und $p^2 \nmid a_0$, so ist P irreduzibel in $\mathbb{Q}[X]$.*

2.6.3. Eine analoge Aussage gilt mit demselben Beweis auch für Polynome mit Koeffizienten in einem beliebigen faktoriellen Ring.

Beweis. Ist P nicht irreduzibel in $\mathbb{Q}[X]$, so besitzt es nach 2.5.9 eine Faktorisierung $P = QR$ in $\mathbb{Z}[X]$ mit Q, R nicht konstant. Wir reduzieren die Koeffizienten modulo p und folgern in $\mathbb{F}_p[X]$ eine Faktorisierung

$$\bar{P} = \bar{Q}\,\bar{R}$$

mit nicht konstanten $\bar{Q}, \bar{R}$. Nach Annahme haben wir aber $\bar{P} = \bar{a}_n X^n$ mit $\bar{a}_n \neq 0$. Es folgt $\bar{Q} = bX^r$ und $\bar{R} = cX^s$ für geeignete $b, c \in \mathbb{F}_p^\times$ und $r, s > 0$. Daraus folgt hinwiederum, daß die konstanten Terme von Q und R durch p teilbar sind, und dann muß der konstante Term von $QR = P$ teilbar sein durch p^2, im Widerspruch zur Annahme. □

Korollar 2.6.4. *Gegeben eine Primzahl p ist das p-te Kreisteilungspolynom $\Phi_p(X) = X^{p-1} + X^{p-2} \ldots + X + 1$ irreduzibel in $\mathbb{Q}[X]$.*

Beweis. Wir haben $X^p - 1 = (X-1)\Phi_p(X)$. Reduzieren wir diese Gleichung modulo p und beachten die Gleichung $X^p - 1 = (X-1)^p$ in $\mathbb{F}_p[X]$, so folgt $\bar{\Phi}_p(X) = (X-1)^{p-1}$ in $\mathbb{F}_p[X]$ und nach der Substitution $X = Y+1$ haben wir $\bar{\Phi}_p(Y+1) = Y^{p-1}$ in $\mathbb{F}_p[Y]$. Jetzt prüfen wir einfach explizit, daß der konstante Term von $\Phi_p(Y+1)$ genau p ist, und haben gewonnen nach dem Eisensteinkriterium 2.6.2. □

Übung 2.6.5. Man zeige für das neunte Kreisteilungspolynom die Formel $\Phi_9(X) = X^6 + X^3 + 1$. Man gebe auch explizite Formeln für alle kleineren Kreisteilungspolynome $\Phi_1, \ldots, \Phi_8$.

Übung 2.6.6. Man zeige, daß das neunte Kreisteilungspolynom $\Phi_9(X) = X^6 + X^3 + 1$ in $\mathbb{Q}[X]$ irreduzibel ist. Hinweis: Man substituiere $X = Y+1$ und wende das Eisensteinkriterium an. Mit einem bereits weiter oben verwendeten Trick kann die Rechnung stark vereinfacht werden.

Ergänzung 2.6.7. Nach ersten Rechnungen mag man vermuten, daß als Koeffizienten von Kreisteilungspolynomen nur 1, 0 und -1 in Frage kommen. Das erste Gegenbeispiel für diese Vermutung liefert das 105-te Kreisteilungspolynom, in dem X^7 mit dem Koeffizienten 2 auftritt. Man kann allgemeiner sogar zeigen, daß jede ganze Zahl als Koeffizient mindestens eines Kreisteilungspolynoms vorkommt [Suz87, SDAT00].

Ergänzende Übung 2.6.8. Man zerlege $(X^n - Y^n)$ in $\mathbb{C}[X,Y]$ in ein Produkt irreduzibler Faktoren.

2.7 Symmetrische Polynome

Definition 2.7.1. Sei k ein Ring. Für jede Permutation $\sigma \in \mathcal{S}_n$ setzen wir die Identität auf k fort zu einem Ringhomomorphismus

$$\begin{array}{rccc} \sigma: & k[X_1,\ldots,X_n] & \to & k[X_1,\ldots,X_n] \\ & X_i & \mapsto & X_{\sigma(i)} \end{array}$$

Ein Polynom $f \in k[X_1,\ldots,X_n]$ heißt **symmetrisch** genau dann, wenn gilt $f = \sigma f \quad \forall \sigma \in \mathcal{S}_n$. Die Menge aller symmetrischen Polynome ist ein Teilring des Polynomrings $k[X_1,\ldots,X_n]$. Wir notieren ihn $k[X_1,\ldots X_n]^{\mathcal{S}_n}$.

2.7.2. Operiert ganz allgemein eine Gruppe G auf einem Ring R durch Ringhomomorphismen, so bilden die G-Invarianten stets einen Teilring R^G, den sogenannten **Invariantenring**.

2.7.3. Operiert eine Gruppe G auf einem Ring R durch Ringhomomorphismen, so operiert unsere Gruppe natürlich auch auf dem Polynomring über R in einer oder sogar in mehreren Veränderlichen. Die Invarianten des Polynomrings fallen dann

mit dem Polynomring über dem Invariantenring zusammen, in Formeln $R[T]^G = R^G[T]$.

Beispiele 2.7.4. Das Produkt $X_1 \ldots X_n$ und die Summe $X_1 + \ldots + X_n$ sind symmetrische Polynome. Allgemeiner definieren wir die **elementarsymmetrischen Polynome** in n Veränderlichen $s_i(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n]^{\mathcal{S}_n}$ durch die Identität

$$(T + X_1)(T + X_2) \ldots (T + X_n) = T^n + s_1 T^{n-1} + s_2 T^{n-2} + \ldots + s_n$$

im Ring $\mathbb{Z}[X_1, \ldots, X_n][T]^{\mathcal{S}_n} = \mathbb{Z}[X_1, \ldots, X_n]^{\mathcal{S}_n}[T]$, so daß wir also haben

$$s_i = \sum_{|I|=i} \left(\prod_{j \in I} X_j \right)$$

wo die Summe über alle i-elementigen Teilmengen $I \subset \{1, \ldots, n\}$ läuft. Speziell ergibt sich $s_1 = X_1 + \ldots + X_n$ und $s_2 = X_1X_2 + X_1X_3 + \ldots + X_1X_n + X_2X_3 + \ldots + X_2X_n + \ldots + X_{n-1}X_n$ und $s_n = X_1 \ldots X_n$.

2.7.5. Gegeben ein kommutativer Ring k sind für beliebige $\zeta_1, \ldots, \zeta_n \in k$ die Koeffizienten des Polynoms $\prod_{i=1}^n (T - \zeta_i) \in k[T]$ per definitionem die elementarsymmetrischen Funktionen in den $(-\zeta_i)$. Grob gesprochen sind also "die Koeffizienten eines Polynoms bis auf Vorzeichen die elementarsymmetrischen Funktionen in seinen Nullstellen".

Ergänzende Übung 2.7.6. Man zeige für symmetrische Polynome im Fall $n \geq k$ die Identität

$$s_{2k}(X_1, \ldots, X_n, -X_1, \ldots, -X_n) = (-1)^k s_k(X_1^2, \ldots, X_n^2)$$

Satz 2.7.7 (über symmetrische Polynome). *Alle symmetrischen Polynome sind polynomiale Ausdrücke in den elementarsymmetrischen Polynomen, und die elementarsymmetrischen Polynome s_i sind algebraisch unabhängig. Für einen beliebigen Ring k haben wir also in Formeln*

$$k[X_1, \ldots, X_n]^{\mathcal{S}_n} = k[' s_1, \ldots, s_n]$$

2.7.8. Das kleine Strichlein an der eröffnenden Klammer ist ein "Freiheitsstrichlein" im Sinne unserer Notation 2.1.13.

Beispiel 2.7.9. Wir haben $X_1^3 + X_2^3 + X_3^3 = s_1^3 - 3s_1s_2 + 3s_3$.

Beispiel 2.7.10. Die Darstellung von $(X_1 - X_2)^2$ durch elementarsymmetrische Polynome ist

$$\begin{aligned} (X_1 - X_2)^2 &= (X_1 + X_2)^2 - 4X_1X_2 \\ &= s_1^2 - 4s_2 \end{aligned}$$

Ein quadratisches Polynom $T^2 - pT + q = (T - \zeta)(T - \xi)$ mit Koeffizienten p, q und Nullstellen ζ, ξ in einem Integritätsbereich k hat also genau dann eine doppelte Nullstelle $\zeta = \xi$, wenn gilt

$$0 = p^2 - 4q$$

Beweis. Da die symmetrischen Polynome einen Ring bilden, folgt aus $s_1, \ldots, s_n \in k[X_1, \ldots, X_n]^{\mathcal{S}_n}$ sofort $k[X_1, \ldots, X_n]^{\mathcal{S}_n} \supset k[s_1, \ldots, s_n]$. Für das weitere verwenden wir die Multiindexnotation wie in **??** und vereinbaren für einen Multiindex $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ die Abkürzung

$$X^\alpha := X_1^{\alpha_1} \ldots X_n^{\alpha_n}$$

Um nun die umgekehrte Inklusion $\subset$ zu zeigen, betrachten wir auf $\mathbb{N}^n$ die **lexikographische Ordnung**, also $(5, 1, 3) \geq (4, 7, 1) \geq (4, 7, 0) \geq (4, 6, 114)$ im Fall $n = 3$. In Formeln ist sie induktiv definiert durch

$$(\alpha_1, \ldots, \alpha_n) \geq (\beta_1, \ldots, \beta_n) \quad \Leftrightarrow \quad \begin{array}{l} \alpha_1 > \beta_1 \\ \text{oder} \\ \alpha_1 = \beta_1 \text{ und } (\alpha_2, \ldots, \alpha_n) \geq (\beta_2, \ldots, \beta_n). \end{array} .$$

Bezüglich dieser Ordnung besitzt jede nichtleere Teilmenge von $\mathbb{N}^n$ ein kleinstes Element. Für ein von Null verschiedenes Polynom $0 \neq f = \sum c_\alpha X^\alpha$ nennen wir das größte $\alpha \in \mathbb{N}^n$ mit $c_\alpha \neq 0$ seinen "Leitindex". Zum Beispiel hat das i-te elementarsymmetrische Polynom s_i den Leitindex $(1, \ldots, 1, 0, \ldots, 0)$ mit i Einsen vorneweg und dann nur noch Nullen. Gälte unsere Inklusion $\subset$ nicht, so könnten wir unter allen symmetrischen Funktionen außerhalb von $k[s_1, \ldots, s_n]$ ein f mit kleinstmöglichem Leitindex α wählen. Wegen $f = \sum c_\alpha X^\alpha$ symmetrisch gilt $c_\alpha = c_\beta$, falls sich die Multiindizes α und β nur in der Reihenfolge unterscheiden. Der Leitindex von f hat folglich die Gestalt

$$\alpha = (\alpha_1, \ldots, \alpha_n) \text{ mit } \alpha_1 \geq \ldots \geq \alpha_n$$

Dann hat das Produkt

$$s_1^{\alpha_1 - \alpha_2} s_2^{\alpha_2 - \alpha_3} \ldots s_{n-1}^{\alpha_{n-1} - \alpha_n} s_n^{\alpha_n} = g$$

denselben Leitindex wie f und den Koeffizienten Eins vor dem entsprechenden Monom. Die Differenz $f - c_\alpha g$ ist folglich entweder Null oder hat zumindest einen echt kleineren Leitindex, gehört also zu $k[s_1, \ldots, s_n]$. Dann gehört aber auch f selbst zu $k[s_1, \ldots, s_n]$ im Widerspruch zu unseren Annahmen. Um die lineare Unabhängigkeit der Monome $s_1^{\gamma_1} \ldots s_n^{\gamma_n}$ in den elementarsymmetrischen Funktionen zu zeigen beachten wir, daß diese Monome paarweise verschiedene Leitindizes haben. Ist nun eine Linearkombination mit Koeffizienten in k unserer Monome null, so notwendig auch der Koeffizient des Monoms mit dem größten Leitindex, und dann induktiv alle Koeffizienten. □

Definition 2.7.11. Gegeben ein Multiindex $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ verwenden wir wie in **??** die Notation

$$|\alpha| = \alpha_1 + \ldots + \alpha_n$$

Ein Polynom in mehreren Veränderlichen heißt **homogen vom Grad** d genau dann, wenn es eine Linearkombination von Monomen X^α ist mit $|\alpha| = d$, in Formeln

$$f = \sum_{|\alpha|=d} c_\alpha X^\alpha$$

Nennt man ein Polynom einfach nur **homogen**, so ist gemeint, daß es einen Grad d gibt derart, daß unser Polynom homogen ist vom Grad d. Das Nullpolynom ist homogen von jedem Grad, aber jedes von Null verschiedene homogene Polynom ist homogen von genau einem Grad. Das Produkt zweier homogener Polynome ist wieder homogen, und ist unser Produkt nicht Null, so ist sein Grad die Summe der Grade der Faktoren.

Beispiel 2.7.12. Das Polynom $X^3Y^3Z + X^2Z^5 - 78X^4YZ^2$ ist homogen vom Grad 7.

Ergänzende Übung 2.7.13. Ist der Koeffizientenring k ein unendlicher Integritätsbereich, so ist ein Polynom $f \in k[X_1, \ldots, X_n]$ homogen vom Grad d genau dann, wenn gilt

$$f(\lambda X_1, \ldots, \lambda X_n) = \lambda^d f(X_1, \ldots, X_n) \qquad \forall \lambda \in k$$

Beispiel 2.7.14. Wir versuchen, $\Delta = (X-Y)^2(Y-Z)^2(Z-X)^2$ durch elementarsymmetrische Funktionen auszudrücken, wo ich statt X_1, X_2, X_3 übersichtlicher X, Y, Z geschrieben habe. Unser Polynom ist homogen vom Grad 6 und das i-te elementarsymmetrische Polynom s_i ist homogen vom Grad i. Wir machen also den Ansatz

$$\Delta = As_1^6 + Bs_1^4s_2 + Cs_1^3s_3 + Ds_1^2s_2^2 + Es_1s_2s_3 + Fs_2^3 + Gs_3^2$$

wobei wir die Summanden nach ihren Leitindizes geordnet haben. Da in Δ keine Monome X^6 oder X^5Y vorkommen, gilt $A = B = 0$. Setzen wir $Z = 0$, so folgt

$$(XY)^2(X^2 - 2XY + Y^2) = D(X+Y)^2(XY)^2 + F(XY)^3$$

und damit $D = 1$ und $F = -4$. Wir kommen so zu einer Darstellung der Form

$$\Delta = Cs_1^3s_3 + s_1^2s_2^2 + Es_1s_2s_3 - 4s_2^3 + Gs_3^2$$

Zählen wir die Monome X^4YZ auf beiden Seiten, so folgt $C = -4$. Setzen wir jetzt für (X, Y, Z) speziell die Werte $(1, 1, -1)$ und $(2, -1, -1)$ ein, so erhalten für (s_1, s_2, s_3) die Werte $(1, -1, -1)$ und $(0, -3, 2)$ und finden

$$4 + 1 + E + G + 4 = 0 = 4G + 4 \cdot 27$$

woraus sofort folgt $G = -27$, $E = 18$ und dann als Endresultat

$$\Delta = s_1^2 s_2^2 - 4s_1^3 s_3 + 18 s_1 s_2 s_3 - 4s_2^3 - 27 s_3^2$$

Ein kubisches Polynom $T^3 + aT^2 + bT + c = (T+\alpha)(T+\beta)(T+\gamma)$ mit Koeffizienten a, b, c und Nullstellen $-\alpha, -\beta, -\gamma$ in einem Integritätsbereich k hat also mehrfache Nullstellen genau dann, wenn gilt

$$0 = a^2 b^2 - 4a^3 c + 18abc - 4b^3 - 27c^2$$

Man nennt das Negative $\Delta_3 := -\Delta$ dieses Ausdrucks in den Koeffizienten die **Diskriminante**, wobei wir das Vorzeichen nur einführen, um keine Unstimmigkeiten mit unserer allgemeinen Definition 2.7.17 aufkommen zu lassen. Hier sind jedoch auch andere Konventionen in Gebrauch.

2.7.15. Die Bezeichnung "Diskriminante" wird verständlich, wenn man mehrfache Nullstellen ansieht als "eigentlich verschiedene" Nullstellen, die nur unglücklicherweise zusammenfallen und deshalb nicht mehr voneinander unterschieden oder lateinisierend "diskriminiert" werden können.

2.7.16. Ist speziell $T^3 + pT + q = (T-\alpha)(T-\beta)(T-\gamma)$ ein Polynom mit Nullstellen α, β, γ ohne quadratischen Term, so ergibt sich für die Diskriminante die Formel

$$-(\alpha-\beta)^2(\beta-\gamma)^2(\gamma-\alpha)^2 = 4p^3 + 27q^2$$

Satz 2.7.17. *Es gibt genau ein Polynom, genannt die n-te* **Diskriminante** $\Delta_n \in \mathbb{Z}[{}'a_1, \ldots, a_n]$, *mit der Eigenschaft, daß beim Einsetzen derjenigen Polynome $a_i \in \mathbb{Z}[{}'\zeta_1, \ldots, \zeta_n]$, die durch die Identität $T^n + a_1 T^{n-1} + \ldots + a_n = (T+\zeta_1)\ldots(T+\zeta_n)$ gegeben werden, im Polynomring $\mathbb{Z}[{}'\zeta_1, \ldots, \zeta_n]$ gilt*

$$\Delta_n(a_1, \ldots, a_n) = \prod_{i \neq j} (\zeta_i - \zeta_j)$$

Beweis. Unser Produkt ist offensichtlich symmetrisch und läßt sich nach 2.7.7 folglich eindeutig schreiben als Polynom in den elementarsymmetrischen Polynomen. □

2.7.18. Für jeden kommutativen Integritätsbereich k und jedes normierte Polynom $T^n + a_1 T^{n-1} + \ldots + a_n$ im Polynomring $k[T]$, das in $k[T]$ vollständig in Linearfaktoren zerfällt, sind für die eben definierte Diskriminante Δ_n nun offensichtlich gleichbedeutend:

1. $\Delta_n(a_1, \ldots, a_n) = 0$;
2. Das Polynom $T^n + a_1 T^{n-1} + \ldots + a_n$ hat mehrfache Nullstellen.

Man nennt das Element $\Delta_n(a_1,\ldots,a_n) \in k$ auch die **Diskriminante des normierten Polynoms** $T^n + a_1T^{n-1} + \ldots + a_n$. Eine explizite Formel für die Diskriminante geben wir in 3.6.21.

Ergänzende Übung 2.7.19. Man zeige, daß die Polynome $P \in \mathbb{Z}[X,Y]$, die bei Vertauschung von X und Y in ihr Negatives übergehen, gerade die Produkte von $(X-Y)$ mit symmetrischen Polynomen sind.

Ergänzende Übung 2.7.20. Sei k ein Körper einer von Zwei verschiedenen Charakteristik. Ein Polynom $f \in k[X_1,\ldots,X_n]$ heißt **antisymmetrisch** genau dann, wenn gilt $\sigma f = \operatorname{sgn}(\sigma) f \quad \forall \sigma \in \mathcal{S}_n$. Man zeige, daß die antisymmetrischen Polynome genau die Produkte von $\prod_{i<j}(X_i - X_j)$ mit symmetrischen Polynomen sind. Hinweis: II.2.5.39. Man zeige dasselbe auch allgemeiner im Fall eines faktoriellen Rings k einer von Zwei verschiedenen Charakteristik.

Übung 2.7.21. Man stelle $X^4 + Y^4 + Z^4 + W^4$ als Polynom in den elementarsymmetrischen Polynomen dar.

Ergänzende Übung 2.7.22. Ist R ein Kring der Charakteristik p, so bilden die Elemente $a \in R$ mit $a^p = a$ einen Teilring.

Ergänzende Übung 2.7.23. Der Ring der symmetrischen Funktionen in n Veränderlichen mit Koeffizienten aus $\mathbb{Q}$ wird auch als Ring erzeugt von $\mathbb{Q}$ und den Potenzsummen $X_1^k + \ldots + X_n^k$ für $1 \le k \le n$.

2.8 Die Schranke von Bezout*

Definition 2.8.1. Sei k ein Körper. Ein Polynom in zwei Veränderlichen $f \in k[X,Y]$ können wir in eindeutiger Weise schreiben in der Gestalt $f = \sum c_{pq} X^p Y^q$ mit $c_{pq} \in k$. Wir definieren den **Grad** oder genauer dem **Totalgrad** von f durch die Vorschrift

$$\operatorname{grad} f = \sup\{p+q \mid c_{pq} \neq 0\}$$

Speziell geben wir im Lichte von **??** dem Nullpolynom den Grad $-\infty$. Analog definieren wir auch den Grad eines Polynoms in beliebig vielen Veränderlichen.

Satz 2.8.2 (Schranke von Bezout). *Sei k ein Körper und seien im Polynomring $k[X,Y]$ zwei von Null verschiedene teilerfremde Polynome f, g gegeben. So haben f und g in der Ebene k^2 höchstens $(\operatorname{grad} f)(\operatorname{grad} g)$ gemeinsame Nullstellen.*

Ergänzung 2.8.3. Ist k algebraisch abgeschlossen und zählt man die gemeinsamen Nullstellen von f und g mit geeignet definierten Vielfachheiten und nimmt auch noch die "Nullstellen im Unendlichen" mit dazu, so haben f und g in diesem verfeinerten Sinne sogar genau $(\operatorname{grad} f)(\operatorname{grad} g)$ gemeinsame Nullstellen. Mehr dazu können Sie in der algebraischen Geometrie lernen.

Zwei verschiedene Ellipsen schneiden sich in höchstens vier Punkten. In der Tat sind sie jeweils Nullstellenmengen von Polynomfunktionen vom Totalgrad Zwei, so daß wir das unmittelbar aus der Schranke von Bezout folgern können.

Beispiel 2.8.4. Ist eines unserer beiden Polynome von der Gestalt $a_nX^n + \ldots + a_1X + a_0 - Y$, so kann man diese Schranke auch elementar einsehen: Man setzt einfach in das andere Polynom $Y = a_nX^n + \ldots + a_1X + a_0$ ein und erhält ein Polynom in X, das eben nur höchstens so viele Nullstellen haben kann, wie sein Grad ist.

Beweis. Sicher reicht es, wenn wir unsere Schranke zeigen für geeignet transformierte Polynome $f \circ \varphi$, $g \circ \varphi$ mit $\varphi \in \mathrm{GL}(2;k)$, d.h. $\varphi : k^2 \xrightarrow{\sim} k^2$ linear. Wir interessieren uns hier insbesondere für die Scherungen $\varphi_\lambda : k^2 \to k^2$, $(x,y) \mapsto (x + \lambda y, y)$ mit $\lambda \in k$. Gegeben $f \in k[X,Y]$ ein Polynom vom Totalgrad $\operatorname{grad} f = n$ enthält $f \circ \varphi_\lambda$ für alle $\lambda \in k$ mit höchstens endlich vielen Ausnahmen einen Term cY^n mit $c \neq 0$. Das ist formal leicht einzusehen und entspricht der anschaulichen Erkenntnis, daß "das Nullstellengebilde von f nur höchstens endlich viele Asymptoten besitzt". Wir wissen nach 2.5.14 schon, daß unsere beiden Polynome höchstens endlich viele gemeinsame Nullstellen haben können. Ist k unendlich, und jeder Körper läßt sich in einen unendlichen Körper einbetten, so finden wir nun $\lambda \in k$ derart, daß unsere transformierten Polynome $f \circ \varphi_\lambda$ bzw. $g \circ \varphi_\lambda$ beide Monome der Gestalt cY^n bzw. dY^m mit $c \neq 0 \neq d$ enthalten, für $n = \operatorname{grad} f$, $m = \operatorname{grad} g$, und daß zusätzlich die gemeinsamen Nullstellen unserer transformierten Polynome paarweise verschiedene x-Koordinaten haben. Anschaulich gesprochen bedeutet das, daß wir die y-Achse so kippen, daß keine unserer Nullstellenmengen "einen in dieser Richtung ins Unendliche gehenden Teil hat" und daß jede Parallele zur y-Achse höchstens eine gemeinsame Nullstelle unserer beiden Polynome trifft. Ohne Beschränkung der Allgemeinheit dürfen wir also annehmen, daß unsere Polynome f und g die Gestalt

$$\begin{aligned} f &= Y^n + a_1(X)Y^{n-1} + \ldots + a_n(X) \\ g &= Y^m + b_1(X)Y^{m-1} + \ldots + b_m(X) \end{aligned}$$

haben mit $a_i, b_j \in k[X]$, $\operatorname{grad} a_i \leq i$, $\operatorname{grad} b_j \leq j$, und daß darüber hinaus die gemeinsamen Nullstellen von f und g paarweise verschiedene x-Koordinaten haben. Die x-Koordinaten gemeinsamer Nullstellen sind aber genau die Nullstellen der im folgenden definierten "Resultante" $R(f,g) \in k[X]$, und in 2.8.8 zeigen wir, daß diese Resultante als Polynom in X höchstens den Grad nm hat. Das beendet dann den Beweis. □

Satz 2.8.5 (über die Resultante). *Gegeben $m, n \geq 0$ gibt es genau ein Polynom mit ganzzahligen Koeffizienten in $n+m$ Veränderlichen, sagen wir $R \in \mathbb{Z}[{}'a_1, \ldots, a_n, b_1, \ldots, b_m]$ derart, daß unter der Substitution der a_i und b_j durch diejenigen Elemente von $\mathbb{Z}[{}'\zeta_1, \ldots, \zeta_n, \xi_1, \ldots, \xi_m]$, die erklärt sind durch die Gleichungen*

$$\begin{aligned} T^n + a_1T^{n-1} + \ldots + a_n &= (T+\zeta_1)\ldots(T+\zeta_n) \\ T^m + b_1T^{m-1} + \ldots + b_m &= (T+\xi_1)\ldots(T+\xi_m) \end{aligned}$$

Das Nullstellengebilde von $f = Y^3 + a_2(X)Y^2 + \ldots + a_0(X)$ als durchgezogenene und von $g = Y^2 + b_1(X)Y + \ldots + b_0(X)$ als gestrichelte Linien. Über jedem Punkt der x-Achse liegen genau drei bzw. zwei Lösungen von f bzw. g.

im Polynomring in den ζ_i und ξ_j gilt

$$R(a_1, \ldots a_n, b_1, \ldots, b_m) = \prod_{i=1,j=1}^{n,m} (\zeta_i - \xi_j)$$

Definition 2.8.6. Gegeben normierte Polynome $f(T) = T^n + a_1T^{n-1} + \ldots + a_n$ und $g(T) = T^m + b_1T^{m-1} + \ldots + b_m$ mit Koeffizienten in einem Kring k benutzen wir die Abkürzung

$$R(a_1, \ldots, a_n, b_1, \ldots, b_m) = R(f, g)$$

und nennen dies Element von k die **Resultante von f und g**. Ist k ein algebraisch abgeschlossener Körper, so verschwindet die Resultante von zwei normierten Polynomen mit Koeffizienten in k per definitionem genau dann, wenn die beiden Polynome eine gemeinsame Nullstelle haben. Im allgemeinen verschwindet die Resultante jedenfalls, wann immer die beiden Polynome eine gemeinsame Nullstelle haben.

Beispiel 2.8.7. Im Fall $m = n = 2$ folgt aus $T^2 + a_1T + a_2 = (T - \zeta_1)(T - \zeta_2)$ und $T^2 + b_1T + b_2 = (T - \xi_1)(T - \xi_2)$ unmittelbar

$$\begin{aligned} a_2 &= \zeta_1\zeta_2, \quad a_1 = \zeta_1 + \zeta_2 \\ b_2 &= \xi_1\xi_2, \quad b_1 = \xi_1 + \xi_2 \end{aligned}$$

und eine kurze Rechnung liefert

$$(\zeta_1 - \xi_1)(\zeta_2 - \xi_2)(\zeta_1 - \xi_2)(\zeta_2 - \xi_1) = (a_2 - b_2)^2 - (a_2 + b_2)a_1b_1 + a_2b_1^2 + b_2a_1^2$$

Der Ausdruck rechts in den Koeffizienten ist also die Resultante der Polynome $f(T) = T^2 + a_1T + a_2$ und $g(T) = T^2 + b_1T + b_2$. Zum Beispiel sehen wir, daß im Fall $a_1 = b_1$ unsere Polynome f und g in einem algebraisch abgeschlossenen Körper genau dann eine gemeinsame Nullstelle haben, wenn gilt $a_2 = b_2$. Das hätten wir natürlich auch so schon gewußt, aber es ist doch ganz beruhigend, unseren Argumenten mal in einem überschaubaren Spezialfall bei der Arbeit zugesehen zu haben.

Beweis. Das Polynom $\prod_{i=1,j=1}^{n,m}(\zeta_i - \xi_j) \in \mathbb{Z}[\zeta_1, \ldots, \zeta_n][\xi_1, \ldots, \xi_m]$ ist symmetrisch in den ξ_j und liegt nach 2.7.7 folglich in

$$\mathbb{Z}[\zeta_1, \ldots, \zeta_n][b_1, \ldots, b_m] = \mathbb{Z}[b_1, \ldots, b_m][\zeta_1, \ldots, \zeta_n]$$

Unser Polynom ist aber auch symmetrisch in den ζ_i, folglich liegt es wieder nach 2.7.7 sogar in $\mathbb{Z}[b_1, \ldots, b_m][a_1, \ldots, a_n]$. □

2.8.8. Wir führen nun noch den Beweis für die Schranke von Bezout zu Ende. Als Polynom in $\mathbb{Z}[\zeta_1, \ldots, \zeta_n, \xi_1, \ldots, \xi_m]$ ist die Resultante ja offensichtlich homogen vom Grad mn. Dahingegen sind die $a_i \in \mathbb{Z}[\zeta_1, \ldots, \zeta_n]$ homogen vom Grad i und die $b_j \in \mathbb{Z}[\xi_1, \ldots, \xi_m]$ homogen vom Grad j. Aus der algebraischen Unabhängigkeit der elementarsymmetrischen Polynome folgt, daß ein Monom $a_1^{\lambda_1} \ldots a_n^{\lambda_n} b_1^{\mu_1} \ldots b_m^{\mu_m}$ nur dann mit von Null verschiedenem Koeffizienten in der Resultante auftauchen kann, wenn gilt

$$\lambda_1 + 2\lambda_2 + \ldots + n\lambda_n + \mu_1 + 2\mu_2 + \ldots + m\mu_m = nm$$

Setzen wir hier insbesondere für a_i gewisse $a_i(X) \in k[X]$ vom Grad $\leq i$ und für b_j gewisse $b_j(X) \in k[X]$ vom Grad $\leq j$ ein, so ist die Resultante ein Polynom in $k[X]$ vom Grad $\leq mn$.

Ergänzung 2.8.9 (**Die Resultante als Determinante**). Sei M die Matrix aus nebenstehendem Bild. Eine explizite Formel für die Resultante ist

$$R(a_1, \ldots, a_n, b_1, \ldots, b_m) = \det M$$

Um das einzusehen, kann man wie folgt argumentieren: Gegeben zwei normierte nicht konstante Polynome $f, g \in k[T]$ mit Koeffizienten in einem Körper k sind ja gleichbedeutend:

(1) Unsere beiden Polynome sind teilerfremd in $k[T]$;

(2) Es gibt Polynome p, q mit $\deg p < \deg g$ und $\deg q < \deg f$, für die gilt $pf + qg = 1$.

In der Tat ist $(2) \Rightarrow (1)$ offensichtlich und $(1) \Rightarrow (2)$ folgt unmittelbar aus dem abstrakten chinesischen Restsatz 2.2.4, wenn wir etwa das Urbild kleinsten Grades von $(0, 1) \in R/\langle f\rangle \times R/\langle g\rangle$ in R aufsuchen. Insbesondere sehen wir so, daß p und q bereits eindeutig bestimmt sind, wenn es sie denn gibt. Nun können wir die Gleichung $pf + qg = 1$ als ein lineares Gleichungssystem für die Koeffizienten von p und q auffassen, und die Matrix dieses Systems ist dann genau die oben gegebene Matrix, wie der Leser leicht selbst einsehen wird. Genau dann ist also unser System eindeutig lösbar, wenn die Determinante der fraglichen Matrix nicht Null ist. Genau dann verschwindet also diese Determinante, wenn f und g nicht teilerfremd sind, und im Fall eines algebraisch abgeschlossenen Körpers k ist das gleichbedeutend dazu, daß f und g eine gemeinsame Nullstelle haben. Speziell erkennen wir so mit II.2.5.39, daß das Polynom $\prod(\zeta_i - \xi_j)$ in $\mathbb{Q}[\zeta_i, \xi_j]$ unsere Determinante teilt, wenn wir sie zu den Polynomen aus 2.8.5 mit Koeffizienten in $\mathbb{Q}[\zeta_i, \xi_j]$ bilden. Wir erkennen sogar genauer, daß unsere Determinante bis auf eine von Null verschiedene Konstante ein Produkt von Faktoren $(\zeta_i - \xi_j)$ ist, wobei

Die Matrix M, deren Determinante die Resultante liefert.

jeder Faktor mindestens einmal vorkommt. Daß hier keine Faktoren mehrfach auftreten und daß die besagte von Null verschiedene Konstante eine Eins ist, können wir unschwer prüfen, indem wir alle ζ_i Null setzen.

Ergänzende Übung 2.8.10. Zwei beliebige homogene Polynome $f(X,Y) = a_0X^n + a_1X^{n-1}Y + \ldots + a_nY^n$ und $g(X,Y) = b_0X^m + b_1X^{m-1}Y + \ldots + b_mY^m$ mit Koeffizienten in einem algebraisch abgeschlossenen Körper k haben genau dann eine gemeinsame Nullstelle außerhalb des Ursprungs, wenn die Determinante derjenigen Variante der nebenstehenden Matrix verschwindet, die entsteht, wenn wir die erste Reihe von Einsen durch a_0 und die zweite Reihe von Einsen durch b_0 ersetzen. Diese Determinante heißt dann auch die **Sylvester-Determinante**.

3 Mehr zu Körpern

3.1 Grundlagen und Definitionen

Beispiele 3.1.1. Ein Körper ist nach II.2.4.28 ein kommutativer von Null verschiedener Ring, in dem jedes Element ungleich Null eine Einheit ist. Aus den Grundvorlesungen bekannt sind die Körper $\mathbb{R}$ und $\mathbb{C}$ der reellen und komplexen Zahlen sowie der Körper $\mathbb{Q}$ der rationalen Zahlen. Allgemeiner haben wir in II.2.8 zu jedem kommutativen Integritätsbereich R seinen Quotientenkörper $\operatorname{Quot} R$ konstruiert, zum Beispiel ist $\operatorname{Quot}\mathbb{Z} = \mathbb{Q}$ unser Körper der rationalen Zahlen und $\operatorname{Quot} K[X] = K(X)$ der Funktionenkörper über einem gegebenen Körper K. Weiter ist nach 2.3.27 der Restklassenring R/pR von einem Hauptidealring nach dem von einem irreduziblen Element $p \in R$ erzeugten Ideal ein Körper, speziell die Restklassenringe $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ für p eine Primzahl in $\mathbb{Z}$ und $K[X]/\langle P\rangle$ für $P \in K[X]$ ein irreduzibles Polynom im Polynomring $K[X]$ über einem Körper K.

Definition 3.1.2. Eine Teilmenge eines Körpers heißt ein **Unterkörper** genau dann, wenn sie so mit der Struktur eines Körpers versehen werden kann, daß die Einbettung ein Körperhomomorphismus ist. Gleichbedeutend ist die Forderung, daß unsere Teilmenge ein Teilring und mit der induzierten Ringstruktur ein Körper ist.

3.1.3. Sicher ist ein beliebiger Schnitt von Unterkörpern eines Körpers wieder ein Unterkörper. Ist K ein Körper und $T \subset K$ eine Teilmenge, so heißt der kleinste Unterkörper von K, der T enthält, der **von** T **erzeugte Unterkörper**. Den kleinsten Unterkörper von K, in anderen Worten den von der leeren Menge $T = \emptyset$ erzeugten Unterkörper, nennt man den **Primkörper von** K.

3.1.4. Für jeden Körper K erinnern wir uns aus II.2.4.37 an die Definition seiner Charakteristik, eines Element $(\operatorname{char} K) \in \mathbb{N}$, durch die Identität

$$\ker(\mathbb{Z} \to K) = \mathbb{Z} \cdot (\operatorname{char} K)$$

Hier meinen wir mit $\mathbb{Z} \to K$ den nach II.2.4.23 eindeutig bestimmten Ringhomomorphismus von $\mathbb{Z}$ nach K.

3.1.5. Die Charakteristik ist also Null, wenn das neutrale Element der multiplikativen Gruppe $K^\times$ als Element der additiven Gruppe $(K,+)$ unendliche Ordnung hat, und ist sonst genau diese Ordnung. Gibt es demnach in noch anderen Worten eine natürliche Zahl $d > 0$ derart, daß in unserem Körper K gilt $1+1+\ldots+1 = 0$ (d Summanden), so ist das kleinstmögliche derartige $d > 0$ die Charakteristik $d = \operatorname{char} K$ von K, und gibt es kein derartiges d, so hat K die Charakteristik Null.

Lemma 3.1.6 (zur Charakteristik). *Die Charakteristik eines Körpers ist entweder Null oder eine Primzahl und es gilt:*

$$\begin{array}{lll} \operatorname{char} K = 0 & \Leftrightarrow & \textit{Der kleinste Unterkörper von } K \textit{ ist isomorph zu } \mathbb{Q}; \\ \operatorname{char} K = p > 0 & \Leftrightarrow & \textit{Der kleinste Unterkörper von } K \textit{ ist isomorph zu } \mathbb{F}_p. \end{array}$$

Beweis. Sei $d = \operatorname{char} K$. Da wir eine Inklusion $\mathbb{Z}/d\mathbb{Z} \hookrightarrow K$ haben, muß $\mathbb{Z}/d\mathbb{Z}$ nullteilerfrei sein, also ist die Charakteristik eines Körpers nach II.2.4.31 entweder null oder eine Primzahl. Im Fall $\operatorname{char} K = p > 0$ prim induziert $\mathbb{Z} \to K$ unter Verwendung der universellen Eigenschaft des Resklassenrings 2.1.7 oder spezieller 2.1.14 einen Isomorphismus von $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ auf einen Unterkörper von K. Im Fall $d = 0$ induziert $\mathbb{Z} \to K$ unter Verwendung der universellen Eigenschaft des Quotientenkörpers II.2.8.4 einen Isomorphismus von $\mathbb{Q} = \operatorname{Quot} \mathbb{Z}$ auf einen Unterkörper von K. Man prüft leicht, daß die Bilder jeweils die kleinsten Unterkörper von K sind. □

3.2 Endliche Körpererweiterungen

Definition 3.2.1. Eine **Körpererweiterung** ist ein Paar $L \supset K$ bestehend aus einem Körper L mit einem Unterkörper K. So ein Paar $L \supset K$ nennt man dann auch genauer eine **Körpererweiterung von** K. Man schreibt statt $L \supset K$ meist L/K und nennt K den **Grundkörper** und L den **Erweiterungskörper** oder **Oberkörper** der Körpererweiterung. Von einer **echten Körpererweiterung** fordern wir zusätzlich, daß der Erweiterungskörper nicht mit dem Grundkörper zusammenfällt.

Beispiele 3.2.2. Ein Grundbeispiel ist die Körpererweiterung $\mathbb{C} \supset \mathbb{R}$. Das Beispiel $\mathbb{C}(X) \supset \mathbb{C}(X^2)$ zeigt, daß es auch bei einer echten Körpererweiterung durchaus vorkommen kann, daß es einen Körperisomorphismus zwischen Grundkörper und Oberkörper gibt. In diesem Beispiel ist mit $\mathbb{C}(X^2)$ der Quotientenkörper des Rings der geraden Polynome $\mathbb{C}[X^2] \subset \mathbb{C}[X]$ gemeint.

3.2.3. In 3.5.7 werden wir unsere Definition abändern und eine Körpererweiterung als Synonym für einen Körperhomomorphismus erklären. Zum jetzigen Zeitpunkt führt dieser Standpunkt jedoch noch nicht zu mehr Klarheit, sondern vielmehr nur zu einer unnötig aufgeblähten Notation, unter der das Verständnis, so fürchte ich, mehr leidet als unter einer späteren Umwidmung des Erweiterungs-Begriffs.

Definition 3.2.4. Gegeben eine Körpererweiterung L/K und Elemente des Erweiterungskörpers $\alpha_1, \ldots, \alpha_n \in L$ bezeichnet man mit $K(\alpha_1, \ldots, \alpha_n) \subset L$ den von K und den α_i erzeugten Unterkörper von L. Er ist im allgemeinen verschieden von dem von K und den α_i erzeugten Teilring $K[\alpha_1, \ldots, \alpha_n] \subset L$.

3.2.5. Das Symbol $K(X)$ kann nun leider auf zweierlei Arten interpretiert werden: Einerseits als der Quotientenkörper des Polynomrings $K[X]$ über K in einer Veränderlichen X, andererseits als der von K und einem weiteren Element X in einem größeren Körper L erzeugte Unterkörper. Wie viele Autoren benutzen wir nach Möglichkeit große Buchstaben vom Ende des Alphabets für die "algebraisch unabhängigen" Variablen in einem Funktionenkörper, d.h. im ersten Fall, und kleine Buchstaben für Elemente einer bereits gegebenen Körpererweiterung, d.h. im zweiten Fall. Wollen wir die Freiheit unserer Veränderlichen besonders betonen, so setzen wir wie in 2.1.13 ein "Freiheitsstrichlein" oben an die vordere Klammer und schreiben $K(\prime X)$ für den Funktionenkörper in einer Variablen X.

Beispiele 3.2.6. Wir haben $\mathbb{R}(\mathrm{i}) = \mathbb{R}[\mathrm{i}] = \mathbb{C}$ und $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$, aber $K[\prime X] \neq K(\prime X)$, der Polynomring ist nämlich verschieden von seinem Quotientenkörper.

Übung 3.2.7. Man zeige $\sqrt{5} \notin \mathbb{Q}(\sqrt{2})$.

Übung 3.2.8. Gegeben $a, b \in \mathbb{Q}^\times$ zeige man, daß $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$ gleichbedeutend dazu ist, daß a/b in $\mathbb{Q}$ ein Quadrat ist.

Ergänzung 3.2.9. Sehr viel allgemeiner kann man für paarweise verschiedene Primzahlen $p, q, \ldots w$ und beliebige $n, m, \ldots, r \geq 2$ zeigen, daß gilt

$$\sqrt[n]{p} \notin \mathbb{Q}(\sqrt[m]{q}, \ldots, \sqrt[r]{w})$$

Das und vieles weitere in dieser Richtung lernt man in der algebraischen Zahlentheorie, die auf dieser Vorlesung aufbaut.

Definition 3.2.10. Sei L/K eine Körpererweiterung und $\alpha \in L$. Gibt es ein vom Nullpolynom verschiedenes Polynom $0 \neq Q \in K[X]$ mit $Q(\alpha) = 0$, so heißt α **algebraisch über** K. Sonst heißt α **transzendent über** K. Unter einer **algebraischen** bzw. **transzendenten Zahl** versteht man eine komplexe Zahl, die algebraisch bzw. transzendent ist über dem Körper der rationalen Zahlen. Ein berühmter Satz von Lindemann besagt, daß die Kreiszahl $\pi \in \mathbb{R}$ transzendent ist über dem Körper $\mathbb{Q}$ der rationalen Zahlen, vergleiche **??**.

3.2.11. Gegeben eine Körpererweiterung L/K und ein Element $\alpha \in L$ betrachten wir die Auswertungsabbildung

$$\begin{array}{ccc} K[X] & \to & L \\ Q & \mapsto & Q(\alpha) \end{array}$$

Ist α transzendent, so ist diese Abbildung injektiv und induziert nach der universellen Eigenschaft des Quotientenkörpers II.2.8.4 einen Isomorphismus $K(X) = \operatorname{Quot} K[X] \xrightarrow{\sim} K(\alpha) \subset L$. Den anderen Fall klärt der folgende Satz.

Satz 3.2.12 (über das Minimalpolynom). *Sei L/K eine Körpererweiterung und sei $\alpha \in L$ algebraisch über K.*

1. *Es gibt in $K[X]$ unter allen normierten Polynomen P mit $P(\alpha) = 0$ genau eines von minimalem Grad, das sogenannte* **Minimalpolynom** $P = \mathrm{Irr}(\alpha, K)$ **von** α **über** K.

2. *Dies Minimalpolynom ist stets irreduzibel in $K[X]$ und jedes Polynom $Q \in K[X]$ mit einer Nullstelle bei α ist ein Vielfaches des Minimalpolynoms von α.*

3. *Das Auswerten bei α liefert einen Isomorphismus*

$$K[X]/\langle \mathrm{Irr}(\alpha, K)\rangle \xrightarrow{\sim} K(\alpha)$$

4. *Ist $d = \mathrm{grad}(\mathrm{Irr}(\alpha, K))$ der Grad des Minimalpolynoms von α über K, so bilden die Potenzen $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$ eine Basis des K-Vektorraums $K(\alpha)$.*

3.2.13. Man beachte, daß das Minimalpolynom von α über K nur in $K[X]$ irreduzibel ist. In $L[X]$ spaltet es zumindest einen Faktor $(X - \alpha)$ ab und ist also reduzibel es sei denn, wir sind im Fall $\alpha \in K$.

3.2.14. Man beachte, daß ein normiertes irreduzibles Polynom aus $K[X]$, daß bei $\alpha \in L$ verschwindet, bereits das Minimalpolynom von α über K sein muß. In der Tat wird ja dies Polynom notwendig vom Minimalpolynom geteilt und ist andererseits bereits selbst irreduzibel. Zum Beispiel sehen wir so, daß das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}$ notwendig $X^3 - 2$ ist, und daß gilt

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \mid a, b, c \in \mathbb{Q}\}$$

Beispiel 3.2.15. Wir betrachten die Körpererweiterung $\mathbb{C}/\mathbb{R}$. Das Element $\mathrm{i} \in \mathbb{C}$ ist algebraisch über $\mathbb{R}$ mit Minimalpolynom $\mathrm{Irr}(\mathrm{i}, \mathbb{R}) = X^2 + 1$. Wir haben $\mathbb{R}(\mathrm{i}) = \mathbb{C}$ und die Abbildung $\mathbb{R}[X] \to \mathbb{C}$ mit $X \mapsto \mathrm{i}$ definiert einen Ringisomorphismus $\mathbb{R}[X]/\langle X^2 + 1\rangle \xrightarrow{\sim} \mathbb{C}$. Die beiden Elemente $1 = \mathrm{i}^0$ und $\mathrm{i} = \mathrm{i}^1$ bilden eine Basis von $\mathbb{C}$ über $\mathbb{R}$.

Übung 3.2.16. Man bestimme das Minimalpolynom der komplexen Zahl $1 + \mathrm{i}$ über $\mathbb{R}$.

Beweis. Da $K[X]$ nach 2.3.23 ein Hauptidealring ist und da das Auswerten $\varphi_\alpha : K[X] \to L$ mit $Q \mapsto Q(\alpha)$ keine Injektion ist, gibt es ein von Null verschiedenes und dann natürlich auch ein normiertes Polynom $P \in K[X]$ mit $\ker(\varphi_\alpha) = \langle P\rangle$. Alle anderen normierten Polynome aus $\langle P\rangle$ haben offensichtlich einen Grad, der echt größer ist als der Grad von P, und das zeigt bereits den ersten Teil des Satzes.

Für unser P haben wir nach 2.1.14 weiter eine Einbettung $K[X]/\langle P\rangle \hookrightarrow L$, folglich ist $K[X]/\langle P\rangle$ ein Integritätsbereich, nach 2.3.27 ist also P irreduzibel und $K[X]/\langle P\rangle$ sogar ein Körper. Dann induziert aber offensichtlich die Einbettung einen Isomorphismus $K[X]/\langle P\rangle \xrightarrow{\sim} K(\alpha)$. Nach 2.1.9 bilden für $d = \operatorname{grad} P$ die Bilder der Potenzen $1, X, X^2, \ldots, X^{d-1}$ eine Basis von $K[X]/\langle P\rangle$ über K, und das zeigt dann schließlich auch die letzte Aussage. □

3.2.17. Ist eine Körpererweiterung erzeugt von einem einzigen Element über dem Grundkörper, so nennt man sie eine **einfache** oder auch eine **primitive Körpererweiterung** des Grundkörpers und das fragliche Element heißt ein **primitives Element** der Körpererweiterung. In dieser Terminologie geben die vorhergehenden Überlegungen einen Überblick über die primitiven Erweiterungen eines gegebenen Körpers: Bis auf den Funktionenkörper sind das genau die Quotienten des Polynomrings nach irreduziblen Polynomen. Dabei können allerdings verschiedene normierte irreduzible Polynome durchaus zu "derselben" primitiven Körpererweiterung führen—und was hier genau mit "derselben" Körpererweiterung gemeint ist, wird im weiteren noch ausführlich diskutiert werden müssen.

Definition 3.2.18. Gegeben eine Körpererweiterung L/K ist L in natürlicher Weise ein K-Vektorraum. Wir setzen

$$[L : K] := \dim_K L \in \mathbb{N} \cup \{\infty\}$$

und nennen diese Zahl den **Grad der Körpererweiterung**. Eine Körpererweiterung von endlichem Grad heißt eine **endliche Körpererweiterung**.

3.2.19. Ist L/K eine Körpererweiterung und $\alpha \in L$ algebraisch über K, so stimmt nach dem letzten Teil des Satzes 3.2.12 über das Minimalpolynom der Grad $[K(\alpha) : K]$ der von α erzeugten Körpererweiterung überein mit dem Grad $\operatorname{grad}(\operatorname{Irr}(\alpha, K))$ des Minimalpolynoms von α über K. Daher rührt wohl auch die Begriffsbildung des "Grades einer Körpererweiterung". Wir vereinbaren für diese Zahl die abkürzende Bezeichnung

$$\operatorname{grad}_K(\alpha) := \operatorname{grad}(\operatorname{Irr}(\alpha, K)) = [K(\alpha) : K]$$

und nennen sie den **Grad von** α **über** K.

Ergänzung 3.2.20. Man kann sich fragen, warum man für die Dimension eines Körpers über einem Unterkörper zusätzlich zu $\dim_K L$ noch eine eigene Notation einführen sollte. Meine Antwort auf diese Frage wäre, daß in der Notation $\dim_K L$ der Körper K unten im Index steht und dadurch weniger wichtig erscheint und schlecht selbst mit Indizes versehen werden kann. Diese Notation ist deshalb nur für das Arbeiten über einem festen Körper K praktisch. Im Zusammenhang der Körpertheorie aber sind alle auftretenden Körper gleichermaßen Hauptdarsteller, und in derartigen Situationen ist eine Notation wie $[L : K]$ geschickter.

Beispiele 3.2.21. Es gilt $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{R} : \mathbb{Q}] = \infty$.

Beispiel 3.2.22. Jede endliche Körpererweiterung L/K eines algebraisch abgeschlossenen Körpers ist trivial, als da heißt, es gilt $L = K$. In der Tat muß das Minimalpolynom jedes Elements von L den Grad Eins haben. Eine andere Formulierung eines sehr ähnlichen Arguments war Übung II.3.5.9.

Proposition 3.2.23. *Sei L/K eine Körpererweiterung. Für $\alpha \in L$ sind gleichbedeutend:*

1. *α ist algebraisch über K;*
2. *$[K(\alpha) : K] < \infty$;*
3. *Es gibt einen Zwischenkörper $K \subset L' \subset L$ mit $[L' : K] < \infty$ und $\alpha \in L'$.*

Beweis. $1 \Rightarrow 2$ folgt unmittelbar aus 3.2.12. Die Implikation $2 \Rightarrow 3$ ist offensichtlich. Aber falls gilt $\dim_K L' < \infty$, können die Potenzen α^ν von α für $\nu = 0, 1, 2, \ldots$ nicht K-linear unabhängig sein, also $3 \Rightarrow 1$. □

Definition 3.2.24. Eine Körpererweiterung vom Grad 2 eine **quadratische Körpererweiterung**.

Proposition 3.2.25 (Quadratische Körpererweiterungen). *Für eine Körpererweiterung L/K mit $\operatorname{char} K \neq 2$ sind gleichbedeutend:*

1. *L/K ist eine quadratische Körpererweiterung, in Formeln $[L : K] = 2$.*
2. *L entsteht aus K durch Adjunktion einer Quadratwurzel, in Formeln $L = K(\alpha)$ für ein $\alpha \in L \backslash K$ mit $\alpha^2 \in K$.*

Beweis. $2 \Rightarrow 1$ ist klar. Für die andere Richtung $1 \Rightarrow 2$ beachte man, daß jedes $\beta \in L \backslash K$ ja notwendig ein Minimalpolynom $P(X) = X^2 + aX + b$ vom Grad zwei hat. Schreiben wir das um zu $P(X) = (X + \frac{a}{2})^2 + (b - \frac{a^2}{4})$, so finden wir $(\beta + \frac{a}{2})^2 = \frac{a^2}{4} - b$ und das gesuchte α ist $\alpha = \beta + \frac{a}{2}$. □

Ergänzung 3.2.26. Wir werden in 3.4.1 sehen, daß auch der Körper $\mathbb{F}_2$ eine Erweiterung vom Grad 2 beitzt. Diese Erweiterung entsteht jedoch sicher nicht durch Adjunktion einer Quadratwurzel, da jedes Element von $\mathbb{F}_2$ seine eigene Quadratwurzel ist.

Satz 3.2.27 (Multiplikativität des Grades). *Für Körper $M \supset L \supset K$ gilt*

$$[M : K] = [M : L][L : K]$$

Beweis. Wir betrachten nur den endlichen Fall. Sei $m_1, \ldots, m_r$ eine Basis von M über L und $l_1, \ldots, l_s$ eine Basis von L über K. Wir behaupten, daß dann die Produkte $l_i m_j$ eine Basis von M über K bilden. Natürlich sind sie ein Erzeugendensystem. Gilt andererseits $\sum_{i,j} k_{ij} l_i m_j = 0$ mit $k_{ij} \in K$, so folgt zunächst $\sum_i k_{ij} l_i = 0$ für alle j aufgrund der linearen Unabhängigkeit der m_j über L und dann $k_{ij} = 0$ für alle i, j aufgrund der linearen Unabhängigkeit der l_i über K. □

Korollar 3.2.28. *Gegeben eine endliche Körpererweiterung ist jedes Element des großen Körpers algebraisch über dem kleinen Körper und sein Grad über dem kleinen Körper teilt den Grad unserer Körpererweiterung.*

Beweis. Sei L/K unsere Körpererweiterung und $\alpha \in L$ unser Element. Die Kette $L \supset K(\alpha) \supset K$ zeigt $[L : K] = [L : K(\alpha)][K(\alpha) : K]$. □

Beispiel 3.2.29. Es gilt $\sqrt{2} \notin \mathbb{Q}(\sqrt[3]{2})$. In der Tat sind nach 2.3.26 die Polynome $X^2 - 2$ und $X^3 - 2$ irreduzibel in $\mathbb{Q}[X]$, nach 3.2.14 sind sie also bereits die Minimalpolynome von $\sqrt{2}$ bzw. $\sqrt[3]{2}$, und folglich hat $\sqrt{2}$ den Grad 2 über $\mathbb{Q}$ und $\sqrt[3]{2}$ den Grad 3.

Übung 3.2.30. Alle Elemente von $\mathbb{Q}(\sqrt{2})$ lassen sich eindeutig in der Form $a + b\sqrt{2}$ schreiben mit $a, b \in \mathbb{Q}$. Man schreibe das Inverse von $7 + \sqrt{2}$ in dieser Form.

Übung 3.2.31. Alle Elemente von $\mathbb{Q}(\sqrt[3]{2})$ lassen sich eindeutig in der Form $a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2$ schreiben mit $a, b, c \in \mathbb{Q}$. Man schreibe das Inverse von $7 + \sqrt[3]{2}$ in dieser Form.

Ergänzende Übung 3.2.32. Sei $K \supset \mathbb{C}$ eine Körpererweiterung von $\mathbb{C}$. Gilt $K \neq \mathbb{C}$, so kann der $\mathbb{C}$-Vektorraum K nicht von einer abzählbaren Teilmenge erzeugt werden, d.h. K hat "überabzählbare Dimension" über $\mathbb{C}$. Hinweis: Abzählbar viele gebrochen rationale Funktionen aus $\mathbb{C}(X)$ können nur abzählbar viele Polstellen haben, und $\mathbb{C}$ ist algebraisch abgeschlossen nach **??**.

Ergänzende Übung 3.2.33. Ist $\sqrt{2} + \sqrt{3}$ algebraisch über $\mathbb{Q}$? Wenn ja, was ist sein Minimalpolynom über $\mathbb{Q}$? Liegt $\sqrt{2}$ in $\mathbb{Q}(\sqrt{2} + \sqrt{3})$?

Ergänzende Übung 3.2.34. Zeigen Sie, daß das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}$ in $\mathbb{Q}(\sqrt[3]{2})$ nicht in Linearfaktoren zerfällt. Zeigen Sie, daß für jede Einheitswurzel ζ das Minimalpolynom von ζ über $\mathbb{Q}$ in $\mathbb{Q}(\zeta)$ in Linearfaktoren zerfällt. Zeigen Sie, daß für ζ eine nichttriviale dritte Einheitswurzel und $K = \mathbb{Q}(\zeta)$ das Minimalpolynom von $\sqrt[3]{2}$ über K in $K(\sqrt[3]{2})$ in Linearfaktoren zerfällt.

Ergänzende Übung 3.2.35. Es seien $P, Q \in K[X]$ irreduzibel mit $\operatorname{grad} P$ und $\operatorname{grad} Q$ teilerfremd. Sei $L = K(\alpha)$ eine Körpererweiterung von K, wobei $\alpha \in L$ eine Nullstelle von P ist. Dann ist Q auch irreduzibel in $L[X]$.

Übung 3.2.36. Seien $R \supset K$ ein Kring mit einem Teilring, der sogar ein Körper ist. Genau ist $\alpha \in R$ Nullstelle eines von Null verschiedenen Polynoms $P \in K[X]$, wenn $K[\alpha]$ endlichdimensional ist als K-Vektorraum.

3.3 Konstruktionen mit Zirkel und Lineal

Definition 3.3.1. Sei $E \subset \mathbb{C}$ eine Teilmenge der komplexen Zahlenebene.

1. Eine (reelle) Gerade durch zwei verschiedene Punkte von E heißt eine "aus E elementar konstruierbare Gerade".

2. Ein Kreis durch einen Punkt von E mit Mittelpunkt in einem anderen Punkt von E heißt ein "aus E elementar konstruierbarer Kreis".

3. Alle aus E elementar konstruierbaren Geraden und Kreise fassen wir zusammen unter dem Oberbegriff der "aus E elementar konstruierbaren Figuren".

4. Ein Punkt $z \in \mathbb{C}$ heißt **elementar konstruierbar aus** E genau dann, wenn er im Schnitt von zwei verschiedenen aus E elementar konstruierbaren Figuren liegt.

Satz 3.3.2 (Konstruierbarkeit und quadratische Erweiterungen). *Die folgenden beiden Teilmengen K und Q von $\mathbb{C}$ stimmen überein:*

1. *Die kleinste Teilmenge $K \subset \mathbb{C}$, die 0 und 1 enthält und stabil ist unter elementaren Konstruktionen;*

2. *Der kleinste Teilkörper $Q \subset \mathbb{C}$, der stabil ist unter dem Bilden von Quadratwurzeln.*

Definition 3.3.3. Wir nennen die Elemente von K die **konstruierbaren Zahlen**.

Beweis. Wir beginnen mit der Inklusion $Q \subset K$. Offensichtlich ist K stabil unter Addition. Um die Stabilität unter Multiplikation und Inversenbildung zu zeigen beachten wir, daß für $a \in \mathbb{C}^\times$ offensichtlich gleichbedeutend sind:

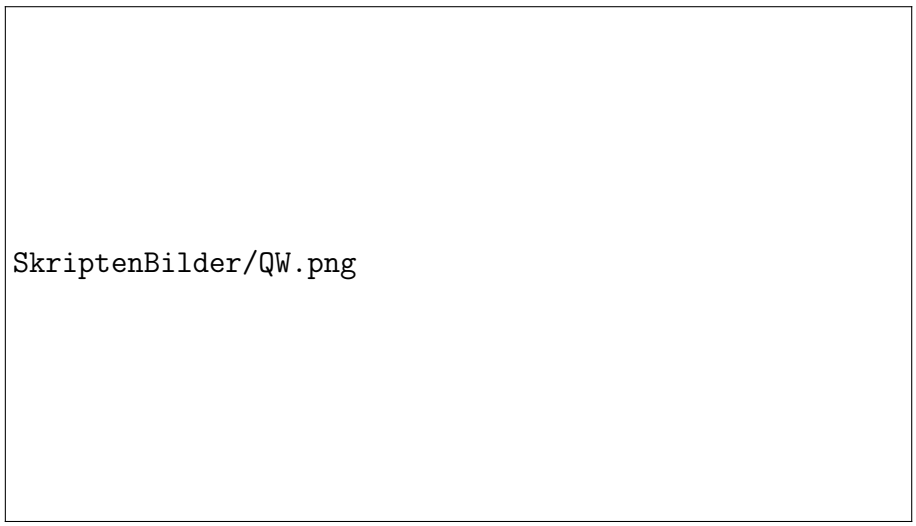
1. a liegt in K;

2. $|a|$ und $\frac{a}{|a|}$ liegen in K;

3. $\mathrm{Re}(a)$ und $\mathrm{Im}(a)$ liegen in K.

Nun ist es unproblematisch, Punkte auf dem Einheitskreis mithilfe von Zirkel und Linal zu invertieren und zu multiplizieren. Daß das auch für reelle Zahlen möglich ist, zeigen die nebenstehenden Abbildungen. Also ist K ein Teilkörper von $\mathbb{C}$. Er ist aber auch stabil unter dem Bild von Quadratwurzeln: In der Tat ist klar, wie wir die Wurzeln von Punkten auf dem Einheitskreis mit Zirkel und Lineal bestimmen können, und daß das Wurzelziehen mit Zirkel und Lineal aus einer

Die Konstruktion von Produkten und Inversen



Die Konstruktion der Wurzel

positiven reellen Zahl möglich ist, zeigt das nebenstehende Bild, in dem ja gilt $(h^2+a^2)+(h^2+1^2)=(a+1)^2$, also $h^2=a$. Also ist $K\subset\mathbb{C}$ ein Teilkörper, der stabil ist unter dem Bilden von Quadratwurzeln, und wir erhalten $Q\subset K$. Wir zeigen nun umgekehrt $K\subset Q$. Sicher ist Q stabil unter der komplexen Konjugation, denn mit Q ist auch $Q\cap\bar{Q}$ ein unter dem Bilden von Quadratwurzeln stabiler Unterkörper von $\mathbb{C}$. Eine komplexe Zahl z gehört folglich zu Q genau dann, wenn ihr Real- und Imaginärteil zu Q gehören. Mit $z=x+\mathrm{i}\,y$ werden unsere aus Q elementar konstruierbaren Figuren nun aber beschrieben durch Gleichungen der Gestalt

$$\begin{aligned}(x-a)^2+(y-b)^2 &= c\\ ax+by &= c\end{aligned}$$

für geeignete $a,b,c\in Q\cap\mathbb{R}$, und simultane Lösungen zweier verschiedener derartiger Gleichungen sind in der Tat Lösungen von linearen oder quadratischen Gleichungen mit Koeffizienten aus Q, ja sogar aus $Q\cap\mathbb{R}$: Im kompliziertesten Fall des Schnitts zweier Kreise bildet man zunächst die Differenz beider Gleichungen und erhält so eine lineare Gleichung in x und y, die man anschließend nach einer Variable auflöst und in eine der Kreisgleichungen einsetzt. Das zeigt, daß $Q\subset\mathbb{C}$ stabil ist unter elementaren Konstruktionen. Da auch 0 und 1 zu Q gehören, folgt $K\subset Q$. □

Korollar 3.3.4. *Jede konstruierbare Zahl ist algebraisch und ihr Grad über $\mathbb{Q}$ ist eine Zweierpotenz.*

Beweis. Es scheint mir offensichtlich, daß Q auch beschrieben werden kann als die Vereinigung aller Teilkörper von $\mathbb{C}$ der Gestalt $\mathbb{Q}(\alpha_1,\alpha_2,\ldots,\alpha_r)$ für Familien $\alpha_1,\alpha_2,\ldots,\alpha_r$ komplexer Zahlen mit der Eigenschaft $\alpha_i^2\in\mathbb{Q}(\alpha_1,\alpha_2,\ldots,\alpha_{i-1})$ für alle i. In der Tat ist die Vereinigung aller derartigen Teilkörper ist offensichtlich selbst ein Teilkörper und sicher der Kleinste unter dem Ziehen von Quadratwurzeln stabile. Sei nun z unsere konstruierbare Zahl. Nach dem Satz gibt es eine Kette von Körpererweiterungen

$$\mathbb{Q}=K_0\subset K_1\subset\ldots\subset K_r$$

mit $[K_i:K_{i-1}]=2$ und $z\in K_r$. Es folgt $[K_r:\mathbb{Q}]=2^r$ und der Grad von z ist nach 3.2.28 ein Teiler von $[K_r:\mathbb{Q}]$. □

Korollar 3.3.5.

1. *Das regelmäßige Siebeneck ist nicht konstruierbar mit Zirkel und Lineal.*
2. *Die Seitenlänge eines Würfels mit Volumen Zwei ist nicht konstruierbar mit Zirkel und Lineal.*
3. *Es gibt keine Konstruktion mit Zirkel und Lineal, die es erlaubt, einen beliebig vorgegebenen Winkel zu dritteln.*

Ergänzung 3.3.6. Wir werden in 4.5.5 allgemeiner zeigen, daß sich für $n \geq 3$ das regelmäßige n-Eck mit Zirkel und Lineal konstruieren läßt genau dann, wenn die Anzahl $\varphi(n) = |\{a \mid 1 \leq a \leq n,\ \langle a, n\rangle = 1\}|$ der zu n teilerfremden Zahlen unter n eine Zweierpotenz ist. Zum Beispiel ist das regelmäßige Dreieck konstruierbar aber nicht das regelmäßige Neuneck, als da heißt, der Winkel $2\pi/3$ kann nicht gedrittelt werden mit Zirkel und Lineal. Hier geben wir für diese beiden Aussagen schon mal direkte Argumente.

Ergänzung 3.3.7. Die Griechen scheinen in der hellenistischen Hochkultur Konstruktionen mit Zirkel und Lineal auf Papyrus in derselben Weise eingesetzt zu haben, wie bei uns bis etwa 1960 Rechenschieber, dann Taschenrechner, und mittlerweile Laptops eingesetzt wurden und werden: Als unverzichtbare Hilfsmittel des Ingenieurs. Das Ziehen von Kubikwurzeln etwa war wichtig, um gemäß der Formel eines gewissen Philon die Dicke des Spannseils einer Wurfmaschine so zu berechnen, daß sie ein vorgegebenes Gewicht über eine vorgegebene Entfernung schleuderte. Mehr dazu findet man in [Rus05] in Abschnitt 2.3 und zu Ende des Abschnitts 4.3.

Ergänzung 3.3.8. Die Frage der **Würfelverdopplung**, also die Frage, mit Zirkel und Lineal aus einer gegebenen Strecke eine weitere Strecke zu konstruieren derart, daß das Längenverhältnis der beiden Strecken gerade $\sqrt[3]{2}$ ist, heißt das **Deli'sche Problem**. Diese Bezeichnung geht auf eine Geschichte zurück, nach der das Orakel in Delphi den Deliern aufgab, zur Abwehr einer Pest den würfelförmigen Altar ihres Tempels zu verdoppeln.

Beweis. 1. Nach 2.6.4 und 3.2.14 hat $\exp(2\pi\,\mathrm{i}\,/7)$ den Grad 6 über $\mathbb{Q}$ und ist nach 3.3.4 also nicht konstruierbar.

2. Nach 3.2.14 hat die gesuchte Länge $\sqrt[3]{2}$ den Grad 3 über $\mathbb{Q}$ und ist nach 3.3.4 also nicht konstruierbar.

3. Sicher gilt $\exp(2\pi\,\mathrm{i}\,/3) \in K$. Es reicht, $\exp(2\pi\,\mathrm{i}\,/9) \notin K$ zu zeigen. Sicher ist $\exp(2\pi\,\mathrm{i}\,/9) = \zeta$ eine Nullstelle des Polynoms $X^9 - 1$. Natürlich zerfällt dieses Polynom in

$$X^9 - 1 = (X^3 - 1)(X^6 + X^3 + 1)$$

und ζ ist Nullstelle des zweiten Faktors, unseres neunten Kreisteilungspolynom aus 2.6.5. Es reicht zu zeigen, daß dieses Polynom irreduzibel ist über $\mathbb{Q}$, denn dann hat ζ den Grad 6 über $\mathbb{Q}$ und kann nach 3.3.4 nicht konstruierbar sein. In 4.5.2 werden wir zeigen, daß alle Kreisteilungspolynome irreduzibel sind. Hier basteln wir nur ein schnelles Argument für unseren speziellen Fall zusammen, vergleiche auch 2.6.6. In $\mathbb{F}_3[X]$ gilt sicher $(X^9 - 1) = (X - 1)^9$ und $(X^3 - 1) = (X-1)^3$ und folglich $X^6+X^3+1 = (X-1)^6$. Substituieren wir in X^6+X^3+1 nun $X = Y+1$, so erhalten wir in $\mathbb{F}_3[Y]$ also das Polynom Y^6. Gehen wir wieder über

zu $\mathbb{Q}[Y]$, so hat $(Y+1)^6+(Y+1)^3+1$ den konstanten Term 3. Damit können wir aus dem Eisenstein-Kriterium 2.6.2 folgern, daß unser Polynom irreduzibel ist. □

Satz 3.3.9 (Konstruierbarkeit, Variante). *Gegeben eine Teilmenge $A \subset \mathbb{C}$ stimmen die folgenden beiden Teilmengen K_A und Q_A von $\mathbb{C}$ überein:*

1. *Die kleinste Teilmenge $K_A \subset \mathbb{C}$, die 0 und 1 enthält und A umfaßt und stabil ist unter elementaren Konstruktionen;*
2. *Der kleinste Teilkörper $Q_A \subset \mathbb{C}$, der A und $\bar{A}$ umfaßt und stabil ist unter dem Bilden von Quadratwurzeln.*

Ergänzung 3.3.10. Wir nennen die Elemente der Menge K_A **aus** A **konstruierbare Zahlen**. Der Beweis unserer Variante ist vollständig analog zum Beweis von 3.3.2 und bleibe dem Leser überlassen. Man erkennt daraus, daß ein Winkel genau dann mit Zirkel und Lineal gedrittelt werden kann, wenn für den zugehörigen Punkt a auf dem Einheitskreis das Polynom X^3-a über $\mathbb{Q}(a)$ nicht irreduzibel ist alias eine Nullstelle hat. Zum Beispiel lassen sich $360°$ und $180°$ mit Zirkel und Lineal dritteln, denn X^3-1 und X^3+1 haben rationale Nullstellen. Ebenso läßt sich $135°$ mit Zirkel und Lineal dritteln, denn für die primitive achte Einheitswurzel $a=(\mathrm{i}-1)/\sqrt{2}$ ist a^3 ein Nullstelle von X^3-a.

3.4 Endliche Körper

Satz 3.4.1 (Klassifikation endlicher Körper). *Die Kardinalität eines endlichen Körpers ist stets eine Primzahlpotenz, und zu jeder Primzahlpotenz gibt es umgekehrt bis auf Isomorphismus genau einen endlichen Körper mit dieser Kardinalität.*

3.4.2. Gegeben eine Primzahlpotenz q notiert man "den" Körper mit q Elementen meist $\mathbb{F}_q$. Ich weiß nicht, ob $\mathbb{F}$ in diesem Zusammenhang für "finite" oder für "field", die englische Bezeichnung für Körper, steht.

3.4.3. Man kann zeigen, daß jeder endliche Schiefkörper schon ein Körper ist, siehe zum Beispiel [Wei74], I, §1.

Beispiel 3.4.4. In $\mathbb{F}_5$ sind 0 und ± 1 die einzigen Quadrate. Wir erhalten also einen Körper mit 25 Elementen, indem wir zu $\mathbb{F}_5$ eine Wurzel aus 2 adjungieren, und können alle Elemente dieses Körpers dann eindeutig schreiben in der Form $a+b\sqrt{2}$ mit $a,b\in\mathbb{F}_5$.

Übung 3.4.5. Wenn wir unseren Satz glauben, muß ein Körperisomorphismus $\mathbb{F}_5(\sqrt{2}) \xrightarrow{\sim} \mathbb{F}_5(\sqrt{3})$ existieren. Geben Sie einen derartigen Körperisomorphismus explizit an.

Beweis. Ein endlicher Körper $\mathbb{F}$ hat sicher positive Charakteristik $p = \operatorname{char}\mathbb{F} > 0$. Nach 3.1.6 ist p eine Primzahl und wir haben eine Einbettung $\mathbb{F}_p \hookrightarrow \mathbb{F}$. Damit wird $\mathbb{F}$ ein endlichdimensionaler $\mathbb{F}_p$-Vektorraum. Für $r = \dim_{\mathbb{F}_p}\mathbb{F} = [\mathbb{F} : \mathbb{F}_p]$ gilt dann offensichtich $|\mathbb{F}| = p^r$. Das zeigt, daß die Kardinalität eines endlichen Körpers stets eine Primzahlpotenz ist. Unser Satz behauptet nun darüber hinaus, daß die Kardinalität eine Bijektion

$$\{\text{endliche Körper, bis auf Isomorphismus}\} \quad \tilde{\to} \quad \{\text{Primzahlpotenzen}\}$$

liefert. Wir unterbrechen nun den Beweis durch einen Satz und zwei Lemmata, um die nötigen Hilfsmittel bereitzustellen. □

Satz 3.4.6 (Zerfällung von Polynomen in Körpererweiterungen). *Gegeben ein Körper K und ein von Null verschiedenes Polynom $P \in K[X]$ gibt es eine endliche Körpererweiterung L von K derart, daß P als Element von $L[X]$ vollständig in Linearfaktoren zerfällt.*

Beweis. Das folgt mit Induktion aus dem anschließenden Lemma, wenn wir beachten, daß nach II.2.4.29 jeder Körperhomomorphismus injektiv ist. □

3.4.7. Natürlich folgt dieser Satz auch unmittelbar aus der Existenz eines algebraischen Abschlusses 3.7.6. Diese Argumentation ist jedoch zumindest im Rahmen der hier gegebenen Darstellung unzulässig, da unser Satz selbst einen wesentlichen Baustein beim Beweis der Existenz algebraischer Abschlüsse darstellt, und zumindest um das folgende Lemma kommt meines Wissens kein Beweis der Existenz algebraischer Abschlüsse herum.

Lemma 3.4.8 (Adjunktion von Nullstellen). *Sei K ein Körper und $P \in K[X]\backslash K$ ein nichtkonstantes Polynom. So gibt es einen Körperhomomorphismus $i : K \to L$ derart, daß das Bild $\hat{\imath}(P)$ von P unter der von i auf den Polynomringen induzierten Abbildung $\hat{\imath} : K[X] \to L[X]$ eine Nullstelle in L hat.*

3.4.9. Die Adjunktion von Quadratwurzeln haben Sie möglicherweise bereits sozusagen zu Fuß als Übung I.3.3.14 ausgearbeitet, um die komplexen Zahlen aus den reellen Zahlen zu gewinnen. Das Verfahren aus dem Beweis unseres Lemmas wird in manchen Quellen als die **Kronecker-Konstruktion** bezeichnet. Es ist eine gute Übung, im Fall der Adjunktion einer Quadratwurzel einen expliziten Isomorphismus zwischen der hier und der in I.3.3.14 konstruierten Körpererweiterung anzugeben.

Beweis. Sei ohne Beschränkung der Allgemeinheit P irreduzibel in $K[X]$. Dann ist $L = K[X]/\langle P\rangle$ nach 2.3.27 ein Körper. Wir notieren $\bar{Q} \in L$ die Nebenklasse von $Q \in K[X]$, betrachten den offensichtlichen Körperhomomorphismus

$$i : K \to L = K[X]/\langle P\rangle$$

mit $i(a) = \bar{a}$ und behaupten, daß die Nebenklasse $\bar{X} \in L$ von $X \in K[X]$ eine Nullstelle des Polynoms $\hat{\imath}(P) \in L[X]$ ist. In der Tat finden wir für unser Polynom $P = a_nX^n + \ldots + a_1X + a_0$ mit Koeffizienten $a_\nu \in K$ sofort $\hat{\imath}(P) = \bar{a}_nX^n + \ldots + \bar{a}_1X + \bar{a}_0$ und dann

$$(\hat{\imath}(P))(\bar{X}) = \bar{a}_n\bar{X}^n + \ldots + \bar{a}_1\bar{X} + \bar{a}_0 = \overline{a_nX^n + \ldots + a_1X + a_0} = \bar{P} = 0\square$$

Lemma 3.4.10. *Sei p eine Primzahl, $q = p^r$ mit $r \geq 1$ eine echte Potenz von p und L ein Körper der Charakteristik p. Zerfällt das Polynom $X^q - X$ über dem Körper L vollständig in Linearfaktoren, so bilden die Nullstellen unseres Polynoms in L einen Unterkörper der Kardinalität q.*

Beweis. Nach II.2.4.39 ist die Abbildung $F : L \to L$, $a \mapsto a^q$ ein Körperhomomorphismus. Die Nullstellen unseres Polynoms sind nun genau die Fixpunkte dieses Körperhomomorphismus, folglich bilden sie einen Unterkörper $\mathbb{F}$ von L. Um zu zeigen, daß dieser Unterkörper $\mathbb{F}$ genau q Elemente hat, müssen wir nachweisen, daß das Polynom $X^q - X$ nur einfache Nullstellen hat. Offensichtlich ist $X = 0$ eine einfache Nullstelle unseres Polynoms, und ist a irgendeine andere Nullstelle, so gilt im Polynomring $\mathbb{F}_p[X]$ die Gleichheit $X^q - X = (X - a)^q - (X - a)$. Also ist jede Nullstelle unseres Polynoms einfach. □

Beweis von 3.4.1, Fortsetzung. Jetzt können wir zeigen, daß es zu jeder echten Potenz q einer Primzahl p auch tatsächlich einen Körper mit genau q Elementen gibt. Wir finden ja nach 3.4.6 eine Körpererweiterung L von $\mathbb{F}_p$, in der das Polynom $X^q - X \in \mathbb{F}_p[X]$ vollständig in Linearfaktoren zerfällt, und nach 3.4.10 bilden die Nullstellen dieses Polynoms in L dann einen Unterkörper der Kardinalität q. Schließlich müssen wir, um unsere Klassifikation der endlichen Körper abzuschließen, noch zeigen, daß je zwei endliche Körper derselben Kardinalität isomorph sind. Ist $\mathbb{F}$ ein endlicher Körper mit $q = p^r$ Elementen, so gilt $a^{q-1} = 1$ für alle $a \in \mathbb{F}^\times$ nach II.7.3.7, also haben wir $a^q - a = 0$ für alle $a \in \mathbb{F}$. Insbesondere sind die Minimalpolynome der Elemente von $\mathbb{F}$ über $\mathbb{F}_p$ genau die $\mathbb{F}_p$-irreduziblen Faktoren des Polynoms $X^q - X \in \mathbb{F}_p[X]$. Die Erzeuger der Körpererweiterung $\mathbb{F}$ sind damit genau die Nullstellen der $\mathbb{F}_p$-irreduziblen Faktoren P vom Grad r unseres Polynoms $X^q - X$. Nach II.7.3.28 gibt es solche Erzeuger und damit auch solche Faktoren und mit 3.2.12 folgt

$$\mathbb{F} \cong \mathbb{F}_p[X]/\langle P\rangle$$

für einen und jeden $\mathbb{F}_p$-irreduziblen Faktor P vom Grad r. Das zeigt, daß ein endlicher Körper durch die Zahl seiner Elemente bis auf Isomorphismus eindeutig bestimmt ist. Das Argument zeigt nebenbei bemerkt auch, wie man in endlichen Körpern explizit rechnen kann. □

3.4.11. Teile dieses Beweises lassen sich mithilfe der allgemeinen Theorie, sobald wir sie einmal entwickelt haben, auch schneller erledigen: Die Eindeutigkeit erhält man aus dem Satz 3.5.2 über die Eindeutigkeit von Zerfällungskörpern. Die Existenz folgt wie oben daraus, daß $X^q - X$ keine mehrfachen Nullstellen hat, aber das kann man nach 3.6.9 auch daraus folgern, daß die Ableitung dieses Polynoms keine Nullstellen hat.

Ergänzende Übung 3.4.12. Geben Sie Verknüpfungstafeln für die Addition und die Multiplikation eines Körpers mit vier Elementen an.

Satz 3.4.13 (Endliche Erweiterungen endlicher Körper). *Gegeben zwei endliche Körper läßt sich der eine in den anderen einbetten genau dann, wenn die Kardinalität des einen eine Potenz der Kardinalität des anderen ist.*

3.4.14. Mit den Methoden der Galois-Theorie werden wir dies Resultat in 4.4.3 sehr viel müheloser einsehen können als im folgenden Beweis.

Beweis. Seien F und L unsere endlichen Körper. Läßt sich F in L einbetten, so wählen wir eine derartige Einbettung, betrachten die Dimension $d = [L : F]$ des F-Vektorraums L und haben $|L| = |F|^d$. Für die Umkehrung betrachten wir die Identität

$$(Y-1)(Y^{c-1} + Y^{c-2} + \ldots + 1) = Y^c - 1$$

Aus dieser Identität folgt

$q-1$	teilt	q^r-1	für beliebige natürliche Zahlen q und r,
X^a-1	teilt	$X^{ca}-1$	für beliebiges a,
$X^{q-1}-1$	teilt	$X^{q^r-1}-1$	nach den beiden vorhergehenden Punkten,
X^q-X	teilt	$X^{q^r}-X$	nach Multiplikation mit X.

Ist nun q eine Primzahlpotenz und $r \geq 1$ eine natürliche Zahl, so zerfällt also das Polynom $X^q - X$ über $\mathbb{F}_{q^r}$ in Linearfaktoren und nach 3.4.10 bilden dann seine Nullstellen einen Unterkörper von $\mathbb{F}_{q^r}$ mit q Elementen. □

Übung 3.4.15. In einem Körper gibt es zu jeder natürlichen Zahl höchstens einen Unterkörper mit dieser Zahl von Elementen.

Übung 3.4.16. Ein endlicher Körper kann nie algebraisch abgeschlossen sein.

Ergänzende Übung 3.4.17. Ist k ein Körper, so wird eine k-Basis des Funktionenkörpers $k(X)$ gebildet von erstens den $(X^n)_{n\geq 1}$ mitsamt zweitens den

$$(X^d P^{-n})_{n\geq 1,\ \operatorname{grad} P > d \geq 0}$$

für $P \in k[X]$ normiert und irreduzibel zuzüglich drittens der 1 aus $k(X)$. Für den Fall k algebraisch abgeschlossen vergleiche man II.2.8.11. Sonst ziehe man sich für den Beweis der linearen Unabhängigkeit mit 3.4.6 auf den Fall von in Linearfaktoren zerfallenden Nennern zurück.

Ergänzende Übung 3.4.18. Man bestimme die Partialbruchzerlegung, also die Darstellung in der Basis aus 3.4.17, von $(1+x^4)^{-1}$ in $\mathbb{Q}(X)$.

3.5 Zerfällungskörper

Definition 3.5.1. Sei K ein Körper und $P \in K[X]$ ein Polynom. Unter einem **minimalen Zerfällungskörper** oder kurz **Zerfällungskörper** von P verstehen wir eine Körpererweiterung L/K derart, daß (1) das Polynom P in $L[X]$ vollständig in Linearfaktoren zerfällt und daß (2) der Körper L über K erzeugt wird von den Nullstellen von P.

Satz 3.5.2 (Eindeutigkeit von Zerfällungskörpern). *Sei K ein Körper und $P \in K[X]$ ein Polynom. Sind L/K und L'/K zwei Zerfällungskörper von P, so gibt es einen Isomorphismus $L \xrightarrow{\sim} L'$, der auf K die Identität induziert.*

3.5.3. Wir zeigen das erst nach den Beweis von 3.5.12.

3.5.4. Da ein Zerfällungskörper für ein Polynom damit in gewisser Weise eindeutig ist, spricht man auch oft von *dem* Zerfällungskörper eines Polynoms. Das ist jedoch auch wieder etwas irreführend: Im allgemeinen gibt es nämlich zwischen zwei Zerfällungskörpern L, L' desselben Polynoms durchaus verschiedene Isomorphismen $L \xrightarrow{\sim} L'$, und das auch dann noch, wenn wir die naheliegende Forderung stellen, daß unsere Isomorphismen auf K die Identität induzieren sollen. Eigentlich bräuchte man eben zum Schreiben über Mathematik außer dem bestimmten und dem unbestimmten Artikel noch ein Zwischending für "wohlbestimmt bis auf nicht eindeutigen Isomorphismus", aber es wäre wohl vermessen, die deutsche Grammatik dahingehend erweitern zu wollen. Wir sind mit unseren beiden Arten von Artikeln verglichen etwa mit dem Russischen sogar schon gut bedient: Sie werden das merken, sobald Sie mathematische Artikel lesen, die aus dieser Sprache übersetzt sind: Oft sind dann in der Übersetzung ohne Verstand bestimmte oder unbestimmte Artikel gewählt worden, was man dann beim Lesen erst im Geiste korrigieren muß, damit sich ein sinnvoller Text ergibt. Um diese Phänomene der "Wohlbestimmtheit bis auf nicht eindeutigen Isomorphismus" im vorliegenden Fall begrifflich zu fassen, führen wir zunächst einmal eine geeignete Terminologie ein.

Definition 3.5.5. Sei K ein Ring. Unter einem **K-Ring** verstehen wir ein Paar (L, i) bestehend aus einem Ring L und einem Ringhomomorphismus $i : K \to L$. Ist (M, j) ein weiterer K-Ring, so verstehen wir unter einem **Homomorphismus von K-Ringen** $L \to M$ einen Ringhomomorphismus $\varphi : L \to M$ mit $\varphi \circ i = j$. Alternativ sprechen wir auch von einem **Homomorphismus über** K. Die Menge aller solchen Homomorphismen notieren wir

$$\mathrm{Ring}^K(L, M)$$

Einen bijektiven Ringhomomorphismus über K nennen wir auch einen **Isomorphismus von K-Ringen** oder einen **Isomorphismus über K**.

Beispiel 3.5.6. Unser Satz II.2.5.4 über das Einsetzen in Polynome kann in dieser Terminologie dahingehend formuliert werden, daß für jeden Ring k und jeden k-Ring (R, i) das Auswerten bei X eine Bijektion

$$\mathrm{Ring}^k(k[X], R) \quad \tilde{\to} \quad \{b \in R \mid bi(a) = i(a)b \; \forall a \in k\}$$

liefert. Die Umkehrabbildung ordnet jedem b den durch das Einsetzen von b erklärten Ringhomomorphismus $k[X] \to R$ zu.

Definition 3.5.7. Ist K ein Körper, so bezeichnen wir wie bereits in 3.2.3 angedeutet einen K-Ring, der seinerseits ein Körper ist, auch als eine **Körpererweiterung von** K oder, wenn wir pedantisch sein wollen, als eine "Körpererweiterung im verallgemeinerten Sinne". Unsere Homomorphismen und Isomorphismen von K-Ringen nennen wir in diesem Kontext **Homomorphismen** bzw. **Isomorphismen von Körpererweiterungen**. Fassen wir $i : K \hookrightarrow L$ auf als die Einbettung eines Unterkörpers $K \subset L$ und ist $j : K \to M$ ein weiterer Körperhomomorphismus, so nennen wir einen Körperhomomorphismus $L \to M$ über K auch eine **Ausdehnung** von j auf L und benutzen Notationen wie zum Beispiel $\tilde{\jmath} : L \to M$.

Ergänzung 3.5.8. Ist k ein Körper, so ist jeder kommutative k-Ring im Sinne der vorhergehenden Definition 3.5.5 alias jeder **k-Kring** eine kommutative k-Ringalgebra im Sinne unserer Definition II.9.5.6, und jede kommutative k-Ringalgebra A wird umgekehrt durch den einzigen Homomorphismus $k \to A$ von k-Ringalgebren zu einem k-Kring. Im Kommutativen sind diese beiden Konzepte also äquivalent.

Proposition 3.5.9 (Ausdehnungen auf primitive Erweiterungen). *Ist $j : K \hookrightarrow M$ eine Körpererweiterung und $K(\alpha)$ eine primitive algebraische Erweiterung von K, so werden die Ausdehnungen von j zu einer Einbettung $\tilde{\jmath} : K(\alpha) \hookrightarrow M$ parametrisiert durch die Nullstellen in M des Minimalpolynoms von α über K. Genauer liefert das Auswerten an α eine Bijektion*

$$\begin{array}{ccc} \mathrm{Ring}^K(K(\alpha), M) & \tilde{\to} & \{\beta \in M \mid \mathrm{Irr}(\alpha, K)(\beta) = 0\} \\ \varphi & \mapsto & \varphi(\alpha) \end{array}$$

3.5.10. In der Formulierung dieser Proposition haben wir beim Auswerten des Polynoms $\mathrm{Irr}(\alpha, K) \in K[X]$ auf $\beta \in M$ stillschweigend die Elemente von K mit ihren Bildern in M unter j identifiziert. Dieselbe abkürzende Notation ist gemeint, wenn wir im gleich folgenden Beweis den Teilkörper $K(\beta) \subset M$ bilden.

Beispiel 3.5.11. Wir haben im Fall $K = \mathbb{Q}$, $M = \mathbb{C}$, $\alpha = \mathrm{i}$ etwa

$$\begin{array}{ccc} \mathrm{Ring}^{\mathbb{Q}}(\mathbb{Q}(\mathrm{i}), \mathbb{C}) & \xrightarrow{\sim} & \{\beta \in \mathbb{C} \mid \beta^2 + 1 = 0\} \\ \varphi & \mapsto & \varphi(\mathrm{i}) \end{array}$$

Beweis. Sicher induziert das Auswerten eine injektive Abbildung zwischen den angegebenen Mengen, und wir müssen nur noch die Surjektivität zeigen. Nach 3.2.12 haben wir jedoch für jede Nullstelle β von $\mathrm{Irr}(\alpha, K)$ in M Isomorphismen

$$K(\alpha) \xleftarrow{\sim} K[X]/\langle \mathrm{Irr}(\alpha, K) \rangle \xrightarrow{\sim} K(\beta)$$

mit $\bar{X} \mapsto \alpha$ bzw. $\bar{X} \mapsto \beta$, und diese liefern unmittelbar die gesuchte Einbettung $K(\alpha) \xrightarrow{\sim} K(\beta) \subset M$ mit $\alpha \mapsto \beta$. □

Proposition 3.5.12 (Ausdehnbarkeitskriterium). *Sei $K(\alpha_1, \ldots, \alpha_n)$ eine endliche Erweiterung eines Körpers K und sei $j : K \hookrightarrow M$ eine Einbettung von K in einen Körper M derart, daß die Minimalpolynome $\mathrm{Irr}(\alpha_\nu, K)$ unserer Erzeuger α_ν in $M[X]$ vollständig in Linearfaktoren zerfallen. So läßt sich die Einbettung j ausdehnen zu einer Einbettung $\tilde{\jmath} : K(\alpha_1, \ldots, \alpha_n) \hookrightarrow M$, im Diagramm*

$$\begin{array}{ccc} K & \hookrightarrow & K(\alpha_1, \ldots, \alpha_2) \\ & \searrow & \vdots \\ & & M \end{array}$$

Beweis. Mit Lemma 3.5.9 sehen wir, daß das Einschränken eine Kette von Surjektionen der Gestalt

$$\mathrm{Ring}^K(K, M) \twoheadleftarrow \mathrm{Ring}^K(K(\alpha_1), M) \twoheadleftarrow \ldots \twoheadleftarrow \mathrm{Ring}^K(K(\alpha_1, \ldots, \alpha_n), M)$$

liefert. Man beachte hierbei, daß es nicht ausreicht, nur zu fordern, daß die Minimalpolynome $\mathrm{Irr}(\alpha_\nu, K)$ jeweils eine Nullstelle in M haben: Dann können wir zwar den ersten Schritt in obigem Argument noch gehen, aber das Minimalpolynom von α_2 über $K(\alpha_1)$ ist ja im allgemeinen nur noch ein Teiler des Minimalpolynoms $\mathrm{Irr}(\alpha_2, K)$ von α_2 über K, und auch wenn $\mathrm{Irr}(\alpha_2, K)$ eine Nullstelle in M hat, muß das für $\mathrm{Irr}(\alpha_2, K(\alpha_1))$ noch lange nicht gelten. Zerfällt jedoch $\mathrm{Irr}(\alpha_2, K)$ vollständig in M, so auch $\mathrm{Irr}(\alpha_2, K(\alpha_1))$. □

Zweiter Beweis. Diese Proposition folgt auch unmittelbar aus der allgemeineren und vielleicht etwas "glatteren" Aussage 3.7.8 über Einbettungen in den algebraischen Abschluß, wie im folgenden ausgeführt wird: Mit 3.7.3.2 dürfen wir M algebraisch über K annehmen. Nach 3.7.8 läßt sich M dann über K in einen algebraischen Abschluß $\bar{K}$ von K einbetten. Wieder nach 3.7.8 können wir auch $K(\alpha_1, \ldots, \alpha_n)$ über K in $\bar{K}$ einbetten, und nach Annahme liegt sein Bild dann notwendig im Bild von M. □

Beweis der Eindeutigkeit von Zerfällungskörpern 3.5.2. Proposition 3.5.12 liefert uns Injektionen $L \hookrightarrow L'$ und $L' \hookrightarrow L$ über K. Da hier beide Seiten endlichdimensionale Vektorräume sind über K und da unsere Injektionen beide K-linear sind, müssen sie beide Isomorphismen sein. □

Übung 3.5.13. Es sei K ein Körper, $P \in K[X]$ ein Polynom vom Grad n und L/K der Zerfällungskörper von P. Zeigen Sie, dass $[L : K] \leq n!$ ist.

Satz 3.5.14 (Maximalzahl von Ausdehnungen). *Ist L/K eine endliche Körpererweiterung und $j : K \hookrightarrow M$ eine Einbettung von K in einen weiteren Körper M, so gibt es höchstens $[L : K]$ Fortsetzungen von j zu einer Einbettung $\tilde{j} : L \hookrightarrow M$, in Formeln*

$$|\operatorname{Ring}^K(L, M)| \leq [L : K]$$

Erster Beweis. Gibt es einen Zwischenkörper L' mit $K \subset L' \subset L$ aber $K \neq L' \neq L$, so folgt der Satz mit vollständiger Induktion über den Grad unserer Körpererweiterung. Sonst gilt $L = K(\alpha)$ für ein $\alpha \in L$, und die Erweiterungen von j zu einer Einbettung von $K(\alpha)$ in M werden nach 3.5.9 parametrisiert durch die Nullstellen in M des Minimalpolynoms von α über K. Dieses Polynom hat aber den Grad $[K(\alpha) : K]$ und höchstens ebensoviele Nullstellen in M. □

Zweiter Beweis. Sind $\sigma_1, \ldots, \sigma_r$ paarweise verschiedene K-lineare Körperhomomorphismen $L \to M$, so müssen sie nach 3.5.15 bereits über M linear unabhängig sein im M-Vektorraum $\operatorname{Ens}(L^\times, M)$. Wäre nun $\lambda_1, \ldots, \lambda_s$ eine Basis von L über K mit weniger Elementen $s < r$, so gäbe es $a_1, \ldots, a_s \in M$ nicht alle Null mit $\sum_i a_i \sigma_i(\lambda_j) = 0$ für alle j, und dann wäre $\sum_i a_i \sigma_i$ die Nullabbildung im Widerspruch zu Satz 3.5.15 über die lineare Unabhängigkeit von Charakteren. □

Satz 3.5.15 (Lineare Unabhängigkeit von Charakteren). *Die Menge aller Homomorphismen von einer Gruppe in die multiplikative Gruppe eines Körpers ist stets linear unabhängig im Vektorraum aller Abbildungen von besagter Gruppe in besagten Körper.*

3.5.16. Dasselbe gilt mit demselben Beweis allgemeiner auch für die Menge aller Homomorphismen von einem Monoid in die multiplikative Gruppe eines Körpers.

Beweis. Bezeichnen wir unsere Gruppe mit G und unserem Körper mit L, so behaupten wir in Formeln, daß $\operatorname{Grp}(G, L^\times)$ eine linear unabhängige Teilmenge des L-Vektorraums $\operatorname{Ens}(G, L)$ ist. Sei in der Tat sonst

$$a_1\chi_1 + a_2\chi_2 + \ldots + a_n\chi_n = 0$$

eine nichttriviale lineare Relation kürzestmöglicher Länge mit $a_i \in L$ und $\chi_i : G \to L^\times$ paarweise verschiedenen Gruppenhomomorphismen. Wegen $\chi(1) = 1$

für alle Charaktere χ haben wir notwendig $n \geq 2$. Wegen $\chi_1 \neq \chi_2$ finden wir $g \in G$ mit $\chi_1(g) \neq \chi_2(g)$. Unsere Gleichung impliziert nun aber für jedes und insbesondere auch für dieses $g \in G$ die Gleichungen

$$a_1\chi_1(g)\chi_1 + a_2\chi_2(g)\chi_2 + a_n\chi_n(g)\chi_n = 0$$
$$a_1\chi_1(g)\chi_1 + a_2\chi_1(g)\chi_2 + a_n\chi_1(g)\chi_n = 0$$

und deren Differenz wäre eine kürzere nichttriviale Linearkombination im Widerspruch zu unserer Annahme. □

Definition 3.5.17. Eine Körpererweiterung L/K heißt **normal** genau dann, wenn sie algebraisch ist und wenn gilt: Jedes *irreduzible* Polynom aus $K[X]$, das in L eine Nullstelle hat, zerfällt in $L[X]$ schon in Linearfaktoren.

3.5.18. In der älteren Literatur, zum Beispiel in [Art], wird der Begriff "normal" manchmal auch abweichend definiert als diejenige Eigenschaft einer Körpererweiterung, die wir später mit "Galois" bezeichnen werden. Ich finde die Begriffsbildung in beiden Varianten ungeschickt: Normalerweise ist eine Körpererweiterung nämlich keineswegs normal im mathematischen Sinne, oder um es anders auszudrücken: Normal zu sein ist für Körpererweiterungen etwas ganz Besonderes. Aber gut, ein Psychiologe ist vermutlich durchaus auch der Ansicht, daß es für einen Menschen etwas ganz Besonderes ist, normal zu sein: So fern vom umgangssprachlichen Wortsinn ist unsere mathematische Terminologie also auch wieder nicht.

Beispiele 3.5.19. $\mathbb{Q}(\sqrt{2})$ ist normal über $\mathbb{Q}$, aber $\mathbb{Q}(\sqrt[3]{2})$ ist nicht normal über $\mathbb{Q}$, denn wir können $\mathbb{Q}(\sqrt[3]{2})$ einbetten in $\mathbb{R}$ und die beiden anderen Wurzeln des in $\mathbb{Q}[X]$ irreduziblen Polynoms $X^3 - 2$ sind nicht reell.

Satz 3.5.20 (Charakterisierung normaler Erweiterungen). *Für eine endliche Körpererweiterung L/K sind gleichbedeutend:*

1. *L/K ist normal;*
2. *L ist der Zerfällungskörper eines Polynoms $P \in K[X]$.*

Beweis. $1 \Rightarrow 2$. Ist L normal über K und erzeugt von $\alpha_1, \ldots, \alpha_r$, so ist L ein Zerfällungskörper für das Produkt der Minimalpolynome $\mathrm{Irr}(\alpha_i, K)$ der α_i über K. Für die andere Implikation machen wir einen Umweg über die folgende etwas technische Aussage:

3. *Für jede Einbettung $j : K \hookrightarrow M$ von K in einen weiteren Körper M haben alle Fortsetzungen von j zu Einbettungen $\varphi, \psi : L \hookrightarrow M$ dasselbe Bild, in Formeln $\varphi(L) = \psi(L)$ $\forall \varphi, \psi \in \mathrm{Ring}^K(L, M)$.*

Jetzt zeigen wir $2 \Rightarrow 3 \Rightarrow 1$ und beginnen mit $2 \Rightarrow 3$. Sowohl φ als auch ψ identifizieren die Nullstellen von P in L mit den Nullstellen von P in M, wenn auch nicht notwendig in derselben Weise. Da nun L erzeugt wird über K von den Nullstellen von P folgt $\varphi(L) = \psi(L)$. Schließlich zeigen wir noch $3 \Rightarrow 1$. Sei $P \in K[X]$ irreduzibel mit einer Nullstelle $\alpha \in L$. Wir ergänzen α zu einem endlichen Erzeugendensystem von L über K, sagen wir $L = K(\alpha, \beta_1, \ldots, \beta_n)$. Dann wählen wir für M eine Körpererweiterung von L, in der sowohl das Minimalpolynom von α als auch die Minimalpolynome aller β_i vollständig in Linearfaktoren zerfallen. Für jede Nullstelle $\alpha' \in M$ von P können wir unsere Einbettung $K \hookrightarrow M$ nach 3.5.9 zunächst fortsetzen zu einer Einbettung $K(\alpha) \hookrightarrow M$ mit $\alpha \mapsto \alpha'$, und dann nach 3.5.12 weiter zu einer Einbettung $L \hookrightarrow M$. Jede Nullstelle von P in M liegt also in $\varphi(L)$ für geeignetes φ, und da alle diese Bilder nach Annahme übereinstimmen, in Formeln $\varphi(L) = L$, zerfällt unser Polynom P schon über L vollständig in Linearfaktoren. □

Übung 3.5.21. Es seien M/L und L/K algebraische Körpererweiterungen. Ist M/K normal, so ist auch M/L normal. Sind L_1 und L_2 normale Körpererweiterungen von K und $L_1, L_2 \subset M$, so ist $L_1 \cap L_2$ normal über K. Geben Sie ein Beispiel an, wo M/L und L/K jeweils normal sind, und M/K nicht normal ist.

Proposition 3.5.22 (Vergrößern zu normaler Erweiterung). *Jede endliche Körpererweiterung L/K läßt sich zu einer endlichen normalen Körpererweiterung N/K vergrößern, es gibt in anderen Worten eine endliche Erweiterung N/L derart, daß N/K normal ist.*

Beweis. Wir nehmen Erzeuger $\alpha_1, \ldots, \alpha_r$ von L über K und konstruieren N als einen Zerfällungskörper über L des Produkts ihrer Minimalpolynome. Dies N ist dann natürlich auch ein Zerfällungskörper des besagten Produkts über K und damit normal über K. □

Übung 3.5.23. Man formuliere präzise und zeige, daß es bis auf nichteindeutigen Isomorphismus genau ein minimales N wie in Proposition 3.5.22 gibt. Dies N heißt dann die **normale Hülle** von L über K.

Übung 3.5.24. Jede endliche Körpererweiterung von $\mathbb{R}$ ist isomorph im Sinne von 3.5.5 zu $\mathbb{R}$ oder $\mathbb{C}$.

Ergänzende Übung 3.5.25. Sei k ein Körper und $a \in k$ und $n \geq 1$. Man zeige, daß im Zerfällungskörper des Polynoms $X^n - a$ auch das Polynom $X^n - 1$ stets in Linearfaktoren zerfällt, daß aber umgekehrt im Zerfällungskörper des Polynoms $X^n - 1$ ein Polynom $X^n - a$ nicht notwendig in Linearfaktoren zerfallen muß.

3.6 Vielfachheit von Nullstellen

3.6.1. Unter einer **mehrfachen Nullstelle** eines Polynoms mit Koeffizienten in einem Körper oder allgemeiner einem kommutativen Integritätsbereich verstehen wir eine Nullstelle einer Vielfachheit mindestens Zwei.

Satz 3.6.2. *Seien $K \subset L$ Körper und sei $P \in K[X]$ ein irreduzibles Polynom. Ist* $\operatorname{char} K = 0$, *so hat P keine mehrfachen Nullstellen in L.*

3.6.3. Wir werden in 3.6.15 gegen Ende dieses Abschnitts sogar eine etwas allgemeinere Aussage zeigen. Das braucht jedoch einige Vorbereitungen. In einem Körper K der Charakteristik $\operatorname{char} K = p$ hat jedes Element $a \in K$ höchstens eine p-te Wurzel. In der Tat, gilt $b^p = a$, so folgt $(X^p - a) = (X - b)^p$ und folglich ist b die einzige Nullstelle des Polynoms $X^p - a$. Betrachten wir nun den Körper $K = \mathbb{F}_p(T)$, so besitzt $a = T$ keine p-te Wurzel in K. Das Polynom $X^p - T$ ist sogar irreduzibel, was der Leser zur Übung zeigen mag. In jedem Fall hat aber jeder irreduzible Faktor dieses Polynoms mehrfache Nullstellen in einer geeigneten Körpererweiterung.

Definition 3.6.4. Für ein Polynom $P = a_n X^n + \ldots + a_2 X^2 + a_1 X + a_0$ mit Koeffizienten in einem beliebigen Ring R definieren wir seine **(formale) Ableitung** $P' \in R[X]$ durch die Vorschrift

$$P' = n a_n X^{n-1} + \ldots + 2a_2 X + a_1$$

Lemma 3.6.5 (Ableitungsregeln). *Auch für unser formales Ableiten gilt die Summenregel $(P+Q)' = P' + Q'$ und die Produktregel $(PQ)' = P'Q + PQ'$.*

Beweis. Die Summenregel ist offensichtlich. Bei der Produktregel sind mithin beide Seiten additiv in P und Q und wir können uns auf den Fall $P = X^i$ und $Q = X^j$ zurückziehen, in dem man die Formel leicht explizit prüft. □

Lemma 3.6.6 (Ableitung und mehrfache Nullstellen). *Ist K ein Körper, $g \in K[X]$ ein von Null verschiedenes Polynom und $\alpha \in K$ eine Nullstelle von g, so ist α genau dann eine mehrfache Nullstelle von g, wenn auch die Ableitung g' von g bei α verschwindet.*

Beweis. Ist $g = (x - \alpha)^2 f$, so folgt mit der Produktregel 3.6.5 leicht $g'(\alpha) = 0$. Gilt umgekehrt $g(\alpha) = g'(\alpha) = 0$ und schreiben wir $g = (x-\alpha)h$, so folgt wieder mit der Produktregel 3.6.5 aus $g'(\alpha) = 0$ schon $h(\alpha) = 0$. □

3.6.7. Gegeben eine Menge von Polynomen in einer Veränderlichen mit Koeffizienten einem Körper, nicht alle Null, besitzt das von unserer Menge erzeugte Ideal genau einen normierten Erzeuger. Er ist offensichtlich unter allen normierten

gemeinsamen Teilern aller Polynome unserer Menge derjenige von größtmöglichem Grad. Wir nennen ihn den **normierten größten gemeinsamen Teiler** unserer Menge von Polynomen. Man kann ihn, analog wie in II.2.3.15 im Fall der ganzen Zahlen erklärt, mit dem euklidischen Algorithmus unschwer explizit berechnen.

Proposition 3.6.8. *Seien $K \subset L$ Körper und $f, g \in K[X]$ Polynome und es gelte $g \neq 0$.*

1. *Das Teilen mit Rest von f durch g führt zum selben Resultat unabhängig davon, ob wir es in $K[X]$ oder in $L[X]$ durchführen.*
2. *Genau dann ist g ein Teiler von f in $L[X]$, wenn dasselbe gilt in $K[X]$.*
3. *Der normierte größte gemeinsame Teiler von f und g in $K[X]$ ist auch der normierte größte gemeinsame Teiler von f und g in $L[X]$.*

Beweis. 1. Schreiben wir $f = qg + r$ mit $\operatorname{grad} r < \operatorname{grad} g$, so sind q und r schon eindeutig bestimmt. Insbesondere ist die Lösung in $K[X]$ auch die einzig mögliche Lösung in $L[X]$.

2. Das ist der Spezialfall von Teil 1 mit Rest $r = 0$.

3. Seien dazu d_K bzw. d_L der normierte größte gemeinsame Teiler von f bzw. g in $K[X]$ bzw. in $L[X]$ nach 3.6.7. Natürlich ist d_K auch ein gemeinsamer Teiler in $L[X]$, also gilt $d_K | d_L$. Andererseits haben wir eine Darstellung $d_K = qf + pg$ mit $q, p \in K[X]$, und daraus folgt umgekehrt $d_L | d_K$. Zusammen zeigt das $d_L = d_K$. □

Lemma 3.6.9 (Ableitung und mehrfache Nullstellen, Variante). *Für ein Polynom mit Koeffizienten in einem Körper sind gleichbedeutend:*

1. *Das Polynom hat mehrfache Nullstellen in seinem Zerfällungskörper.*
2. *Das Polynom und seine Ableitung sind nicht teilerfremd.*

3.6.10. Bei der Bedingung "teilerfremd" kommt es wegen 3.6.8 nicht darauf an, ob wir sie in unserem ursprünglichen Polynomring oder im Polynomring mit Koeffizienten in einem wie auch immer gearteten Erweiterungskörper verstehen. Ein Polynom, das keine mehrfachen Nullstellen in seinem Zerfällungskörper hat, nennt man auch **separabel**.

Beweis. Sei K unser Körper und $P \in K[X]$ unser Polynom.

$1 \Rightarrow 2$. Ist α eine mehrfache Nullstelle des Polynoms P in seinem Zerfällungskörper L, so ist $(X - \alpha)$ ein Teiler von P und P' in $L[X]$ und es folgt $\langle P, P' \rangle \neq$

$\langle 1 \rangle$.

$2 \Rightarrow 1$. Gilt $\langle P, P' \rangle \neq \langle 1 \rangle$, so betrachten wir den Zerfällungskörper M des Produkts PP'. In M gibt es dann ein Element α derart, daß $(X - \alpha)$ sowohl P als auch P' teilt. In anderen Worten ist α eine Nullstelle von P und P' und damit eine mehrfache Nullstelle von P nach 3.6.6. □

Satz 3.6.11 (Irreduzible Polynome mit mehrfachen Nullstellen). *Sei K ein Körper und $P \in K[X]$ ein irreduzibles Polynom. So sind gleichbedeutend:*

1. *Das Polynom P hat mehrfache Nullstellen in seinem Zerfällungskörper.*
2. *Die Ableitung P' von P ist das Nullpolynom.*
3. *Es gilt $\operatorname{char} K = p > 0$ und es gibt $Q \in K[X]$ mit $P(X) = Q(X^p)$.*

Beweis. Dem Leser überlassen. □

Definition 3.6.12.
1. Sei L/K eine Körpererweiterung. Ein Element $\alpha \in L$ heißt **separabel über** K genau dann, wenn es algebraisch ist über K und sein Minimalpolynom $\operatorname{Irr}(\alpha, K)$ keine mehrfachen Nullstellen hat.
2. Eine Körpererweiterung L/K heißt **separabel** genau dann, wenn jedes Element von L separabel ist über K.

Beispiel 3.6.13. In Charakteristik Null ist jede algebraische Körpererweiterung separabel nach 3.6.11. Nicht separabel ist $\mathbb{F}_p(\sqrt[p]{T})$ über $\mathbb{F}_p(T)$.

Definition 3.6.14. Ein Körper heißt **vollkommen** (englisch **perfect**, französisch **parfait**) genau dann, wenn er entweder die Charakteristik Null hat oder aber für $p = \operatorname{char} K$ die Abbildung $x \mapsto x^p$ eine Surjektion $K \twoheadrightarrow K$ ist. Zum Beispiel ist jeder endliche Körper vollkommen.

Satz 3.6.15 (Irreduzible Polynome über vollkommenen Körpern). *Jedes irreduzible Polynom aus dem Polynomring über einem vollkommenen Körper ist separabel. Jede algebraische Erweiterung eines vollkommenen Körpers ist separabel.*

Beweis. Sei K unser vollkommener Körper. Den Fall $\operatorname{char} K = 0$ haben wir bereits durch 3.6.2 erledigt. Sei also ohne Beschränkung der Allgemeinheit $\operatorname{char} K = p > 0$ und $P \in K[X]$ irreduzibel. Wäre P nicht separabel, so hätte P nach 3.6.11 die Form $P = b_n(X^p)^n + \ldots + b_1 X^p + b_0$. Nehmen wir aber nun $a_n, \ldots, a_0 \in K$ mit $a_i^p = b_i$ und betrachten $Q = a_n X^n + \ldots + a_0$, so folgt $P = Q^p$ im Widerspruch zur Irreduzibilität von P. □

Übung 3.6.16. Man zeige: Ein Polynom mit Koeffizienten in einem Körper der Charakteristik Null ist separabel genau dann, wenn es von keinem Quadrat eines irreduziblen Polynoms geteilt wird.

Satz 3.6.17 (Charakterisierung separabler Erweiterungen). *Für eine Körpererweiterung L/K sind gleichbedeutend:*

1. *L/K ist separabel.*
2. *L wird erzeugt über K von Elementen, die separabel sind über K.*

Ist L/K endlich, so sind auch gleichbedeutend:

3. *Für jede Vergrößerung N/L von L zu einer normalen Erweiterung von K gilt $|\mathrm{Ring}^K(L,N)| = [L:K]$.*
4. *Es gibt mindestens eine Körpererweiterung N/L von L mit der Eigenschaft $|\mathrm{Ring}^K(L,N)| = [L:K]$.*

Beweis. Zeigen wir $1 \Leftrightarrow 2$ für endliche Erweiterungen, so folgt es im allgemeinen. Wir dürfen uns also für den Rest des Beweises auf den Fall L/K endlich beschränken. $1 \Rightarrow 2$ ist klar. Für $2 \Rightarrow 3$ dürfen wir mit Induktion über den Grad $[L:K]$ annehmen $L = K(\alpha)$. Da α separabel ist, sind die $[L:K]$ Nullstellen seines Minimalpolynoms in N paarweise verschieden und liefern mit 3.5.9 paarweise verschiedene Erweiterungen der Einbettung $K \hookrightarrow N$ zu Körperhomomorphismen $K(\alpha) \hookrightarrow N$. Die Implikation $3 \Rightarrow 4$ ist klar. Für $4 \Rightarrow 1$ argumentieren wir durch Widerspruch: Wäre ein $\alpha \in L$ nicht separabel, so gäbe es nach 3.5.9 für jedes N weniger als $[K(\alpha):K]$ Ausdehnungen von $K \hookrightarrow N$ zu einer Einbettung $K(\alpha) \hookrightarrow N$ und damit nach 3.5.14 notwendig auch weniger als $[L:K]$ Ausdehnungen von $K \hookrightarrow N$ zu einer Einbettung $L \hookrightarrow N$. □

Übung 3.6.18. Seien $M \supset L \supset K$ Körper. Ist M/L separabel und L/K separabel, so ist M/K separabel. In jeder algebraischen Körpererweiterung M/K gibt es unter allen Zwischenkörpern $L \subset M$, die separabel sind über K, einen größten. Er heißt der **separable Abschluß von K in M**.

Übung 3.6.19. Eine algebraische Körpererweiterung derart, daß nur die Elemente des kleinen Körpers über diesem separabel sind, heißt **rein inseparabel**. Man zeige, daß eine algebraische Erweiterung L/K eines Körpers K der Charakteristik p rein inseparabel ist genau dann, wenn für jedes Element von L die p^r-te Potenz für hinreichend großes r in K liegt. Salopp gesprochen sind also rein inseparable Erweiterungen genau die Erweiterungen, die durch die sukzessive Adjunktion p-ter Wurzeln in Charakteristik p entstehen.

Ergänzende Übung 3.6.20. Gegeben ein Körper k induziert die Einbettung $k[X] \hookrightarrow k[\![X]\!] \hookrightarrow k((X))$ einen Ringhomomorphismus und nach II.2.8.4 eine Einbettung $k(X) \hookrightarrow k((X))$. Man zeige, daß diese Einbettung im Fall $\operatorname{char} k = 0$ für rationale Funktionen, die bei $X = 0$ keinen Pol haben, durch ein formales Analogon der Taylorformel beschrieben werden kann. Hierbei gilt es zunächst, die Ableitung eines Quotienten vermittels der Quotientenregel zu erklären.

Ergänzung 3.6.21 (**Die Diskriminante als Determinante**). Ich behaupte für die $a_i \in \mathbb{Z}[\zeta_1, \ldots, \zeta_n]$ gegeben durch die Identität $T^n + a_1 T^{n-1} + \ldots + a_n = (T + \zeta_1) \ldots (T + \zeta_n)$, daß die Determinante der nebenstehenden Matrix M gegeben wird durch die Formel

$$\det M = \prod_{i \neq j} (\zeta_i - \zeta_j)$$

und folglich genau unsere Diskriminante aus 2.7.17 ist. Um das zu zeigen, beachten wir zunächst, daß beide Seiten symmetrische Polynome sind und daß zumindest in $\mathbb{Q}[\zeta_1, \ldots, \zeta_n]$ alle $(\zeta_i - \zeta_j)$ nach 3.6.9 und II.2.5.39 und 2.8.9 das Polynom $(\det M)$ teilen müssen. Dann aber wechselt notwendig $(\det M)/(\zeta_i - \zeta_j)$ unter der Vertauschung von ζ_i und ζ_j sein Vorzeichen und muß nach II.2.5.39 folglich ein weiteres Mal durch $(\zeta_i - \zeta_j)$ teilbar sein. Mithin ist $\det M$ in $\mathbb{Q}[\zeta_1, \ldots, \zeta_n]$ durch $\prod_{i \neq j} (\zeta_i - \zeta_j)$ teilbar. Sicher ergibt das Wegteilen ein symmetrisches Polynom, das höchstens auf den Hyperebenen $\zeta_i = \zeta_j$ verschwindet. Wäre dies Polynom nicht konstant, so könnten wir mit denselben Argumenten ein weiteres Mal einen Faktor $\prod_{i \neq j} (\zeta_i - \zeta_j)$ herausziehen. Das führt jedoch zu einem Widerspruch, wenn wir etwa erst durch $\zeta_1^{2(n-1)}$ teilen, für $\zeta_2, \ldots, \zeta_n$ paarweise verschiedene rationale Zahlen einsetzen, und $\zeta_1 \in \mathbb{Q}$ gegen ∞ streben lassen: $(\det M)/\zeta_1^{2(n-1)}$ bleibt dann nämlich beschränkt, wie wir sehen, indem wir alle Spalten außer der Ersten mit ζ_1^{-1} multiplizieren, und $(\prod_{i \neq j} (\zeta_i - \zeta_j))/\zeta_1^{2(n-1)}$ strebt gegen eine von Null verschiedene Zahl, aber $(\prod_{i \neq j} (\zeta_i - \zeta_j))^r / \zeta_1^{2(n-1)}$ strebt für $r \geq 2$ stets nach Unendlich. Es gilt also nur noch, die Konstante $c \in \mathbb{Q}$ zu bestimmen mit

$$\det M = c \prod_{i \neq j} (\zeta_i - \zeta_j)$$

Dazu setzen wir $\zeta_i = -\zeta^i$ mit ζ einer primitiven n-ten Einheitswurzel. Dann folgt $(T + \zeta_1) \ldots (T + \zeta_n) = T^n - 1$ und $(\det M) = (-1)^{n(n-1)} n^n (-1)^{n-1}$ und andererseits

$$\prod_{i \neq j} (\zeta_i - \zeta_j) = (-1)^{n(n-1)} \prod_{i=1}^{n} \left(\zeta^i \prod_{j \neq i} (1 - \zeta^{j-i}) \right)$$

Das Produkt aller n-ten Einheitswurzeln ist nun sicher $(-1)^{n-1}$ und das zweite Produkt kann berechnet werden als der Wert an der Stelle $t = 1$ des Polynoms

SkriptenBilder/BildDisk.png

Die Determinante dieser Matrix stimmt überein mit der Diskriminante des Polynoms $T^n + a_1 T^{n-1} + \ldots + a_n$, wie sie in 2.7.18 für jedes normierte Polynom erklärt wird. Im übrigen ist diese Determinante im wesentlichen die Resultante unseres Polynoms und seiner Ableitung.

$(t^n-1)/(t-1) = t^{n-1}+\ldots+t+1$. So erhalten wir für die gesuchte Konstante c schließlich

$$(-1)^{n(n-1)}(-1)^{n-1}n^n = (-1)^{n(n-1)}(-1)^{n-1}n^n c$$

und damit $c = 1$ wie gewünscht.

3.7 Der algebraische Abschluß

3.7.1. In der Literatur ist es üblich, sich bei der Entwicklung der Körpertheorie stark auf den Satz von der Existenz eines algebraischen Abschlusses zu stützen. Das hat jedoch meines Erachtens den Nachteil, daß der Beweis dieses Satzes das Zorn'sche Lemma benötigt, dessen Herleitung aus dem a priori anschaulich besser motivierten Auswahlaxiom seinerseits nicht ganz einfach ist. Um die Entwicklung der Grundlagen der Algebra von diesen Schwierigkeiten zu entlasten, entwickle ich in diesem Text die Grundzüge der Körpertheorie unabhängig von dem Satz von der Existenz eines algebraischen Abschlusses und diskutiere diesen Satz hier nur, damit weiterführende Vorlesungen darauf zurückgreifen können. Der folgende Abschnitt ist also für die weitere Entwicklung dieser Vorlesung unerheblich und kann ohne Schaden übersprungen werden.

Definition 3.7.2. Eine Körpererweiterung heißt **algebraisch** genau dann, wenn alle Elemente der Erweiterung algebraisch sind über dem Grundkörper.

Satz 3.7.3 (über algebraische Körpererweiterungen).

1. *Jede endlich erzeugte algebraische Körpererweiterung ist endlich.*
2. *Sei L/K eine Körpererweiterung. Diejenigen Elemente von L, die algebraisch sind über K, bilden einen Unterkörper von L.*
3. *Seien $M \supset L \supset K$ Körper. Ist M algebraisch über L und L algebraisch über K, so ist M algebraisch über K.*

Beweis. (1) Sei $L = K(\alpha_1,\ldots,\alpha_n)$. Sind alle α_i algebraisch über K, so sind sie erst recht algebraisch über $K(\alpha_1,\ldots,\alpha_{i-1})$. Wir betrachten die Körperkette

$$K \subset K(\alpha_1) \subset K(\alpha_1,\alpha_2) \subset \ldots \subset K(\alpha_1,\ldots,\alpha_n) = L$$

Da hier alle Schritte endlich sind nach 3.2.23, ist auch L/K endlich nach der Multiplikativität des Grades 3.2.27. (2) Sind α und $\beta \in L$ algebraisch über K, so haben wir $[K(\alpha,\beta):K] < \infty$ nach Teil 1. Mithin sind alle Elemente von $K(\alpha,\beta)$ algebraisch über K nach 3.2.23. (3) Für $\alpha \in M$ betrachten wir die Koeffizienten

$\beta_0, \ldots, \beta_r \in L$ seines Minimalpolynoms über L. Dann ist α sogar algebraisch über $K(\beta_0, \ldots, \beta_r)$. Der Turm von endlichen Körpererweiterungen

$$K \subset K(\beta_0, \ldots, \beta_r) \subset K(\beta_0, \ldots, \beta_r, \alpha)$$

zeigt dann, daß α algebraisch ist über K. □

Ergänzende Übung 3.7.4. Man zeige, daß eine algebraische Körpererweiterung eines unendlichen Körpers stets dieselbe Kardinalität hat wie der Ausgangskörper.

Definition 3.7.5. Ein **algebraischer Abschluß** eines Körpers ist eine algebraische Erweiterung unseres Körpers durch einen algebraisch abgeschlossenen Körper.

Satz 3.7.6 (über den algebraischen Abschluß). *Jeder Körper besitzt einen algebraischen Abschluß, und dieser algebraische Abschluß ist eindeutig bis auf im allgemeinen nicht eindeutigen Isomorphismus von Körpererweiterungen.*

3.7.7. Wegen dieser partiellen Eindeutigkeit erlaubt man sich meist den bestimmten Artikel und spricht von *dem* algebraischen Abschluß eines Körpers K und notiert ihn

$$\bar{K}$$

Ein algebraischer Abschluß von $\mathbb{R}$ wäre etwa der Körper $\mathbb{C}$, wie wir ihn in II.2.1.4 als Teilring des Rings der reellen (2×2)-Matrizen eingeführt haben, mit der dort konstruierten Einbettung von $\mathbb{R}$, ein anderer der wie in I.3.3.14 zu $K = \mathbb{R}$ durch das explizite Erklären einer Multiplikation auf $\mathbb{R}^2$ konstruierte Körper, wieder mit der dort konstruierten Einbettung von $\mathbb{R}$. Sicher sind diese beiden Körpererweiterungen von $\mathbb{R}$ isomorph, aber es gibt zwischen ihnen genau zwei Isomorphismen, von denen keiner "besser" ist als der andere. Die größte separable Teilerweiterung in einem algebraischen Abschluß eines Körpers nennt man seinen **separablen Abschluß**.

Beweis. Gegeben ein Körper K konstruiert man ohne Schwierigkeiten eine Menge Ω, deren Kardinalität echt größer ist als die Kardinalität jeder algebraischen Erweiterung von K in dem Sinne, daß es für keine algebraische Erweiterung von K eine surjektive Abbildung nach Ω gibt. Die Menge $\Omega = \mathcal{P}(K[X] \times \mathbb{N})$ wäre etwa eine Möglichkeit: Jedes Element einer algebraischen Erweiterung L von K ist ja eine von endlich vielen Nullstellen eines Polynoms aus $K[X]$, so daß wir unter Zuhilfenahme des Auswahlaxioms sicher eine injektive Abbildung $L \hookrightarrow K[X] \times \mathbb{N}$ finden können. Die Existenz einer Surjektion $L \twoheadrightarrow \Omega$ stünde damit im Widerspruch zu I.2.2.19, wonach es keine Surjektion $K[X] \times \mathbb{N} \twoheadrightarrow \mathcal{P}(K[X] \times \mathbb{N})$ geben kann. Jetzt betrachte man die Menge aller Tripel (M, s, φ) bestehend aus einer Teilmenge $M \subset \Omega$, einer Struktur s eines Körpers darauf und einem Köperhomomorphismus $\varphi : K \to M$, bezüglich dessen M algebraisch ist über K. Nach

dem Zorn'schen Lemma **??** existiert bezüglich der offensichtlichen Ordnungsrelation ein maximales derartiges Tripel, und bei solch einem maximalen Tripel ist M notwendig algebraisch abgeschlossen: Sonst könnten wir nämlich nach 3.4.6 eine endliche Erweiterung L/M von M finden und die Einbettung $M \hookrightarrow \Omega$ zu einer Einbettung von Mengen $L \hookrightarrow \Omega$ ausdehnen—hier verwenden wir implizit nocheinmal das Zorn'sche Lemma, nach dem es eine maximale Ausdehnung auf eine Teilmenge von L geben muß, die aber nicht surjektiv sein kann und deshalb bereits auf ganz L definiert sein muß—und erhielten ein noch größeres Tripel. Das zeigt die Existenz. Seien weiter $K \hookrightarrow \bar{K}$ und $K \hookrightarrow E$ zwei algebraische Abschlüsse von K. Nach 3.7.8, das wir im Anschluß beweisen, läßt sich die Identität auf K fortsetzen zu einem Körperhomomorphismus $\varphi : \bar{K} \to E$. Er ist natürlich injektiv und liefert für jedes Polynom $P \in K[X]$ eine Bijektion zwischen den Nullstellen von P in $\bar{K}$ und den Nullstellen von P in E. Folglich muß er auch surjektiv sein. □

Proposition 3.7.8 (Ausdehnung von Körpereinbettungen). *Eine Einbettung eines Körpers in einen algebraisch abgeschlossenen Körper läßt sich auf jede algebraische Erweiterung unseres ursprünglichen Körpers ausdehnen.*

3.7.9. Ist also in Formeln $K \hookrightarrow L$ eine algebraische Körpererweiterung, so läßt sich jede Einbettung $K \hookrightarrow F$ von K in einen algebraisch abgeschlossenen Körper F ausdehnen zu einer Einbettung $L \hookrightarrow F$. Es reicht hier sogar, wenn wir von F nur fordern, daß die Minimalpolynome $\operatorname{Irr}(\alpha, K)$ aller Elemente α irgendeines Erzeugendensystems von L über K vollständig in Linearfaktoren zerfallen, sobald wir sie als Polynome in $F[X]$ betrachten.

Beweis. Ohne Beschränkung der Allgemeinheit dürfen wir $K \subset L$ annehmen. Nach dem Zorn'schen Lemma gibt es unter allen Zwischenkörpern M mit $K \subset M \subset L$, auf die sich unsere Einbettung $K \hookrightarrow F$ fortsetzen läßt, mindestens einen Maximalen. Ich behaupte $M = L$. Sonst gäbe es nämlich $\alpha \in L \backslash M$, und dies α wäre algebraisch über M, mit Minimalpolynom $f \in M[X]$. Die Minimalpolynom hätte eine Nullstelle $\beta \in F$, und nach 3.5.9 könnten wir dann $M \hookrightarrow F$ fortsetzen zu einer Einbettung $M(\alpha) \to F$, $\alpha \mapsto \beta$ im Widerspruch zur Maximalität von M. □

Beispiel 3.7.10. Einen algebraischen Abschluß eines endlichen Primkörpers $\mathbb{F}_p$ können wir wie folgt konstruieren: Wir wählen eine Folge $r_0, r_1, \ldots$ von natürlichen Zahlen so, daß jeweils gilt $r_i | r_{i+1}$ und daß jede natürliche Zahl eines unserer Folgenglieder teilt. Dann haben wir Einbettungen $\mathbb{F}_{p^{r_i}} \subset \mathbb{F}_{p^{r_{i+1}}}$ und die aufsteigende Vereinigung

$$\bar{\mathbb{F}}_p = \bigcup_{i=0}^{\infty} \mathbb{F}_{p^{r_i}}$$

ist offensichtlich ein algebraischer Abschluß von $\mathbb{F}_p$. Eigentlich hatte ich versprochen, beliebige Vereinigungen nur zu bilden von Systemen einer gegebenen Teilmenge. Wenn Sie es mit diesem Versprechen genau nehmen, muß ich mich darauf zurückziehen, daß hier eigentlich ein Kolimes im Sinne von **??** gemeint ist.

Übung 3.7.11. Gegeben ein endlicher Körper ist die multiplikative Gruppe seines algebraischen Abschlusses in unkanonischer Weise isomorph zur Gruppe aller Elemente von $\mathbb{Q}/\mathbb{Z}$, deren Ordnung teilerfremd ist zur Charakteristik unseres Körpers.

Übung 3.7.12. Ist L/K eine Körpererweiterung durch einen algebraisch abgeschlossenen Körper, so bilden die über K algebraischen Elemente von L einen algebraischen Abschluß von K.

Alternativer Beweis für die Existenz eines algebraischen Abschlusses. Sei K unser Körper. Wir betrachten die Menge $S = K[X]\backslash K$ aller nicht konstanten Polynome mit Koeffizienten in K und bilden den riesigen Polynomring

$$R = K[X_f]_{f\in S}$$

in dem es also für jedes nichtkonstante Polynom f aus $K[X]$ eine eigene Variable X_f gibt. In diesem riesigen Polynomring betrachten wir das Ideal $\mathfrak{a} \subset R$, das von allen $f(X_f)$ erzeugt wird, und zeigen $\mathfrak{a} \neq R$. Sonst könnten wir nämlich $1 \in R$ schreiben als eine endliche Summe

$$1 = \sum_{f\in E} g_f f(X_f)$$

für $E \subset S$ endlich und geeignete $g_f \in R$. Nun gibt es nach 3.4.6, angewandt auf das Produkt der f aus E, eine Körpererweiterung L von K derart, daß alle f aus E in L eine Nullstelle $\alpha_f \in L$ haben. Für die übrigen $f \in S$ wählen wir Elemente $\alpha_f \in L$ beliebig und betrachten den Einsetzungshomomorphismus

$$\begin{array}{rccc} \varphi: & R & \to & L \\ & X_f & \mapsto & \alpha_f \end{array}$$

Dieser Ringhomomorphismus müßte nun die Eins in R auf die Null in L abbilden und das kann nicht sein. Folglich gilt $\mathfrak{a} \neq R$ und es gibt nach IV.1.4.4 ein maximales Ideal $\mathfrak{m} \supset \mathfrak{a}$. Dann ist $K_1 = R/\mathfrak{m}$ nach **??** ein Körper, und jedes nichtkonstante Polynom $f \in K[X]\backslash K$ hat eine Nullstelle in K_1, nämlich die Nebenklasse von X_f. Iterieren wir diese Konstruktion, so erhalten wir ein Kette von Körpern

$$K = K_0 \subset K_1 \subset K_2 \subset \ldots$$

derart, daß jedes nichtkonstante Polynom mit Koeffizienten in K_i eine Nullstelle hat in K_{i+1}. Die aufsteigende Vereinigung $\bigcup_{i=0}^{\infty} K_i$ ist dann ein algebraisch abgeschlossener Körper, der K enthält. Eigentlich hatte ich versprochen, beliebige Vereinigungen nur zu bilden von Systemen einer gegebenen Teilmenge. Wenn Sie es mit diesem Versprechen genau nehmen, muß ich mich darauf zurückziehen, daß hier eigentlich ein Kolimes im Sinne von **??** gemeint ist. □

Definition 3.7.13. Sei K ein Körper und $\mathcal{P} \subset K[X]$ ein Menge von Polynomen. Unter einem **Zerfällungskörper von** $\mathcal{P}$ verstehen wir eine Körpererweiterung L/K derart, daß (1) jedes Polynom $P \in \mathcal{P}$ in $L[X]$ vollständig in Linearfaktoren zerfällt und daß (2) der Körper L über K erzeugt wird von den Nullstellen der Polynome $P \in \mathcal{P}$.

Ergänzende Übung 3.7.14. Man zeige, daß eine Körpererweiterung L/K normal ist genau dann, wenn sie der Zerfällungskörper einer Menge von Polynomen $\mathcal{P} \subset K[X]$ ist. Hinweis: Man kopiere den Beweis von 3.5.20. Bei Punkt 3 dort reicht es, für M einen algebraischen Abschluß von K zu betrachten.

3.8 Schiefkörper über den reellen Zahlen*

3.8.1. Der Inhalt des folgenden Abschnitts ist für die weitere Entwicklung dieser Vorlesung nicht von Belang. Die Thematik schien mir jedoch so interessant, daß ich sie nicht auslassen wollte. Anwendungen ergeben sich insbesondere in der Darstellungstheorie endlicher Gruppen und allgemeiner in der abstrakten Theorie nicht notwendig kommutativer Ringe, in der die Schiefkörper eine wichtige Rolle spielen. Unter einem Schiefkörper verstehen wir wie in II.2.9.2 einen Ring R, der nicht der Nullring ist, und in dem alle von Null verschiedenen Elemente Einheiten sind.

Proposition 3.8.2 (**Schiefkörper über den reellen Zahlen**). *Jede endlichdimensionale $\mathbb{R}$-Ringalgebra, die ein Schiefkörper ist, ist als $\mathbb{R}$-Ringalgebra isomorph zu $\mathbb{R}, \mathbb{C}$ oder zum Schiefkörper $\mathbb{H}$ der Quaternionen II.2.9.4.*

3.8.3. Statt endlicher Dimension über $\mathbb{R}$ brauchen wir sogar nur anzunehmen, daß unsere Ringalgebra als $\mathbb{R}$-Vektorraum abzählbar erzeugt ist. Derselbe Beweis funktioniert, sobald wir etwa nach 3.2.32 wissen, daß auch jede Erweiterung abzählbarer Dimension von $\mathbb{R}$ bereits algebraisch ist.

Beweis. Sei K unsere $\mathbb{R}$-Ringalgebra. Die Struktur als $\mathbb{R}$-Ringalgebra liefert uns einen eindeutig bestimmten Homomorphismus von $\mathbb{R}$-Ringalgebren $\mathbb{R} \to K$, der wegen $K \neq 0$ sogar injektiv sein muß. Wir fassen ihn von nun an zur Vereinfachung der Notation als die Inklusion einer Teilmenge $\mathbb{R} \subset K$ auf. Gegeben $\alpha \in K \backslash \mathbb{R}$ können wir unsere Einbettung $\mathbb{R} \hookrightarrow K$ zu einer Einbettung $\mathbb{C} \hookrightarrow K$

fortsetzen, deren Bild α enthält: In der Tat ist die $\mathbb{R}$-Ringalgebra $\mathbb{R}[\alpha]$ notwendig eine echte algebraische Körpererweiterung von $\mathbb{R}$ und muß nach 3.5.24 also isomorph sein zu $\mathbb{C}$. Um die Notation nicht unnötig aufzublähen, denken wir uns von nun an vermittels dieser Einbettung $\mathbb{C}$ als einen Teilkörper $\mathbb{C} \subset K$. Jetzt machen wir K zu einem $\mathbb{C}$-Vektorraum durch Multiplikation von links. Die Multiplikation mit $\mathrm{i} \in \mathbb{C}$ von rechts wird dann ein $\mathbb{C}$-linearer Endomorphismus $J \in \mathrm{End}_{\mathbb{C}} K$ mit $J^2 = -\mathrm{id}_K$. Als Endomorphismus endlicher Ordnung II.6.4.11 oder einfacher als Endomorphismus der Ordnung vier ist er diagonalisierbar nach II.6.4.10 und liefert eine Zerlegung $K = K^+ \oplus K^-$ mit $K^\pm = \{a \in K \mid \mathrm{i}\, a = \pm a\, \mathrm{i}\}$. Nun ist K^+ ein endlichdimensionaler Schiefkörper über $\mathbb{C}$ mit $\mathbb{C}$ im Zentrum, woraus sofort folgt $K^+ = \mathbb{C}$. Gilt $K \neq \mathbb{C}$, so gibt es nach dem Beginn des Beweises auch in $K^- \oplus \mathbb{R}$ ein Element j mit Quadrat -1. Setzen wir $\mathrm{j} = \beta + \alpha$ an mit $\beta \in K^-$ und $\alpha \in \mathbb{R}$, so folgt $-1 = \mathrm{j}^2 = \beta^2 + 2\alpha\beta + \alpha^2$ mit dem ersten und letzten Term in K^+ und dem mittleren Term in K^-. Damit folgt $2\alpha\beta = 0$ und dann $\alpha = 0$ und man erkennt $\mathrm{j} \in K^-$. Für jedes von Null verschiedene $\mathrm{j} \in K^-$ induziert aber die Multiplikation mit j von rechts einen Isomorphismus $K^+ \xrightarrow{\sim} K^-$. Der Rest des Arguments kann dem Leser überlassen bleiben. □

Ergänzung 3.8.4. Eine **Kompositionsalgebra** ist ein reeller endlichdimensionaler euklidischer Vektorraum V zusammen mit einer bilinearen Abbildung $\mu : V \times V \to V$ derart, daß gilt $\|\mu(v,w)\| = \|v\| \cdot \|w\| \quad \forall v, w \in V$. Topologische Methoden zeigen, daß die Dimension eine Bijektion

$$\left\{ \begin{array}{c} \text{Kompositionsalgebren mit Einselement,} \\ \text{bis auf Isomorphismus} \end{array} \right\} \xrightarrow{\sim} \{0,1,2,4,8\}$$

liefert. Die fraglichen Kompositionsalgebren sind 0, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ und die sehr merkwürdige Struktur der sogenannten **Oktonionen** $\mathbb{O}$, auch genannt die **Cayley'schen Zahlen**, bei denen die Multiplikation nicht mehr assoziativ ist. Ausführlichere Informationen dazu findet man zum Beispiel in [E+92].

4 Galoistheorie

4.1 Galoiserweiterungen

Definition 4.1.1. Ein Isomorphismus von einem Körper mit sich selber heißt auch ein **Automorphismus** unseres Körpers. Sei L/K eine Körpererweiterung. Die Gruppe aller Körperautomorphismen von L, die K punktweise festhalten, heißt die **Galoisgruppe** $\mathrm{Gal}(L/K)$ der Körpererweiterung L/K. Sprechen wir von der Galoisgruppe eines Polynoms oder genauer von der Galoisgruppe über K eines Polynoms $P \in K[T]$, so meinen wir die Galoisgruppe seines Zerfällungskörpers L/K.

Ergänzung 4.1.2. Bezeichnet Ring die Kategorie der Ringe und Ring^K die Kategorie der Ringe unter K, so können wir die Galoisgruppe in kategorientheoretischer Notation schreiben als $\mathrm{Gal}(L/K) = (\mathrm{Ring}^K)^\times(L)$.

Beispiele 4.1.3. $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ ist eine Gruppe mit zwei Elementen, der Identität und der komplexen Konjugation. Betrachten wir in $\mathbb{R}$ die dritte Wurzel $\sqrt[3]{2}$ von 2, so besteht $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ nur aus der Identität, denn jeder Körperhomomorphismus $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2})$ muß die einzige Lösung der Gleichung $x^3 = 2$ in diesem Körper auf sich selbst abbilden.

Lemma 4.1.4. *Der Grad einer Körpererweiterung ist eine obere Schranke für die Kardinalität ihrer Galoisgruppe. Ist also in Formeln L/K unsere Körpererweiterung, so gilt in $\mathbb{N} \cup \{\infty\}$ die Ungleichung*

$$|\mathrm{Gal}(L/K)| \leq [L : K]$$

4.1.5. Aus dem im Anschluß bewiesenen Satz 4.1.11 folgt unmittelbar, daß für den Fall einer endlichen Körpererweiterung die Kardinalität der Galoisgruppe sogar den Grad der Körpererweiterung teilen muß, in Formeln

$$|\mathrm{Gal}(L/K)| \mid [L : K]$$

Beweis. Das folgt sofort aus Satz 3.5.14, nach dem sogar die Zahl der Körperhomomorphismen über K von L in einen beliebigen weiteren Körper M über K beschränkt ist durch $[L : K]$. □

Proposition 4.1.6. *Ist q eine Primzahlpotenz und $r \geq 1$, so ist $\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ eine zyklische Gruppe der Ordnung r, erzeugt vom* **Frobenius-Homomorphismus**

$$F : \mathbb{F}_{q^r} \xrightarrow{\sim} \mathbb{F}_{q^r}, \quad a \mapsto a^q$$

4.1.7. In II.2.4.39 hatten wir bereits einen Frobenius-Homomorphismus eingeführt. Der Frobenius-Homomorphismus hier ist seine l-te Potenz für l gegeben durch $q = p^l$ mit p prim.

Beweis. Sicher erzeugt F in der Galoisgruppe eine zyklische Untergruppe der Ordung r. Nach dem vorhergehenden Satz 4.1.4 hat die Galoisgruppe jedoch höchstens r Elemente. □

Definition 4.1.8. Eine Körpererweiterung L/K heißt eine **Galoiserweiterung** oder kurz **Galois** genau dann, wenn sie normal und separabel ist.

4.1.9. Gegeben eine endliche Galoiserweiterung L/K gilt für die Kardinalität der Galoisgruppe die Identität

$$|\operatorname{Gal}(L/K)| = [L : K]$$

In der Tat gibt es nach (3.6.17, $1 \Rightarrow 3$) für L endlich, separabel und normal über K genau $[L : K]$ verschiedene Körperhomomorphismen $L \to L$ über K. Als Körperhomomorphismen sind diese natürlich injektiv, und wegen der Gleichheit der K-Dimensionen sind sie dann auch surjektiv.

4.1.10. Operiert eine Gruppe G auf einer Menge X, so schreiben wir ganz allgemein X^G für die Menge der Fixpunkte. Ist speziell X ein Körper L und G eine Gruppe von Körperautomorphismen von L, so ist $L^G \subset L$ offensichtlich ein Unterkörper von L. Er heißt der **Fixkörper** von G.

Satz 4.1.11 (Galoiserweiterungen durch Gruppenoperationen). *Sei L ein Körper, G eine* endliche *Gruppe von Automorphismen von L und L^G der Fixkörper von G. So gilt:*

1. *Für alle $\alpha \in L$ wird das Minimalpolynom von α über L^G gegeben durch die Formel*
$$\operatorname{Irr}(\alpha, L^G) = \prod_{\beta \in G\alpha} (X - \beta)$$
2. *Die Körpererweiterung L/L^G ist eine endliche Galoiserweiterung vom Grad $[L : L^G] = |G|$ mit der Galoisgruppe $\operatorname{Gal}(L/L^G) = G$.*

Beweis. Schreiben wir $\prod_{\beta \in G\alpha}(X-\beta) = \sum a_i X^i$, so gilt für jedes Element $\sigma \in G$ die von der Mitte her zu entwickelnde Gleichungskette

$$\sum \sigma(a_i)X^i = \prod_{\beta \in G\alpha} (X - \sigma(\beta)) = \prod_{\beta \in G\alpha} (X - \beta) = \sum a_i X^i$$

Also gehört unser Produkt zu $L^G[X]$. Es teilt das Minimalpolynom $\operatorname{Irr}(\alpha, L^G)$, da ja mit α auch alle $\sigma(\alpha)$ für $\sigma \in G$ Nullstellen des Minimalpolynoms sein müssen. Da aber das Minimalpolynom irreduzibel und normiert ist, und da unser Produkt immerhin normiert ist, müssen diese beiden Polynome übereinstimmen und der

erste Punkt ist erledigt. Per definitionem ist dann L/L^G normal und separabel, also Galois. Als nächstes zeigen wir die Abschätzung

$$[L : L^G] \leq |G|$$

Wir argumentieren durch Widerspruch. Nehmen wir an, die Elemente von G seien $\sigma_1, \ldots, \sigma_r$ und es gebe in L eine um Eins größere über L^G linear unabhängige Familie $x_0, \ldots, x_r$. In der Matrix der $\sigma_i(x_j)$ sind dann notwendig die Spalten $\sigma_*(x_j)$ linear abhängig, wir finden also $y_0, \ldots, y_r$ in L nicht alle Null mit $\sum_j y_j \sigma_i(x_j) = 0 \ \forall i$ alias $\sum_j \sigma_i^{-1}(y_j) x_j = 0 \ \forall i$. Summieren wir diese Gleichungen, so ergibt sich

$$\sum_j \lambda_j x_j = 0$$

für $\lambda_j = \sum_i \sigma_i^{-1}(y_j)$. Sicher gilt $\lambda_j \in L^G$ für alle j. Nach dem Satz über die lineare Unabhängigkeit von Charakteren 3.5.15 gibt es jedoch ein $z \in L$ mit $\sum_i \sigma_i^{-1}(z) \neq 0$. Indem wir notfalls von $y_0, \ldots, y_r$ zu $yy_0, \ldots, yy_r$ übergehen, dürfen wir also annehmen, daß eines der λ_j nicht verschwindet, im Widerspruch zu unserer Annahme der linearen Unabhängigkeit der x_j. Mit unserer Abschätzung $[L : L^G] \leq |G|$ bewaffnet folgern wir schließlich die Gleichheit $G = \mathrm{Gal}(L/L^G)$ ohne weitere Schwierigkeiten aus der Ungleichungskette

$$|G| \leq |\operatorname{Gal}(L/L^G)| = [L : L^G] \leq |G| \qquad \square$$

Ergänzende Übung 4.1.12. Ist L/K eine algebraische, aber nicht notwendig endliche Körpererweiterung und $G \subset \mathrm{Gal}(L/K)$ eine beliebige Untergruppe, so ist L/L^G immer noch eine Galoiserweiterung, deren Galoisgruppe jedoch nicht mit G übereinzustimmen braucht. Zum Beispiel erzeugt der Frobenius-Homomorphismus nicht die Galoisgruppe $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$, aber der Fixkörper seines Erzeugnisses ist dennoch $\mathbb{F}_p$.

Satz 4.1.13 (Charakterisierungen endlicher Galoiserweiterungen). *Sei L/K eine endliche Körpererweiterung und $G = \mathrm{Gal}(L/K)$ ihre Galoisgruppe. So sind gleichbedeutend:*

1. *L/K ist eine Galoiserweiterung.*
2. *Die Ordnung der Galoisgruppe stimmt überein mit dem Grad der Körpererweiterung, in Formeln $|G| = [L : K]$.*
3. *Der Unterkörper K stimmt mit dem Fixkörper der Galoisgruppe überein, in Formeln $K = L^G$.*

Beweis. $1 \Rightarrow 2$ war 4.1.9. Die Implikation $2 \Rightarrow 3$ folgt durch Dimensionsvergleich daraus, daß wir $|G| = [L : L^G]$ ja bereits nach 4.1.11 wissen. $3 \Rightarrow 1$ folgt direkt aus 4.1.11. □

Ergänzung 4.1.14. Auch für eine beliebige algebraische Körpererweiterung gilt noch, daß sie genau dann Galois ist, wenn der Unterkörper der Fixkörper der Galoisgruppe ist. Hier folgt die eine Implikation aus 4.1.12, und die andere aus 3.7.9.

Übung 4.1.15. Unter der Voraussetzung $\operatorname{char} K \neq 2$ ist jede quadratische Körpererweiterung L von K Galois mit Galoisgruppe $\mathbb{Z}/2\mathbb{Z}$, und die Elemente $\alpha \in L \backslash K$ mit $\alpha^2 \in K$ sind genau diejenigen von Null verschiedenen Elemente von L, die vom nichttrivialen Element der Galoisgruppe auf ihr Negatives geschickt werden.

Definition 4.1.16. Eine Wirkung einer Gruppe auf einer Menge heißt **treu** genau dann, wenn nur das neutrale Element jedes Element der Menge festhält.

4.1.17. Wir erinnern aus II.8.1.6.6, daß eine Wirkung einer Gruppe auf einer Menge transitiv heißt genau dann, wenn unsere Menge nicht leer ist und je zwei ihrer Elemente durch ein geeignetes Gruppenelement ineinander überführt werden können.

Satz 4.1.18 (Operation der Galoisgruppe auf Nullstellen). *Sei K ein Körper. Ist $P \in K[X]$ ein* irreduzibles *Polynom und L/K sein Zerfällungskörper, so operiert die Galoisgruppe $\operatorname{Gal}(L/K)$ auf der Menge $\{\alpha \in L \mid P(\alpha) = 0\}$ der Nullstellen von P in L treu und transitiv.*

Beweis. Dem Leser zur Übung überlassen. Hinweis: 3.5.9 und 3.5.12. □

4.1.19. Die Grundfrage der Galoistheorie ist, welche Permutationen der Nullstellenmenge eines vorgegebenen irreduziblen Polynoms denn nun von einem Automorphismus seines Zerfällungskörpers oder genauer von einem Element der Galoisgruppe herkommen. Hierzu gebe ich gleich zwei Beispiele.

Beispiel 4.1.20. Ist L der Zerfällungskörper von $X^3 - 2$ über $\mathbb{Q}$, so kommen alle Permutationen der Nullstellenmenge unseres Polynoms von Elementen der Galoisgruppe her und wir haben folglich $\operatorname{Gal}(L/\mathbb{Q}) \cong \mathcal{S}_3$. In der Tat ist $L/\mathbb{Q}$ normal als Zerfällungskörper und sogar Galois, da in Charakteristik Null jede Körpererweiterung separabel ist. Damit folgt insbesondere $[L : \mathbb{Q}] = |\operatorname{Gal}(L/\mathbb{Q})|$. Jetzt realisieren wir L als einen Teilkörper

$$L = \mathbb{Q}(\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}) \subset \mathbb{C}$$

der komplexen Zahlen, mit $\sqrt[3]{2} \in \mathbb{R}$ der reellen dritten Wurzel von 2 und $\zeta = \exp(2\pi\,\mathrm{i}\,/3)$ einer dritten Einheitswurzel. Diese Darstellung zeigt $L \neq \mathbb{Q}(\sqrt[3]{2})$,

da ja unser L nicht in $\mathbb{R}$ enthalten ist. In $\mathbb{Q}(\sqrt[3]{2})[X]$ zerfällt unser Polynom X^3-2 also in einen linearen und einen irreduziblen quadratischen Faktor, folglich ist L eine quadratische Erweiterung von $\mathbb{Q}(\sqrt[3]{2})$. Zusammen ergibt sich $[L:\mathbb{Q}] = 6$ und mithin $|\operatorname{Gal}(L/\mathbb{Q})| = 6$. Die Operation von $\operatorname{Gal}(L/\mathbb{Q})$ auf der Menge $\{\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}\}$ definiert nun nach 4.1.18 eine Einbettung $\operatorname{Gal}(L/\mathbb{Q}) \hookrightarrow \mathcal{S}_3$, und da beide Seiten gleichviele Elemente haben, muß diese Einbettung ein Isomorphismus sein.

Beispiel 4.1.21. Ist L der Zerfällungskörper von X^3+X^2-2X-1 über $\mathbb{Q}$, so kommen genau die zyklischen Permutationen der Nullstellenmenge unseres Polynoms von Elementen der Galoisgruppe her und wir haben folglich $\operatorname{Gal}(L/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$. In der Tat können wir mit $\zeta = \exp(2\pi\,\mathrm{i}\,/7)$ einer siebten Einheitswurzel die drei komplexen Nullstellen unseres Polynoms schreiben als $\alpha = \zeta + \bar{\zeta}$, $\beta = \zeta^2 + \bar{\zeta}^2$ sowie $\gamma = \zeta^3 + \bar{\zeta}^3$, wie man leicht nachrechnet. Ich bin im übrigen den umgekehrten Weg gegangen und habe mein Polynom aus den Linearfaktoren zu diesen drei Nullstellen zusammenmultipliziert. Wie dem auch sei besitzt unser Polynom keine ganzzahligen Nullstellen und ist nach II.2.5.31 also irreduzibel über $\mathbb{Q}$. Unsere Nullstellen erfüllen nun jedoch die Relationen $\alpha^2 = \beta + 2$, $\beta^2 = \gamma + 2$ und $\gamma^2 = \alpha + 2$, woraus unmittelbar die Behauptung folgt. In 4.8.6 geben wir im übrigen ein Kriterium an, das es erlaubt, die Galoisgruppe einer kubischen Gleichung ganz mechanisch zu bestimmen.

Ergänzende Übung 4.1.22. Jede normale Körpererweiterung mit trivialer Galoisgruppe ist rein inseparabel. Für jede normale Körpererweiterung K/k mit Galoisgruppe G ist K^G/k rein inseparabel. Hinweis: Im Fall unendlicher Erweiterungen verwende man 3.7.8.

Übung 4.1.23. Man bestimme die Galoisgruppe des Zerfällungskörpers von X^4-5 über $\mathbb{Q}$ und über $\mathbb{Q}[\mathrm{i}]$.

Proposition 4.1.24. *Operiert eine endliche Gruppe G auf einem kommutativen Integritätsbereich R, so definiert die offensichtliche Einbettung einen Isomorphismus*

$$\operatorname{Quot}(R^G) \xrightarrow{\sim} (\operatorname{Quot} R)^G$$

des Quotientenkörpers seines Invariantenrings mit den Invarianten seines Quotientenkörpers.

Beweis. Jeden Bruch $f/h \in (\operatorname{Quot} R)^G$ können wir mit $\prod_{\sigma\in G\setminus 1}\sigma(h)$ erweitern zu einem Bruch, dessen Nenner in R^G liegt, da er ja das Produkt aller $\sigma(h)$ mit $\sigma \in G$ ist und bei diesem Produkt zwar die Faktoren von der Gruppenoperation permutiert werden, das Produkt als Ganzes jedoch invariant bleibt. So ein Bruch kann aber nur dann G-invariant sein, wenn auch sein Zähler in R^G liegt. □

Beispiel 4.1.25. Für jeden Körper k ist also nach 4.1.11 in den Notationen von 2.7.7 die Erweiterung

$$k('s_1, \ldots, s_n) = k('X_1, \ldots, X_n)^{\mathcal{S}_n} \subset k('X_1, \ldots, X_n)$$

eine Galoiserweiterung mit Galoisgruppe $\mathcal{S}_n$. Unsere Erweiterung ist natürlich auch ein Zerfällungskörper der **allgemeinen Gleichung**

$$T^n + s_1 T^{n-1} + \ldots + s_{n-1} T + s_n$$

wo wir die s_i schlicht als algebraisch unabhängige Variablen des Funktionenkörpers $k('s_1, \ldots, s_n)$ über k auffassen. Nach unserer Konvention sollten wir hier vielleicht sogar große Buchstaben vom Ende des Alphabets benutzen, zum Beispiel Y_i statt s_i. Insbesondere ist die allgemeine Gleichung irreduzibel, da ja alle ihre Wurzeln einfach sind und zueinander konjugiert unter der Galoisgruppe. Die Irreduzibilität dieses Polynoms kann aber auch bereits aus 2.5.13 abgeleitet werden.

Ergänzende Übung 4.1.26. Man zeige, daß sich jede endliche Erweiterung eines vollkommenen Körpers zu einer endlichen Galoiserweiterung vergrößern läßt. Man zeige, daß sich wie in II.6.4.3 behauptet jeder Endomorphismus x eines endlichdimensionalen Vektorraums über einem vollkommenen Körper auf genau eine Weise zerlegen läßt als $x = x_\mathrm{s} + x_\mathrm{n}$ mit x_s halbeinfach, x_n nilpotent und $x_\mathrm{s} x_\mathrm{n} = x_\mathrm{n} x_\mathrm{s}$.

Übung 4.1.27. Man zeige, daß die Galoisgruppe der durch Adjunktion einer n-ten Wurzel von T entstehenden und meist $\mathbb{C}(\sqrt[n]{T})/\mathbb{C}(T)$ notierten Körpererweiterung des Funktionenkörpers $\mathbb{C}(T)$ zyklisch von der Ordnung n ist.

Übung 4.1.28. Man zeige: Gegeben eine Körpererweiterung L/K und zwei verschiedene normierte irreduzible Polynome in $K[X]$ kann kein Element der Galoisgruppe eine Nullstelle des einen Polynoms in eine Nullstelle des anderen Polynoms überführen.

4.2 Anschauung für die Galoisgruppe*

4.2.1. Formal ist der nun folgende Abschnitt für die logische Kohärenz dieser Vorlesung nicht von Belang. Es wird darin auch nichts bewiesen. Ich denke jedoch, daß die im folgenden erklärten Ideen bei der historischen Entwicklung der Theorie von zentraler Bedeutung waren und hoffe, daß sie Ihnen beim Verständnis helfen werden. Um die Aussage des Hauptsatzes in diesem Abschnitt zu verstehen, sollten Sie mit den Grundbegriffen der Theorie topologischer Räume vertraut sein, wie sie etwa in der Analysis **??** erklärt wurden. Weiter benötigen Sie Grundkenntnisse über die komplexe projektive Gerade alias Riemann'sche Zahlenkugel

$\mathbb{P}^1\mathbb{C}$ im Umfang von II.8.7.3, und schließlich die Sprache der Kategorientheorie, insbesondere den Begriff einer Äquivalenz von Kategorien II.10.2.20.

4.2.2. Für jede Menge Z und jeden Ring k wurde in II.2.8.5 der Ring $\mathrm{Ensf}(Z,k)$ der fast überall definierten Funktionen auf Z mit Werten in k erklärt. Für jede Abbildung $f : Y \to Z$ mit endlichen Fasern liefert das Vorschalten von f einen Ringhomomorphismus $(\circ f) : \mathrm{Ensf}(Z,k) \to \mathrm{Ensf}(Y,k)$ in die Gegenrichtung, das **Zurückholen**.

4.2.3. Gegeben ein topologischer Raum Z erklären wir feiner auch den Teilring $\mathrm{Topf}(Z) \subset \mathrm{Ensf}(Z,\mathbb{C})$ der fast überall definierten stetigen komplexwertigen Funktionen. Ich meine damit fast überall definierte Funktionen, die durch eine auf dem Komplement einer endlichen Menge stetige Funktion repräsentiert werden können. Für jede stetige Abbildung $f : Y \to Z$ mit endlichen Fasern liefert das Vorschalten von f auch einen Ringhomomorphismus $(\circ f) : \mathrm{Topf}(Z) \to \mathrm{Topf}(Y)$ in die Gegenrichtung, das **Zurückholen** fast überall definierter stetiger Funktionen.

Definition 4.2.4. Wir verstehen unter einer **endlichen verzweigten Überlagerung der Riemann'schen Zahlenkugel** $\mathbb{P}^1\mathbb{C}$ eine stetige Abbildung $p : Z \to \mathbb{P}^1\mathbb{C}$ von einem kompakten Hausdorffraum Z nach $\mathbb{P}^1\mathbb{C}$ derart, daß es für jeden Punkt $z \in Z$ einen **Verzweigungsindex** $n = n(z) \in \mathbb{N}_{\geq 1}$ und ein kommutatives Diagramm von punktierten topologischen Räumen

$$\begin{array}{ccc} u & \in & (\mathbb{C},0) \hookrightarrow (Z,z) \\ \downarrow & & \downarrow \quad \downarrow p \\ u^n & \in & (\mathbb{C},0) \hookrightarrow (\mathbb{P}^1\mathbb{C}, p(z)) \end{array}$$

gibt mit offenen stetigen injektiven Horizontalen. Unter einem punktierten Raum verstehen wir hierbei einen Raum mit einem ausgezeichneten Punkt, und unter einem Morphismus von punktierten Räumen eine stetige Abbildung, die den ausgezeichneten Punkt in den ausgezeichneten Punkt überführt. Eine offene Abbildung von topologischen Räumen schließlich ist eine Abbildung, unter der das Bild jeder offenen Menge wieder offen ist.

4.2.5. Man erkennt unschwer, daß gegeben eine endliche verzweigte Überlagerung der Riemann'schen Zahlenkugel $p : Z \to \mathbb{P}^1\mathbb{C}$ der Verzweigungsindex an jeder Stelle $z \in Z$ wohldefiniert ist, daß er nur für höchstens endlich viele Punkte aus Z echt größer als Eins sein kann, und daß die Summe der Verzweigungsindizes über alle Punkte einer gegebenen Faser der Projektion p nicht von der Wahl der Faser abhängt. Diese Zahl heißt dann die **Blätterzahl** unserer verzweigten Überlagerung.

Dies Bild kam bereits in II.2.1.6 vor als Illustration für die Abbildung $z \mapsto z^2$ der komplexen Zahlenebene auf sich selbst. Es illustriert damit auch die lokale Struktur einer verzweigten Überlagerung in einer Umgebung einer Stelle x mit Verzeigungsindex $n(x) = 2$. Der Begriff der Verzweigung kommt wohl vom reellen Bild her, wenn man bei einem Polynom mit $(\mathbb{R}[T])[X]$ in zwei Veränderlichen untersucht, wie die Nullstellen als Polynom in X abhängen vom Wert von T. Mehrfache Nullstellen werden sich beim Wackeln an T oft in mehrere einfache Nullstellen trennen alias verzweigen, und das ist die Vorstellung, die dem Begriff der Verzweigung zugrundeliegt. Zum Beispiel hat $X^2 - T$ bei $T = 0$ eine doppelte reelle Nullstelle, die sich beim Verwackeln zu $T > 0$ in zwei reelle Nullstellen trennt, während sie beim Verwackeln zu $T < 0$ im Reellen nicht mehr zu sehen ist und sich in zwei rein imaginäre Nullstellen trennt. Wie sich die komplexen Nullstellen beim Bewegen von T in der komplexen Ebene verhalten, illustriert das obige Bild.

4.2.6. Gegeben eine verzweigte Überlagerung $p : Z \to \mathbb{P}^1\mathbb{C}$ betrachten wir im Ring $\mathrm{Topf}(Z)$ der fast überall definierten stetigen komplexwertigen Funktionen auf Z die Teilmenge

$$\mathcal{M}(Z) := \{\alpha \in \mathrm{Topf}(Z) \mid \text{Es gibt } P \in \mathbb{C}(T)[X] \text{ mit } P \neq 0 \text{ aber } P(\alpha) = 0\}$$

Beim Auswerten unseres Polynoms P auf der fast überall definierten Funktion α legen wir die Einbettungen

$$\mathbb{C}(T) \hookrightarrow \mathrm{Topf}(\mathbb{C}) \xleftarrow{\sim} \mathrm{Topf}(\mathbb{P}^1\mathbb{C}) \hookrightarrow \mathrm{Topf}(Z)$$

zugrunde, wobei der mittlere Isomorphismus durch das Zurückholen mit der üblichen Einbettung $\mathbb{C} \subset \mathbb{P}^1\mathbb{C}$ gegeben wird und die letzte Einbettung durch das Zurückholen mit unserer Projektion p.

Vorschau 4.2.7. In der Terminologie **??** hieße $\mathcal{M}(Z)$ der "ganze Abschluß von $\mathbb{C}(T)$ in $\mathrm{Topf}(Z)$". Dort wird auch gezeigt, daß solch ein ganzer Abschluß stets ein Teilring ist.

Satz 4.2.8 (Körpererweiterungen und Topologie). *1. Gegeben eine zusammenhängende endliche verzweigte Überlagerung $p : Z \to \mathbb{P}^1\mathbb{C}$ der Riemann'schen Zahlenkugel ist die Teilmenge $\mathcal{M}(Z) \subset \mathrm{Topf}(Z)$ ein Teilring und sogar ein Körper.*

2. *Ist $q : Y \to \mathbb{P}^1\mathbb{C}$ eine weitere endliche verzweigte Überlagerung der Riemann'schen Zahlenkugel und $f : Y \to Z$ ein "Morphismus von Überlagerungen" alias eine stetige Abbildung mit $p \circ f = q$, so induziert das Zurückholen mit f einen Ringhomomorphismus $\mathcal{M}(Z) \to \mathcal{M}(Y)$.*

3. *Der Funktor $Z \mapsto \mathcal{M}(Z)$ ist eine Äquivalenz von Kategorien*

$$\left\{\begin{array}{c}\textit{Endliche verzweigte}\\ \textit{zusammenhängende}\\ \textit{Überlagerungen von } \mathbb{P}^1\mathbb{C}\end{array}\right\} \xrightarrow{\sim} \left\{\begin{array}{c}\textit{Endliche}\\ \textit{Köpererweiterungen}\\ \textit{von } \mathbb{C}(T)\end{array}\right\}^{\mathrm{opp}}$$

4.2.9. Wir zeigen diesen Satz hier nicht. Der Schlüssel zum Beweis ist die Theorie der sogenannten "Riemann'schen Flächen". Im Rahmen dieser Theorie zeigt man feiner, daß es für jede endliche verzweigte Überlagerung $Z \to \mathbb{P}^1\mathbb{C}$ genau eine Struktur als Riemann'sche Fläche auf dem topologischen Raum Z gibt derart, daß unsere Überlagerungsabbildung ein Morphismus von Riemann'schen Flächen wird. Weiter zeigt man, daß unser $\mathcal{M}(Z)$ dann genau der Ring der "meromorphen Funktionen" auf Z ist, und daß dieser Ring im Fall von zusammenhängendem Z ein Körper ist.

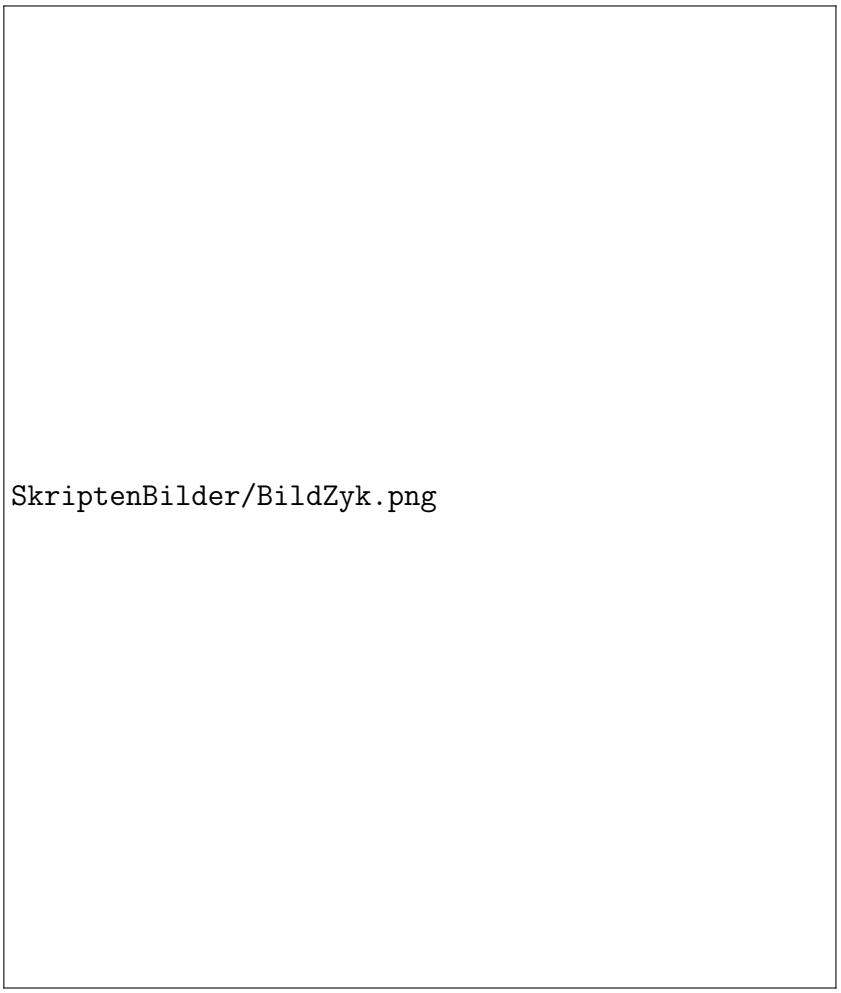
Beispiel 4.2.10. Das Adjungieren einer n-ten Wurzel U aus T zu $\mathbb{C}(T)$, also die Körpererweiterung $\mathbb{C}(T) \hookrightarrow \mathbb{C}(U)$ mit $T \mapsto U^n$, entspricht der verzweigten Überlagerung $p : Z = \mathbb{P}^1\mathbb{C} \to \mathbb{P}^1\mathbb{C}$ mit $p(z) = z^n$ für $z \in \mathbb{C} \subset \mathbb{P}^1\mathbb{C}$ und $p(\infty) = \infty$. Das ist eine verzweigte n-blättrige Überlagerung, die nur bei 0 und ∞ verzweigt und dort jeweils den Verzweigungsindex n hat. Die Galoisgruppe ist in diesem Fall nach 4.1.27 isomorph zur zyklischen Gruppe der n-ten komplexen Einheitswurzeln. Genauer erhalten wir einen derartigen Isomorphismus, indem wir jeder n-te Einheitswurzel ζ den Automorphismus $\mathbb{C}(U) \xrightarrow{\sim} \mathbb{C}(U)$, $U \mapsto \zeta U$ zuordnen. Das sollte im Lichte unseres Satzes nun auch anschaulich klar sein.

4.2.11. Ganz allgemein heißt eine stetige Abbildung $p : Z \to B$ von topologischen Räumen eine **Überlagerung** oder genauer eine **unverzweigte Überlagerung** genau dann, wenn jeder Punkt $b \in B$ eine offene Umgebung U besitzt derart, daß $p^{-1}(U)$ eine disjunkte Zerlegung in offene Teilmengen $p^{-1}(U) = \bigsqcup_{i\in I} U_i$ zuläßt, die von p jeweils homöomorph auf U abgebildet werden, für die also $p : U_i \to U$ stets eine Bijektion mit stetiger Umkehrabbildung ist. Ist $q : Y \to B$ eine weitere Überlagerung, so versteht man unter einem "Morphismus von Überlagerungen" oder auch einer **Decktransformation** eine stetige Abbildung $f : Z \to Y$ mit $q \circ f = p$. Eine **endliche Überlagerung** ist eine Überlagerung mit endlichen Fasern. Man kann nun zeigen und es ist hoffentlich auch anschaulich einleuchtend, daß wir für jede endliche Teilmenge $E \subset \mathbb{P}^1\mathbb{C}$ durch Einschränken von Überlagerungen eine Äquivalenz von Kategorien

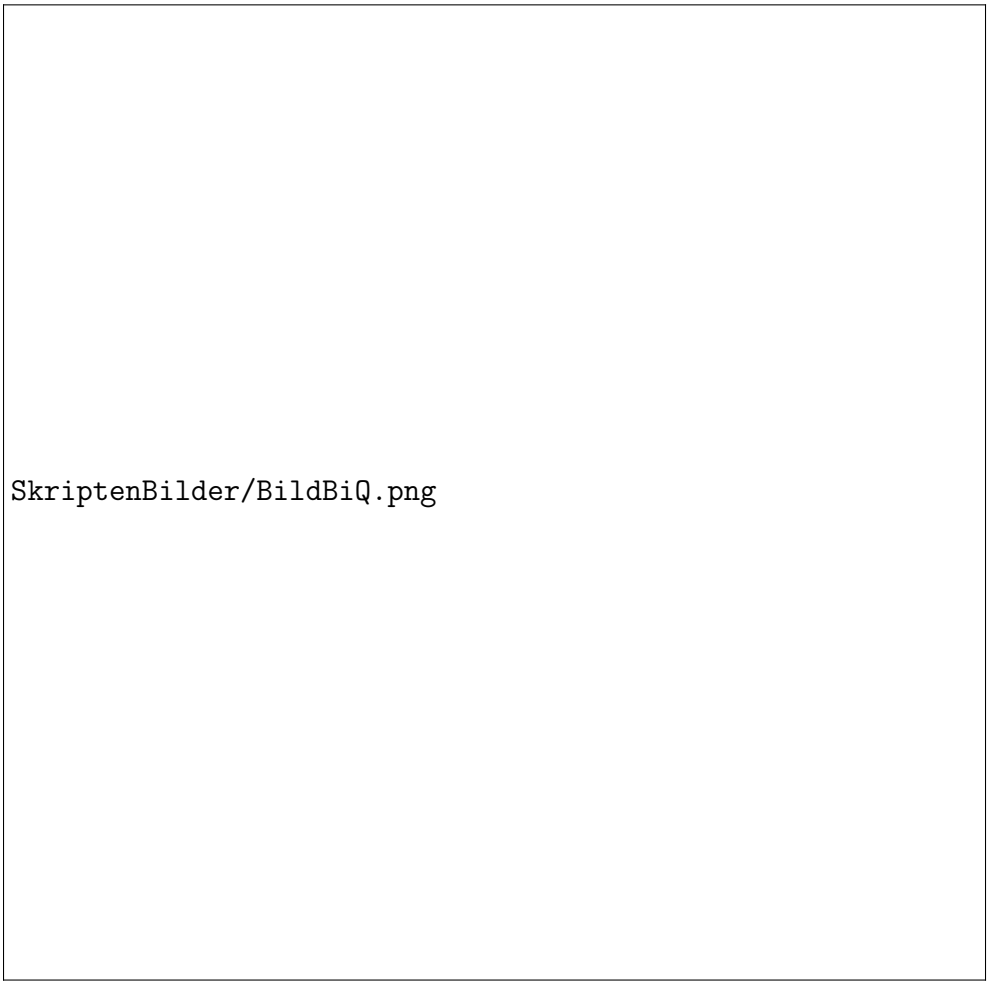
$$\begin{array}{ccc} \left\{\begin{array}{c}\text{Endliche verzweigte}\\ \text{zusammenhängende}\\ \text{Überlagerungen von } \mathbb{P}^1\mathbb{C} \text{ ohne}\\ \text{Verzweigungspunkte über } E\end{array}\right\} & \xrightarrow{\sim} & \left\{\begin{array}{c}\text{Endliche unverzweigte}\\ \text{zusammenhängende}\\ \text{Überlagerungen von}\\ \mathbb{P}^1\mathbb{C}\backslash E\end{array}\right\} \\ (p : Z \to \mathbb{P}^1\mathbb{C}) & \mapsto & (p : Z\backslash p^{-1}(E) \to \mathbb{P}^1\mathbb{C}\backslash E) \end{array}$$

erhalten. Den quasiinversen Funktor nenne ich das **Fortsetzen zu einer verzweigten Überlagerung von** $\mathbb{P}^1\mathbb{C}$.

4.2.12. Um Bilder von Überlagerungen zu zeichnen und so die Galoisgruppe anschaulich zu machen, ist es oft praktisch, für eine gegebene endliche Teilmenge $E \subset \mathbb{P}^1\mathbb{C}$ der Riemann'schen Zahlenkugel eine Teilmenge $S \subset \mathbb{C}\backslash E$ ihres Komplements zu wählen, die salopp gesprochen entsteht, indem wir um jeden unserer Punkte $e \in E$ mit einer Ausnahme—im Fall $\infty \in E$ der Ausnahme ∞—einen kleinen Kreis zeichnen, und jeden dieser kleinen Kreise mit einem festen weiteren Punkt so verbinden, daß diese ganzen Verbindungswege sich untereinander und mit unseren kleinen Kreisen nie kreuzen. Haben wir S in dieser Art gewählt, so erhalten wir durch Restriktion auf S eine weitere Äquivalenz von Kategorien



Anschauung für die durch Adjunktion einer dritten Wurzel aus T entstehenden Körpererweiterung des Funktionenkörpers $\mathbb{C}(T)$ nach 4.2.12. Ich finde, man sieht in diesem Fall auch recht anschaulich, daß die Galoisgruppe zyklisch von der Ordnung drei sein muß.



Eine Überlagerung mit drei Verzweigungspunkten, davon je einer im rechten und einer im linken Kreis. Zu sehen ist die Menge S und ihre Überlagerung. Die Galoisgruppe ist die Gruppe der Decktransformationen dieser Überlagerung in sich selber, in diesem Fall die Klein'sche Vierergruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$$\begin{array}{ccc} \left\{\begin{array}{c}\text{Endliche unverzweigte}\\ \text{zusammenhängende}\\ \text{Überlagerungen von}\\ \mathbb{P}^1\mathbb{C}\backslash E\end{array}\right\} & \xrightarrow{\sim} & \left\{\begin{array}{c}\text{Endliche unverzweigte}\\ \text{zusammenhängende}\\ \text{Überlagerungen von}\\ S\end{array}\right\} \\ (p: Z \to \mathbb{P}^1\mathbb{C}\backslash E) & \mapsto & (p: p^{-1}(S) \to S) \end{array}$$

Formal folgt das aus der "Homotopieinvarianz der Kategorie der Überlagerungen" **??** oder etwas weniger direkt mit der "Homotopieinvarianz der Fundamentalgruppe" **??** aus dem "Satz über den Faserfunktor" **??**. Die Überlagerungen von derartigen Mengen S lassen sich nun sehr viel besser zeichnen, und ihre Automorphismengruppen, die ja unter unserer Äquivalenz von Kategorien gewissen Galoisgruppen entsprechen, sind auch zumindest in kleinen Fällen der Anschauung noch gut zugänglich.

Vorschau 4.2.13. Ich will noch skizzieren, wie man in 4.2.8 zumindest auf Objekten einen quasiinversen Funktor konstruieren kann. Der Satz vom primitiven Element 4.3.3 wird uns bald sagen, daß jede endliche Körpererweiterung von $\mathbb{C}(T)$ primitiv ist. Gegeben eine primitive algebraische Körpererweiterung $\mathbb{C}(T)(\alpha)$ von $\mathbb{C}(T)$ betrachten wir nun das Minimalpolynom $P \in \mathbb{C}(T)[X]$ von α. Wir schreiben es

$$P = X^n + a_{n-1}X^{n-1} + \ldots + a_0$$

mit $a_i \in \mathbb{C}(T)$. Es gibt sicher $E \subset \mathbb{C}$ endlich derart, daß alle Koeffizienten a_i unseres Minimalpolynoms auf $\mathbb{C}\backslash E$ wohldefinierte komplexwertige Funktionen sind. Die Menge F der Punkte $q \in \mathbb{C}\backslash E$ derart, daß das zu q spezialisierte Polynom

$$P_q := X^n + a_{n-1}(q)X^{n-1} + \ldots + a_0(q) \in \mathbb{C}[X]$$

mehrfache Nullstellen hat, muß nun auch endlich sein: In der Tat ist nämlich P teilerfremd zu seiner Ableitung P' nach X und folglich existiert in $\mathbb{C}(T)[X]$ eine Darstellung $1 = HP + KP'$ mit $H, K \in \mathbb{C}(T)[X]$. An den Stellen $q \in \mathbb{C}\backslash E$, an denen die Koeffizienten von H und K wohldefinierte komplexwertige Funktionen sind, können dann P_q und P'_q keine gemeinsame Nullstelle haben. In dieser Situation kann man zeigen, daß die Projektion auf die zweite Koordinate von

$$Z := \{(z, q) \in \mathbb{C} \times (\mathbb{C}\backslash(E \cup F)) \mid P_q(z) = 0\}$$

auf $\mathbb{C}\backslash(E \cup F)$ eine zusammenhängende unverzweigte endliche Überlagerung ist. Deren Fortsetzung zu einer verzweigten Überlagerung von $\mathbb{P}^1\mathbb{C}$ entspricht dann unserer Körpererweiterung $\mathbb{C}(T)(\alpha) \supset \mathbb{C}(T)$ unter der Äquivalenz von Kategorien aus 4.2.8.

4.3 Satz vom primitiven Element

Lemma 4.3.1. *Ein affiner Raum über einem unendlichen Körper kann nicht durch endlich viele echte affine Teilräume überdeckt werden.*

4.3.2. In anderen Worten ausgedrückt soll das heißen, daß ein affiner Raum über einem unendlichen Körper nie die Vereinigung endlich vieler echter affiner Teilräume sein kann.

Beweis. Wir dürfen annehmen, daß unter unseren Teilräumen keiner in einem anderen enthalten ist. Wir argumentieren nun mit Induktion über die Zahl unserer affinen Teilräume und nehmen als Induktionsbasis den Fall, daß unsere endliche Menge von Teilräumen leer ist. Ist sonst H einer unserer Teilräume, so finden wir mit Induktion einen Punkt $e \in H$, der in keinem anderen unserer Teilräume liegt. Nehmen wir nun eine Gerade durch diesen Punkt, die auch in H nicht enthalten ist, so trifft diese Gerade jeden unserer Teilräume in höchstens einem Punkt, hat aber selbst unendlich viele Punkte. □

Satz 4.3.3 (vom primitiven Element). *Ist L/K eine endliche separable Körpererweiterung, so gibt es ein Element $\alpha \in L$ mit $L = K(\alpha)$.*

Beweis. Da die multiplikative Gruppe jedes endlichen Körpers nach II.7.3.28 zyklisch ist, dürfen wir ohne Beschränkung der Allgemeinheit K unendlich annehmen. Nach 3.5.22 können wir L vergrößern zu einer normalen Erweiterung N von K. Wegen der Separabilität von L/K gibt es dann nach 3.6.17 genau $[L : K]$ Körperhomomorphismen über K von L nach N, in Formeln

$$|\mathrm{Ring}^K(L, N)| = [L : K]$$

Nach 4.3.1 gibt es Elemente $\alpha \in L$ derart, daß die $\sigma(\alpha)$ für $\sigma \in \mathrm{Ring}^K(L, N)$ paarweise verschieden sind, da sonst die Teilräume $\ker(\sigma - \tau) \subset L$ für $\sigma \neq \tau \in |\mathrm{Ring}^K(L, N)|$, die ja echte K-Untervektorräume von L sind, bereits ganz L überdecken müßten. Für jedes solches α liefert die Restriktion natürlich eine Injektion $\mathrm{Ring}^K(L, N) \hookrightarrow \mathrm{Ring}^K(K(\alpha), N)$, denn verschiedene $\sigma \neq \tau$ links bilden auch schon unser α auf verschiedene Elemente von N ab. Die Identität $L = K(\alpha)$ folgt dann aus der Kette von Gleichungen und Ungleichungen $[L : K] = |\mathrm{Ring}^K(L, N)| \leq |\mathrm{Ring}^K(K(\alpha), N)| = [K(\alpha) : K]$, bei der die Gleichungen aus 3.6.17 folgen. □

Ergänzung 4.3.4. Ist L/K eine endliche Galois-Erweiterung, so ist $\alpha \in L$ nach 4.1.13 ein primitives Element genau dann, wenn es von keinem Element der Galoisgruppe festgehalten wird. Wir können sogar stets ein $\alpha \in L$ so wählen, daß es mit seinen Galois-Konjugierten eine K-Basis von L bildet: Das sagt uns der “Satz

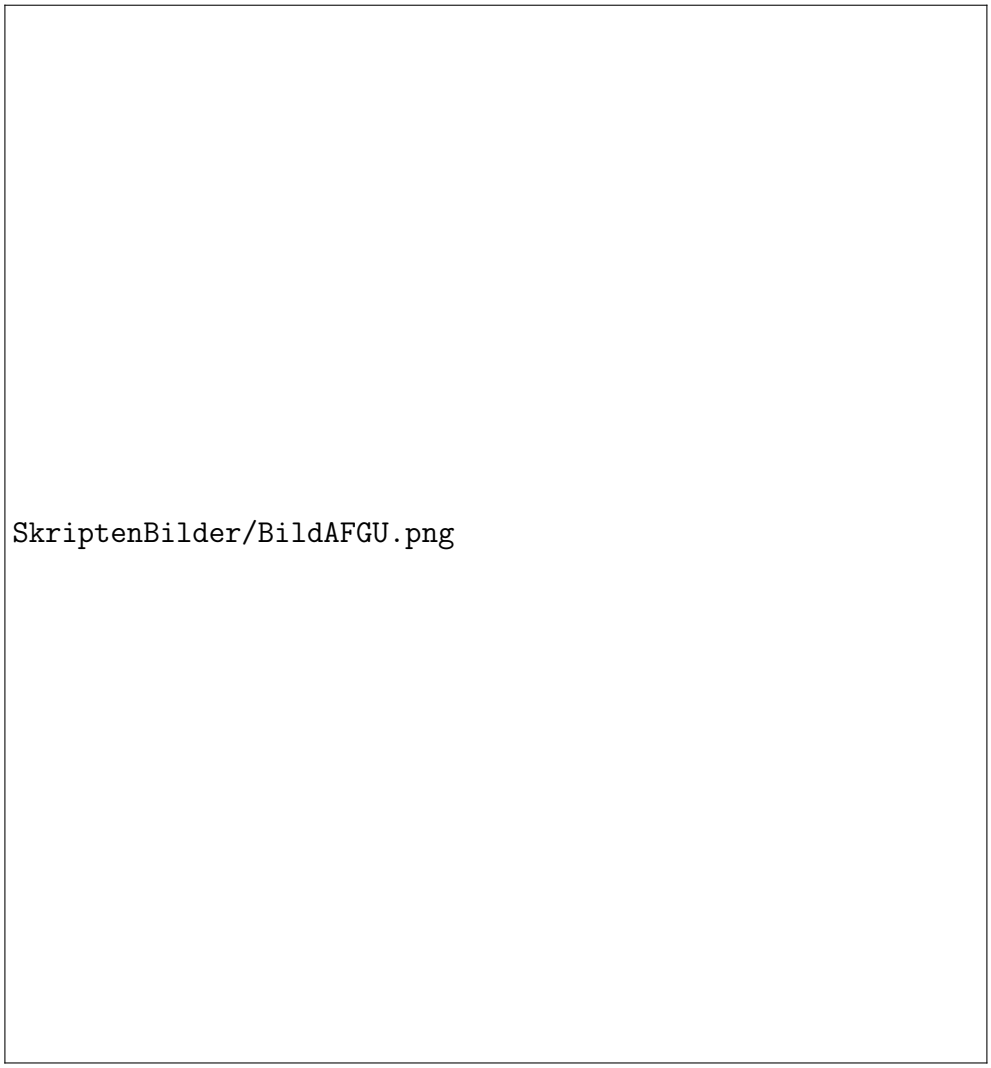


Illustration zum Beweis von 4.3.1

von der Normalbasis", für dessen Beweis ich auf [Lor96] verweise. Diese schärfere Aussage stimmt keineswegs für jedes primitive Element, wie das Beispiel $L = \mathbb{C}$, $K = \mathbb{R}$, $\alpha = \mathrm{i}$ zeigt.

4.4 Galoiskorrespondenz

Satz 4.4.1 (Galoiskorrespondenz). *Gegeben eine endliche Galoiserweiterung L/K mit Galoisgruppe $G = \mathrm{Gal}(L/K)$ haben wir eine inklusionsumkehrende Bijektion*

$$\left\{\begin{array}{c}\textit{Zwischenkörper } M\\ \textit{der Körpererweiterung}\\ K \subset M \subset L\end{array}\right\} \overset{\sim}{\leftrightarrow} \left\{\begin{array}{c}\textit{Untergruppen } H\\ \textit{der Galoisgruppe}\\ H \subset G\end{array}\right\}$$

$$\begin{array}{ccc} M & \overset{\phi}{\mapsto} & \mathrm{Gal}(L/M) \\ L^H & \overset{\psi}{\mapsfrom} & H \end{array}$$

Unter dieser Bijektion entsprechen die Normalteiler H von G genau denjenigen Zwischenkörpern M, die normal sind über K, und in diesen Fällen definiert das Einschränken von Elementen der Galoisgruppe einen Isomomorphismus von Gruppen $G/H \xrightarrow{\sim} \mathrm{Gal}(L^H/K)$ alias eine kurze exakte Sequenz

$$\mathrm{Gal}(L/M) \hookrightarrow \mathrm{Gal}(L/K) \twoheadrightarrow \mathrm{Gal}(M/K)$$

Ergänzung 4.4.2. In der Sprache der Kategorientheorie nimmt diese Aussage die folgende Form an: Ist L/K eine endliche Galoiserweiterung mit Galoisgruppe G, so liefert Funktor $\mathrm{Kring}^K(\ , L)$ der K-linearen Körperhomomorphismen nach L eine Äquivalenz von Kategorien

$$\left\{\begin{array}{l}\text{Körpererweiterungen von } K,\\ \text{die sich in } L \text{ einbetten lassen}\end{array}\right\} \xrightarrow{\sim} \{\text{transitive } G\text{-Mengen}\}^{\mathrm{opp}}$$

Beweis. Nach 3.5.21 und der Definition der Separabilität 3.6.12 ist für jeden Zwischenkörper M auch L/M normal und separabel, also Galois, und damit folgt $\psi \circ \phi = \mathrm{id}$ aus unserer Erkenntnis 4.1.13, daß bei einer endlichen Galoiserweiterung der Grundkörper gerade der Fixkörper der Galoisgruppe ist. Ohne alle Schwierigkeiten folgt $\phi \circ \psi = \mathrm{id}$ aus unserer Erkenntnis 4.1.11, daß das Bilden des Fixkörpers zu einer endlichen Gruppe von Körperautomorphismen stets eine Galoiserweiterung mit besagter Gruppe als Galoisgruppe liefert. Das zeigt die erste Behauptung. Man prüft leicht $g(L^H) = L^{gHg^{-1}}$ für alle $g \in G$. In Worten entspricht unter unserer Galoiskorrespondenz also das Verschieben von Zwischenkörpern mit einem Element $g \in G$ der Konjugation von Untergruppen mit

besagtem Element $g \in G$. Insbesondere ist L^H invariant unter G genau dann, wenn H in G ein Normalteiler ist. Da aber G transitiv operiert auf den Wurzeln der Minimalpolynome aller Elemente von L, ist L^H invariant unter G genau dann, wenn es normal ist über K. Schließlich faktorisiert dann die durch Einschränken von Körperhomomorphismen gegebene Abbildung $G \to \mathrm{Gal}(L^H/K)$ über G/H und liefert eine Injektion $G/H \hookrightarrow \mathrm{Gal}(L^H/K)$, die mit einem Abzählargument bijektiv sein muß. □

Beispiel 4.4.3. Nach 4.1.6 ist für jede Potenz $q = p^r$ mit $r \geq 1$ einer Primzahl p die Galoisgruppe $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ eine zyklische Gruppe der Ordnung r, erzeugt vom Frobenius-Homomorphismus $a \mapsto a^p$. Die Untergruppen dieser Gruppe $\mathbb{Z}/\mathbb{Z}r$ sind nach II.7.3.11 genau die Gruppen $\mathbb{Z}d/\mathbb{Z}r$ für Teiler d von r. Das liefert im Lichte der Galoiskorrespondenz 4.4.1 einen neuen Beweis unserer Klassifikation 3.4.13 aller Unterkörper eines endlichen Körpers.

Definition 4.4.4. Sei $\mathrm{char}\, K \neq 2$. Eine Körpererweiterung L/K heißt **biquadratisch** genau dann, wenn sie Grad $[L : K] = 4$ hat und erzeugt ist von zwei Elementen $L = K(\alpha, \beta)$ für $\alpha, \beta \in L$ mit $\alpha^2, \beta^2 \in K$.

Beispiel 4.4.5. $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ ist biquadratisch über $\mathbb{Q}$, denn $(a + b\sqrt{5})^2 = a^2 + 2ab\sqrt{5} + 5b^2$ kann nie 3 sein, weder für $a = 0$ noch für $b = 0$ und erst recht nicht für $a \neq 0, b \neq 0$.

Lemma 4.4.6. *Jede biquadratische Erweiterung ist Galois, und ihre Galois-Gruppe ist die Klein'sche Vierergruppe* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Beweis. Für die nichttrivialen Elemente $\sigma \in \mathrm{Gal}(L/K(\alpha))$, $\tau \in \mathrm{Gal}(L/K(\beta))$ haben wir

$$\sigma : \begin{cases} \alpha & \mapsto & \alpha \\ \beta & \mapsto & -\beta \end{cases} \qquad \tau : \begin{cases} \alpha & \mapsto & -\alpha \\ \beta & \mapsto & \beta \end{cases}$$

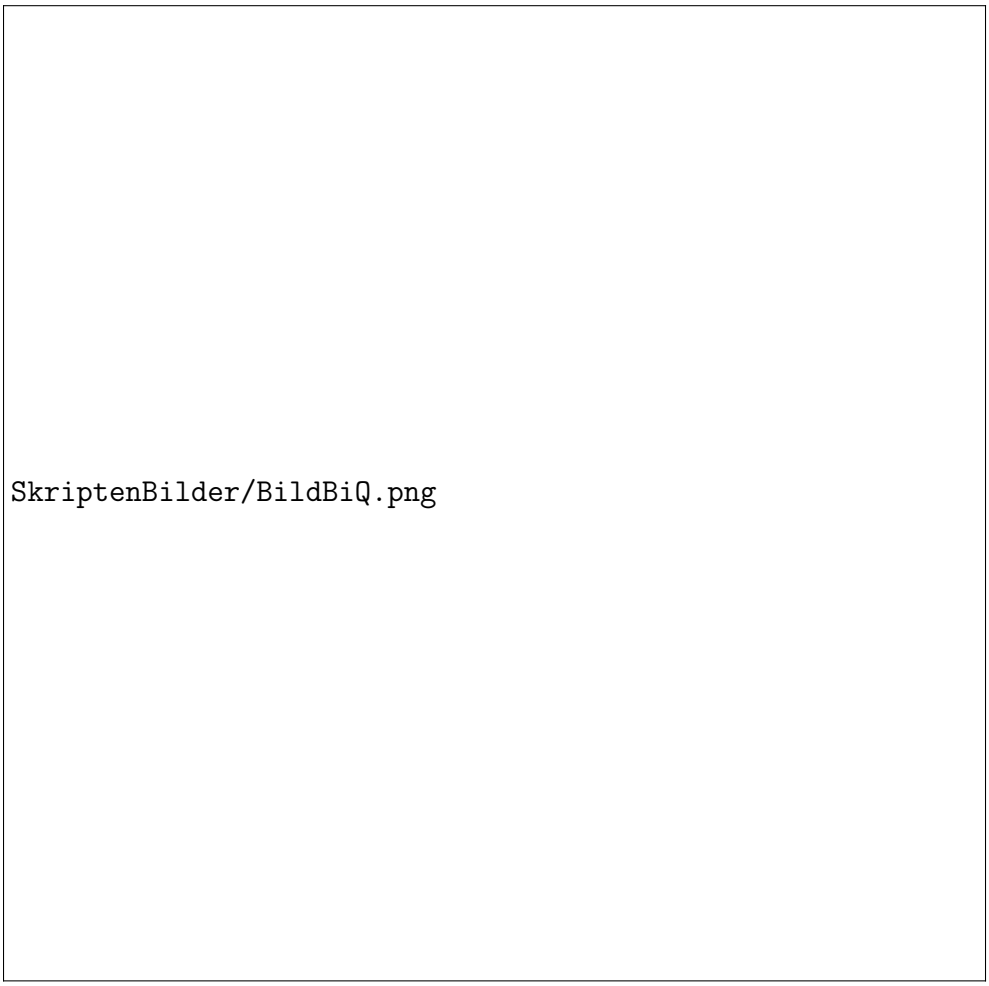
und wir haben $\{\mathrm{id}, \sigma, \tau, \sigma\tau\} \subset \mathrm{Gal}(L/K)$. Das muß dann aber schon die ganze Galois-Gruppe sein. □

4.4.7. Die Klein'sche Vierergruppe $\mathbb{F}_2^2$ hat fünf Untergruppen: Den Nullpunkt, drei Geraden und die ganze Gruppe. Sie entsprechen in unserer biquadratischen Erweiterung aus 4.4.6 den Unterkörpern

$$L \supset K(\alpha), K(\beta), K(\alpha\beta) \supset K$$

Eine K-Basis von L besteht aus $1, \alpha, \beta, \alpha\beta$, wie die simultane Eigenraumzerlegung von L unter σ und τ zeigt. Insbesondere ist $\alpha + \beta$ ein primitives Element.

Übung 4.4.8. Man drücke $\sqrt{3}$ aus als Polynom in $\sqrt{3} + \sqrt{5}$ mit rationalen Koeffizienten: Das muß möglich sein, da dies Element nach 4.4.7 primitiv ist in $\mathbb{Q}(\sqrt{3}, \sqrt{5})$.



Dies Bild ist wie in 4.2.12 zu verstehen und stellt eine biquadratische Erweiterung des Funktionenkörpers $\mathbb{C}(T)$ dar, etwa durch die Adjunktion von Quadratwurzeln aus $(T \pm 1)$, wo die beiden Punkte ± 1 in den beiden Kreisen unten zu denken sind.

Ergänzung 4.4.9. In der algebraischen Zahlentheorie können Sie lernen, warum ganz allgemein für paarweise teilerfremde natürliche Zahlen $a_1, \ldots, a_n$ die Körpererweiterung $\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n})$ über $\mathbb{Q}$ die Galoisgruppe $(\mathbb{Z}/2\mathbb{Z})^n$ hat. Daß es sich dabei um eine Galoiserweiterung handelt, sollten Sie jedoch auch hier bereits unmittelbar einsehen können.

Übung 4.4.10. Seien L/K eine endliche Körpererweiterung und $K_1, K_2 \subset L$ zwei Zwischenkörper mit K_i/K Galois und $K_1 \cap K_2 = K$. So ist auch der von K_1 und K_2 erzeugte Unterkörper $K_1K_2 \subset L$ Galois über K und es gilt $\mathrm{Gal}(K_1K_2/K) \xrightarrow{\sim} \mathrm{Gal}(K_1/K) \times \mathrm{Gal}(K_2/K)$ vermittels der Restriktionen.

Übung 4.4.11. Man zeige, daß jede endliche separable Körpererweiterung nur endlich viele Zwischenkörper besitzen kann. Man gebe eine des weiteren auch eine endliche Körpererweiterung mit unendlich vielen Zwischenkörpern an.

Satz 4.4.12 (Fundamentalsatz der Algebra). *Der Körper der komplexen Zahlen ist algebraisch abgeschlossen.*

4.4.13. Ein alternativer Beweis, der mehr Analysis und weniger Algebra verwendet, wird in **??** gegeben. Mit den Mitteln der Funktionentheorie kann man einen sehr eleganten Beweis geben, den wir in **??** erläutern. Mir persönlich gefällt der Beweis mit den Mitteln der Topologie an besten, der in **??** als Übungsaufgabe behandelt wird.

Beweis. Sei $[L : \mathbb{R}]$ eine endliche normale Erweiterung von $\mathbb{R}$, $G = \mathrm{Gal}(L/\mathbb{R})$ ihre Galoisgruppe, und $S \subset G$ eine 2-Sylow von G. So haben wir $[L : \mathbb{R}] = |G|$ und $[L : L^S] = |S|$ und folglich ist $L^S/\mathbb{R}$ eine Erweiterung von ungeradem Grad. Da jedes Polynom aus $\mathbb{R}[X]$ von ungeradem Grad nach dem Zwischenwertsatz **??** eine reelle Nullstelle hat, folgt $L^S = \mathbb{R}$. Mithin haben wir $S = G$ und G ist eine 2-Gruppe. Damit entsteht nach 1.4.10 und der Galoiskorrespondenz L aus $\mathbb{R}$ durch sukzessive Körpererweiterungen vom Grad 2, also nach 3.2.25 durch sukzessive Adjunktion von Quadratwurzeln. Adjungiert man aber eine echte Quadratwurzel zu $\mathbb{R}$, so erhält man $\mathbb{C}$, und in $\mathbb{C}$ hat jedes Element schon eine Quadratwurzel. Daraus folgt $L = \mathbb{R}$ oder $L = \mathbb{C}$. □

Übung 4.4.14. Für jeden Körper k, dessen Charakteristik kein Teiler von n ist, hat der Zerfällungskörper des Polynoms

$$T^n + a_2T^{n-2} + \ldots + a_{n-1}T + a_n$$

mit Koeffizienten im Funktionenkörper $k('a_2, \ldots, a_n)$ in $n-1$ algebraisch unabhängigen Veränderlichen als Galoisgruppe die volle symmetrische Gruppe $\mathcal{S}_n$. Hinweis: Man gehe aus von 4.1.25; Die Galoisgruppe eines Polynoms über einem Körper K ändert sich nicht unter Substitutionen des Typs $T = Y + \lambda$ für $\lambda \in K$; die Galoisgruppe ändert sich nicht beim Übergang zu Funktionenkörpern $\mathrm{Gal}(L/K) = \mathrm{Gal}(L(X)/K(X))$. Die Irreduzibilität folgt bereits aus 2.5.13.

Ergänzung 4.4.15. Bei der Behandlung kubischer Gleichungen in 4.8.4 werden wir sehen, daß auch im Fall eines Körpers k der Charakteristik drei das Polynom $T^3 + pT + q$ über $k(\!'p, q)$ die volle symmetrische Gruppe als Galoisgruppe hat. Andererseits ist im Fall eines Körpers k der Charakteristik zwei das Polynom $T^2 + p$ über $k(\!'p)$ inseparabel und seine Galoisgruppe ist trivial und ist nicht die volle symmetrische Gruppe.

4.5 Die Galoisgruppen der Kreisteilungskörper

4.5.1. Gegeben $n \geq 1$ interessieren wir uns nun für den Zerfällungskörper über $\mathbb{Q}$ des Polynoms $X^n - 1$. Dieser Zerfällungsköper heißt der n-te **Kreisteilungskörper** und wird bezeichnet mit $\mathbb{Q}(\sqrt[n]{1})$. Er ist offensichtlich normal und separabel und mithin eine Galois-Erweiterung von $\mathbb{Q}$. Ich stelle mir als n-ten Kreisteilungskörper meist konkret den Unterkörper $\mathbb{Q}(\zeta) \subset \mathbb{C}$ vor mit $\zeta = \exp(2\pi\,\mathrm{i}\,/n)$. Auch ohne Rückgriff auf den Körper der komplexen Zahlen wissen wir nach II.7.3.28, daß die n-ten Einheitswurzeln in $\mathbb{Q}(\sqrt[n]{1})$ eine zyklische Gruppe der Ordnung n bilden. Die Erzeuger dieser Gruppe heißen die **primitiven n-ten Einheitswurzeln**. Nach unserer Definition der Kreisteilungspolynome in 2.6.1 sind sie gerade die Nullstellen des n-ten Kreisteilungspolynoms

$$\Phi_n = \prod_{\mathrm{ord}\,\zeta = n} (X - \zeta)$$

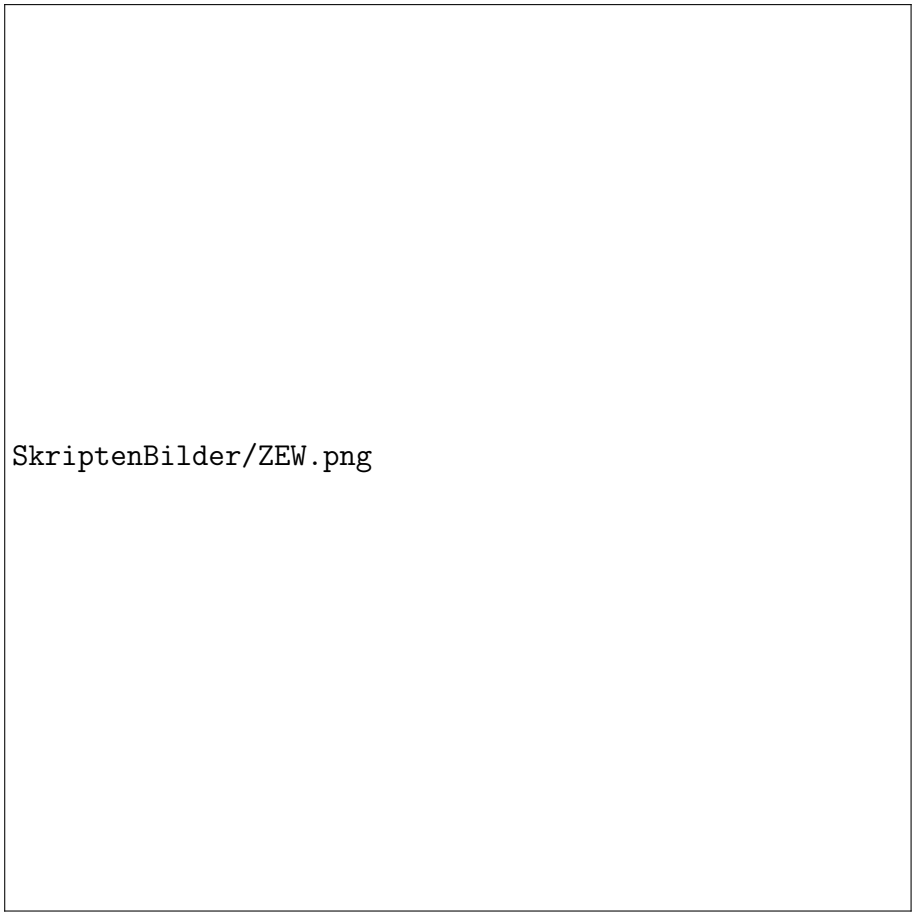
Wir hatten schon vor 2.6.4 mit Induktion über n gezeigt, daß dieses Polynom Koeffizienten in $\mathbb{Q}$ und sogar in $\mathbb{Z}$ hat, und 2.6.4 besagte, daß für $n = p$ prim das p-te Kreisteilungspolynom Φ_p irreduzibel ist in $\mathbb{Q}[X]$. Nun zeigen wir ganz allgemein, daß für alle $n \geq 1$ das n-te Kreisteilungspolynom Φ_n irreduzibel ist in $\mathbb{Q}[X]$. Nach 2.5.9 ist das ganz allgemein für normierte Polynome in $\mathbb{Z}[X]$ gleichbedeutend dazu, irreduzibel zu sein in $\mathbb{Z}[X]$.

Satz 4.5.2 (Galoisgruppen der Kreisteilungskörper). *1. Die Kreisteilungspolynome $\Phi_n(X)$ sind alle irreduzibel in $\mathbb{Q}[X]$.*

2. Bezeichnet μ_n die Gruppe der n-ten Einheitswurzeln im n-ten Kreisteilungskörper $\mathbb{Q}(\sqrt[n]{1})$ und $\mathrm{Ab}^\times(\mu_n)$ ihre Automorphismengruppe, so liefern die offensichtichen Abbildungen Isomorphismen

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[n]{1})/\mathbb{Q}) \xrightarrow{\sim} \mathrm{Ab}^\times(\mu_n) \xleftarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$$

In dieser Weise ist also die Galoisgruppe des n-ten Kreisteilungskörpers kanonisch isomorph zur Einheitengruppe des Restklassenrings $\mathbb{Z}/n\mathbb{Z}$.



Die zwölften Einheitswurzeln in $\mathbb{C}$, eingekringelt die vier primitiven zwölften Einheitswurzeln

3. *Gegeben zwei primitive n-te Einheitswurzeln $\zeta, \xi \in \mathbb{Q}(\sqrt[n]{1})$ existiert genau ein Körperhomomorphismus $\sigma : \mathbb{Q}(\sqrt[n]{1}) \to \mathbb{Q}(\sqrt[n]{1})$ mit $\sigma(\zeta) = \xi$.*

Ergänzung 4.5.3. Wählt man eine Einbettung des n-ten Kreisteilungskörpers $\mathbb{Q}(\sqrt[n]{1})$ nach $\mathbb{C}$, so ist das Bild stets der von $\mathbb{Q}$ und $\mathrm{e}^{2\pi\,\mathrm{i}/n}$ in $\mathbb{C}$ erzeugte Teilkörper. Von den Automorphismen unseres Kreisteilungskörpers läßt sich jedoch außer der Identität nur ein einziger stetig auf $\mathbb{C}$ fortsetzen, und dieser Automorphismus ist für jede Wahl der Einbettung derselbe und kann beschrieben werden als der einzige Automorphismus der Ordnung zwei oder alternativ als der Automorphismus, der jede Einheitswurzel auf ihr multiplikatives Inverses wirft.

Beweis. 1. Ist ζ eine primitive n-te Einheitswurzel, so sind alle anderen primitiven n-ten Einheitswurzeln von der Form ζ^a für $a \in \mathbb{Z}$ mit a teilerfremd zu n, in Formeln mit $\langle a, n\rangle = \langle 1\rangle$. Sei nun $\Phi_n = fg$ eine Zerlegung in $\mathbb{Z}[X]$ mit f irreduzibel. Es reicht zu zeigen, daß für jede Nullstelle $\zeta \in \mathbb{C}$ von f und $p \in \mathbb{N}$ prim mit $p \nmid n$ auch ζ^p eine Nullstelle ist von f, denn dann sind alle Wurzeln von Φ_n schon Wurzeln von f und es folgt $\Phi_n = f$. Aber sei sonst ζ eine Nullstelle von f und p prim mit $p \nmid n$ und $g(\zeta^p) = 0$. Nach 3.2.12.2 teilt dann f das Polynom $g(X^p)$, und nach Übergang zu $\mathbb{F}_p[X]$ ist $\bar f$ Teiler von $\bar g(X^p) = \bar g^p$. Dann haben aber $\bar f$ und $\bar g$ eine gemeinsame Nullstelle im Zerfällungskörper von $X^n - 1$ über $\mathbb{F}_p$, und das steht im Widerspruch dazu, daß nach 3.6.9 das Polynom $X^n - 1$ über $\mathbb{F}_p$ für $p \nmid n$ keine mehrfachen Nullstellen hat in seinem Zerfällungskörper.

2. Sicher wird $\mathbb{Q}(\sqrt[n]{1})$ erzeugt von jeder primitiven n-ten Einheitswurzel ζ, und da Φ_n nach Teil 1 ihr Minimalpolynom ist, folgt mit 3.2.12

$$[\mathbb{Q}(\sqrt[n]{1}) : \mathbb{Q}] = \deg \Phi_n = |(\mathbb{Z}/n\mathbb{Z})^\times|$$

Sicher liefert die Operation der Galoisgruppe auf den n-ten Einheitswurzeln weiter eine Einbettung $\mathrm{Gal}(\mathbb{Q}(\sqrt[n]{1})/\mathbb{Q}) \hookrightarrow \mathrm{Ab}^\times(\mu_n)$ und nach II.8.3.3 haben wir einen kanonischen Isomorphismus $(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Ab}^\times(\mu_n)$. Da diese drei Gruppen alle gleichviele Elemente haben, folgt der Satz. □

4.5.4. Es ist in diesem Zusammenhang bequem, die sogenannte **Euler'sche φ-Funktion** $\varphi : \mathbb{Z}_{\geq 1} \to \mathbb{Z}_{\geq 1}$ einzuführen. Sie wird definiert durch die Vorschrift

$$\begin{aligned}
\varphi(n) &= \text{Zahl der zu } n \text{ teilerfremden } d \in \mathbb{N} \text{ mit } 1 \leq d \leq n \\
&= \text{Zahl der Erzeuger der Gruppe } \mathbb{Z}/n\mathbb{Z} \\
&= |\{x \in \mathbb{Z}/n\mathbb{Z} \mid \mathrm{ord}(x) = n\}| \\
&= |(\mathbb{Z}/n\mathbb{Z})^\times|
\end{aligned}$$

Nach 4.5.2 haben wir also auch $\varphi(n) = \deg \Phi_n = [\mathbb{Q}(\sqrt[n]{1}) : \mathbb{Q}]$.

Satz 4.5.5 (Konstruierbarkeit regelmäßiger n-Ecke). *Genau dann ist das regelmäßige n-Eck konstruierbar mit Zirkel und Lineal, wenn der Wert $\varphi(n)$ der eben definierten Euler'schen φ-Funktion eine Zweierpotenz ist.*

Beweis. Sei ζ eine primitive n-te Einheitswurzel. Ist $\varphi(n) = [\mathbb{Q}(\zeta) : \mathbb{Q}]$ keine Zweierpotenz, so kann ζ nicht konstruierbar sein nach 3.3.4. Ist $\varphi(n)$ eine Zweierpotenz, so ist $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ eine 2-Gruppe. Nach 1.4.10 oder einfacher induktiv nach II.7.3.24 gibt es dann in G eine Kette von Normalteilern von G der Gestalt

$$G = G_r \supset G_{r-1} \supset \ldots \supset G_0 = 1$$

mit $G_i/G_{i-1} \cong \mathbb{Z}/2\mathbb{Z}$ für $1 \leq i \leq r$. Deren Fixkörper bilden dann hinwiederum eine Kette

$$\mathbb{Q} = K_r \subset K_{r-1} \subset \ldots \subset K_0 = \mathbb{Q}(\zeta)$$

von Teilkörpern mit $[K_{i-1} : K_i] = 2$ für $1 \leq i \leq r$. Diese Kette hinwiederum zeigt, daß ζ konstruierbar ist. □

Lemma 4.5.6 (zur Euler'schen φ-Funktion).

1. *Sind n und m teilerfremd, so gilt $\varphi(nm) = \varphi(n)\varphi(m)$.*
2. *Ist p prim, so gilt $\varphi(p^r) = p^{r-1}(p-1)$.*

Beweis. 1. Der Isomorphismus $\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ von Ringen induziert einen Isomorphismus $(\mathbb{Z}/nm\mathbb{Z})^\times \cong (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$ der zugehörigen Einheitengruppen.

2. Es gibt p^{r-1} Vielfache n von p mit $1 \leq n \leq p^r$, also gilt

$$\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$$ □

4.5.7. Damit $\varphi(n)$ eine Zweierpotenz ist, darf also nur der Primfaktor 2 in n mehrfach vorkommen, und alle anderen Primfaktoren müssen die Gestalt $2^r + 1$ haben. Nur dann kann aber $2^r + 1$ eine Primzahl sein, wenn r selbst eine Zweierpotenz ist, denn sonst wäre $r = st$ mit $t > 1$ ungerade, und wir könnten die Gleichung

$$(1 - X^t) = (1 - X)(1 + X + \ldots + X^{t-1})$$

spezialisieren zu $X = -2^s$ und so $1 + 2^r$ nichttrivial faktorisieren.

Ergänzung 4.5.8. Die Zahlen $F_k = 1+2^{2^k}$ heißen **Fermat'sche Zahlen**. F_0, F_1, F_2, F_3, F_4 sind prim, aber $F_5 = 1 + 2^{32} = 641 \cdot 6700417$ ist nicht prim. Es ist nicht bekannt, ob es außer den 5 ersten noch weitere Fermat'sche Zahlen gibt, die prim sind. Bekannt ist, daß F_k für $5 \leq k \leq 32$ nicht prim ist, jedenfalls habe ich das 2009 mit Zitat in Wikipedia gelesen.

Ergänzung 4.5.9. Wenn man schon die Eulersche φ-Funktion einführt, so darf die witzige Identität

$$n = \sum_{d|n} \varphi(d)$$

nicht fehlen. Um sie zu zeigen bemerke man, daß auch für jedes Vielfache $n = cd$ einer Zahl d schon gilt $\varphi(d) = |\{x \in \mathbb{Z}/n\mathbb{Z} \mid \operatorname{ord}(x) = d\}|$. In der Tat definiert nämlich die Multiplikation mit c eine Einbettung $\mathbb{Z}/d\mathbb{Z} \hookrightarrow \mathbb{Z}/n\mathbb{Z}$, deren Bild genau aus allen $x \in \mathbb{Z}/n\mathbb{Z}$ besteht, deren Ordnung d teilt.

Übung 4.5.10. Man zeige, daß man aus einem regelmäßigen 7-Eck mit Zirkel und Lineal ein regelmäßiges 35-Eck konstruieren kann.

Übung 4.5.11. Wieviele zu 140000 teilerfremde Zahlen a mit $1 \leq a \leq 140000$ gibt es?

4.6 Das Quadratische Reziprozitätsgesetz

4.6.1. Gegeben ganze Zahlen $a, b \in \mathbb{Z}$ stellen wir uns nun die Frage, ob es ganze Zahlen $x, y \in \mathbb{Z}$ gibt mit

$$a = x^2 + by$$

Ist das der Fall, so nennt man a einen **quadratischen Rest modulo** b. Gleichbedeutend können wir auch fragen, ob eine Restklasse $\bar{x} \in \mathbb{Z}/b\mathbb{Z}$ existiert mit $\bar{a} = \bar{x}^2$, ob also $\bar{a}$ ein Quadrat ist in $\mathbb{Z}/b\mathbb{Z}$. Es mag nicht a priori klar sein, ob diese Frage derart wichtig ist, daß ihre Behandlung einen eigenen Abschnitt verdient. A posteriori hat sich die Untersuchung dieser Frage und ihrer Verallgemeinerungen jedoch als derart fruchtbar erwiesen, daß es mir angemessen scheint, sie hier zu diskutieren. Zunächst reduzieren wir unsere Frage dazu auf den Fall b prim und erklären dann, wie sie in diesem Fall durch das sogenannte "quadratische Reziprozitätsgesetz" gelöst wird. Es gibt verschiedene Beweise des quadratischen Reziprozitätsgesetzes, dessen verblüffende Aussage viele Mathematiker fasziniert hat. Wir geben hier einen Beweis mit den Methoden der Galoistheorie. Er ist wohl nicht der elementarste Beweis, aber in meinen Augen doch der Beweis, bei dem am wenigsten "gezaubert" wird. Darüber hinaus weist er die Richtung, in der die interessantesten Verallgemeinerungen zu finden sind.

4.6.2 (**Reduktion auf $b = p^n$ eine Primzahlpotenz**). Gegeben $b_1, b_2 \in \mathbb{Z}$ teilerfremd ist a ein Quadrat modulo $b_1 b_2$ genau dann, wenn es ein Quadrat ist modulo b_1 und ein Quadrat modulo b_2. Das folgt unmittelbar aus unserem Ringisomorphismus

$$\mathbb{Z}/b_1 b_2\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/b_1\mathbb{Z} \times \mathbb{Z}/b_2\mathbb{Z}$$

nach dem chinesischen Restsatz II.7.3.17. Nach dieser Bemerkung werden wir uns bei der Untersuchung unserer ursprünglichen Frage auf den Fall beschränken,

daß b eine Primzahlpotenz ist. Für Zahlen b, deren Primfaktorzerlegung wir nicht kennen, ist uns damit zwar wenig geholfen, aber für diese b ist nun einmal schlicht kein schnelles Verfahren bekannt, mit dem die Frage entschieden werden könnte, ob ein gegebenes a quadratischer Rest modulo b ist oder nicht.

4.6.3 (**Reduktion auf a teilerfremd zu $b = p^n$**). Sei nun also b eine Primzahlpotenz, sagen wir $b = p^s$. Ist dann $a = p^r\alpha$ die Darstellung von a als Produkt mit α teilerfremd zu p, so ist die Gleichung

$$a = p^r\alpha = x^2 + yp^s$$

für $r \geq s$ bereits mit $x = 0$ lösbar. Haben wir dahingegen $r + t = s$ mit $t > 0$, so folgt aus der Identität $p^r\alpha = x^2 + yp^rp^t$, daß diese Gleichung nur unter der Annahme r gerade ganzzahlig lösbar ist, und unter dieser Annahme genau dann, wenn die Gleichung

$$\alpha = \tilde{x}^2 + yp^t$$

lösbar ist alias wenn α ein Quadrat ist modulo p^t. Auf diese Weise können wir uns bei der Untersuchung unserer ursprünglichen Frage weiter auf den Fall zurückziehen, daß b eine Primzahlpotenz ist und zusätzlich a teilerfremd zu b.

4.6.4 (**Reduktion von $b = p^n$ auf $b = p$ für $p \neq 2$**). Ist p eine ungerade Primzahl und a teilerfremd zu p, so ist a ein Quadrat modulo p^n für $n \geq 2$ genau dann, wenn a ein Quadrat ist modulo p. Das folgt leicht aus II.7.4.24 oder besser seinem Beweis, wo Sie gezeigt haben, daß die Projektion $(\mathbb{Z}/p^n\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ faktorisiert über einen Isomorphismus als

$$(\mathbb{Z}/p^n\mathbb{Z})^\times \xrightarrow{\sim} \mathbb{Z}/p^{n-1}\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$$

mit der Projektion als zweitem Pfeil. Da die Zwei teilerfremd ist zu p, ist aber jedes Element von $\mathbb{Z}/p^{n-1}\mathbb{Z}$ das Doppelte von einem anderen, und das beendet auch bereits unsere Reduktion. Durch durch Induktion über n kann man sogar explizit eine Lösung finden: Gegeben $\tilde{x}, \tilde{y} \in \mathbb{Z}$ mit $a = \tilde{x}^2 + \tilde{y}p^n$ machen wir zur Lösung der Gleichung $a = x^2 + yp^{n+1}$ den Ansatz $x = \tilde{x} + \lambda p^n$ und finden für λ die Gleichung

$$a = \tilde{x}^2 + 2\lambda p^n\tilde{x} + \lambda^2 p^{2n} + yp^{n+1}$$

Wegen $a - \tilde{x}^2 = \tilde{y}p^n$ kann sie umgeschrieben werden zu

$$2\lambda\tilde{x} = \tilde{y} - \lambda^2 p^n - yp$$

Da nun nach Annahme 2 und a und damit auch $\tilde{x}$ invertierbar sind in $\mathbb{Z}/p\mathbb{Z}$, hat diese Gleichung stets eine Lösung λ.

4.6.5 (**Reduktion von $b = 2^n$ auf $b = 8$**). Eine ungerade Zahl ist ein quadratischer Rest modulo 2^n für $n \geq 3$ genau dann, wenn sie ein quadratischer Rest ist modulo 8 alias kongruent zu 1 modulo 8. Daß diese Bedingung notwendig ist, scheint mir offensichtlich. Um zu zeigen, daß sie auch hinreichend ist, erinnern wir wieder aus II.7.4.24 oder besser seinem Beweis, daß sich die offensichtliche Surjektion $(\mathbb{Z}/2^n\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/8\mathbb{Z})^\times$ als rechte Vertikale in ein kommutatives Diagramm

$$\begin{array}{ccccc} (\mathbb{Z}/2^n\mathbb{Z})^\times & \xrightarrow{\sim} & \mathbb{Z}/2^{n-2}\mathbb{Z} \times (\mathbb{Z}/4\mathbb{Z})^\times & \xrightarrow{\sim} & \mathbb{Z}/2^{n-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ \downarrow & & \downarrow & & \downarrow \\ (\mathbb{Z}/8\mathbb{Z})^\times & \xrightarrow{\sim} & \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/4\mathbb{Z})^\times & \xrightarrow{\sim} & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \end{array}$$

mit den offensichtlichen Surjektionen in den Vertikalen einbetten läßt. Aus diesem Diagramm ist die Behauptung dann unmittelbar ersichtlich. Um eine explizite Lösung zu finden, machen wir wieder Induktion über s und gehen also aus von einer Lösung der Gleichung $a = x^2 + y2^s$ mit $s \geq 3$. Ist y gerade, also $y = 2\tilde{y}$, so steht unsere Lösung für $s+1$ schon da. Sonst ersetzen wir x durch $x + 2^{s-1}$ und finden so auch eine Lösung mit y gerade.

Übung 4.6.6. Gibt es eine Quadratzahl, deren Darstellung im Dezimalsystem mit der Ziffernfolge 39 endet? Für welche Ziffern $a, b\ in\{0, 1, \ldots, 9\}$ gibt es eine Quadratzahl, die mit der Ziffernfolge ab endet?

4.6.7. Mit diesen Überlegungen haben wir also unsere ursprüngliche Frage zurückgeführt auf die Frage, welche Zahlen quadratische Reste sind modulo ungerader Primzahlen. Ganz allgemein wissen wir seit II.2.5.22, wiewiele Elemente eines endlichen Körpers $\mathbb{F}$ Quadrate sind, nämlich im Fall einer von 2 verschiedenen Charakteristik genau $(|\mathbb{F}| + 1)/2$ Elemente. Aber welche? In 4.6.17 erklären wir, wie diese Frage für endliche Primkörper durch das Zusammenwirken von quadratischem Reziprozitätsgesetz 4.6.8 und Ergänzungssatz 4.6.16 effizient gelöst werden kann.

Satz 4.6.8 (Quadratisches Reziprozitätsgesetz). *Seien p und q zwei verschiedene ungerade Primzahlen.*

1. *Ist p oder q kongruent zu 1 modulo 4, so ist p ein Quadrat modulo q genau dann, wenn q ein Quadrat ist modulo p.*
2. *Sind p und q kongruent zu 3 modulo 4, so ist p ein Quadrat modulo q genau dann, wenn q kein Quadrat ist modulo p.*

Beispiel 4.6.9. Wir betrachten $p = 7$ und $q = 103$. Wir finden $103 \equiv 5 \pmod 7$ und durch Ausprobieren sehen wir, daß $0, 1, 2, 4$ die einzigen Quadrate im Körper mit 7 Elementen sind. Insbesondere ist 103 kein Quadrat modulo 7. Unsere Primzahlen sind nun beide kongruent zu 3 modulo 4, und Teil 2 des quadratischen Reziprozitätsgesetzes sagt uns dann, daß 7 notwendig ein Quadrat modulo 103 sein muß.

Vorschau 4.6.10. Vom höheren Standpunkt aus betrachtet mögen Sie, falls Sie sich weiter mit Zahlentheorie beschäftigen, die im folgenden gegebene Argumentation wie folgt einordnen: Man kann die Frage nach der Lösbarkeit diophantischer Gleichungen oft uminterpretieren als Frage nach dem "Verzweigungsverhalten" endlicher algebraischer Erweiterungen des Körpers der rationalen Zahlen. Allgemeiner als im analogen Fall der Riemann'schen Flächen kann sich der Grad der Erweiterung lokal auf drei Weisen bemerkbar machen: (1) Verzweigung, (2) mehrere Stellen über einer gegebenen lokalen Stelle und (3) Erweiterung des Restklassenkörpers. Erster zu untersuchender Fall ist natürlich a priori der Fall quadratischer Erweiterungen, und speziell der Fall der Adjunktion der Wurzel aus einer Primzahl oder auch aus dem Negativen einer Primzahl. Als viel einfacher erweist sich jedoch der Fall der Kreisteilungskörper, in dem alles explizit ausgerechnet werden kann. Und nun basiert der im folgenden gegebene Beweis des quadratischen Reziprozitätsgesetzes im wesentlichen auf dem Trick, den durch Adjunktion der Quadratwurzel einer Primzahl, genauer den durch Adjunktion der Quadratwurzel aus $(-1)^{\frac{p-1}{2}}p$ für eine ungerade Primzahl p, entstehenden Körper als Teilkörper des p-ten Kreisteilungskörpers zu realisieren und besagte Frage im Fall quadratischer Erweiterungen auf diesem Wege zu lösen.

4.6.11. Wir schicken dem Beweis einige allgemeine Überlegungen voraus. Ich erinnere zunächst an II.7.4.16: Jede zyklische Gruppe gerader Ordnung besitzt genau eine zweielementige Untergruppe und auch genau einen surjektiven Gruppenhomomorphismus auf "die" zweielementige Gruppe, dessen Kern die einzige Untergruppe vom Index Zwei ist.

4.6.12. Im Fall der additiven Gruppe $\mathbb{Z}/2n\mathbb{Z}$ ist etwa $\{\bar{0},\bar{n}\} = n\mathbb{Z}/2n\mathbb{Z}$ die einzige zweielementige Untergruppe, die Multiplikation mit n ist der einzige surjektive Gruppenhomomorphismus $\mathbb{Z}/2n\mathbb{Z} \twoheadrightarrow \{\bar{0},\bar{n}\}$, und die einzige Untergruppe vom Index Zwei ist die Untergruppe $2\mathbb{Z}/2n\mathbb{Z}$ aller Restklassen gerader Zahlen.

4.6.13. Im Fall der multiplikativen Gruppe $\mathbb{F}_p^\times$ für p eine ungerade Primzahl ist entsprechend $\{1,-1\}$ die einzige zweielementige Untergruppe, das Potenzieren mit $(p-1)/2$ ist der einzige surjektive Gruppenhomomorphismus $\mathbb{F}_p^\times \twoheadrightarrow \{1,-1\}$, und die einzige Untergruppe vom Index Zwei besteht genau aus den Quadraten in $\mathbb{F}_p^\times$. Führen wir insbesondere für p prim und $a \in \mathbb{Z}$ das sogenannte **Legendre-Symbol** ein durch die Vorschrift

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & a \text{ ist ein Vielfaches von } p; \\ 1 & a \text{ ist kein Vielfaches von } p, \text{ aber ein Quadrat modulo } p; \\ -1 & \text{sonst,} \end{cases}$$

so erhalten wir für p eine ungerade Primzahl die Identität

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

In der Tat folgt das für a teilerfremd zu p aus den vorhergehenden Überlegungen, und in den anderen Fällen ist es eh klar. Des weiteren hängt auch für beliebige Primzahlen p das Legendresymbol nur von der Restklasse modulo p ab und es gilt die Multiplikativität

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

In der Tat folgt das für a und b teilerfremd zu p aus den vorhergehenden Überlegungen, und in den anderen Fällen ist es eh klar.

Lemma 4.6.14. *Sei L/K eine endliche Galoiserweiterung mit zyklischer Galoisgruppe G von gerader Ordnung und sei $\chi : G \twoheadrightarrow \{+1,-1\}$ der nach 4.6.11 eindeutig bestimmte surjektive Gruppenhomomorphismus auf die zweielementige Gruppe. So gilt:*

1. *Der Körper L enthält genau eine quadratische Erweiterung von K;*
2. *Ist die Charakteristik Null, so entsteht diese quadratische Erweiterung durch die Adjunktion einer Quadratwurzel aus einem und jedem von Null verschiedenen Element der Gestalt*

$$\alpha = \alpha(x) = \sum_{\tau\in G} \chi(\tau)\tau(x) \qquad \textit{mit } x \in L;$$

3. *Für alle $\tau \in G$ und alle $x \in L$ wird die Operation der Galoisgruppe auf $\alpha = \alpha(x)$ beschrieben durch die Identität $\tau(\alpha) = \chi(\tau)\alpha$.*

Beweis. Nach 4.6.11 ist $H = \ker\chi$ die einzige Untergruppe von $H \subset G$ vom Index zwei. Nach der Galoiskorrespondenz gibt es mithin genau eine quadratische Erweiterung von K in L, nämlich den Fixkörper von H. Der Fixkörper von H ist im Fall der Charakteristik Null nun gerade das Bild von

$$x \mapsto \sum_{\tau\in H} \tau(x)$$

Diese Abbildung landet nämlich im Fixkörper von H und jeder Fixpunkt von H wird darunter auf sein $|H|$-faches abgebildet. In diesem Fixkörper L^H müssen wir nun nach 4.1.15 genau die Elemente suchen, die von dem nichttrivialen Element von $\mathrm{Gal}(L^H/K) = G/H$ in ihr Negatives überführt werden. Diese müssen für ein und jedes $\sigma \in G\backslash H$ sogar im Bild der Abbildung

$$x \mapsto \alpha(x) := (\mathrm{id} - \sigma)\sum_{\tau\in H} \tau(x) = \sum_{\tau\in G} \chi(\tau)\tau(x)$$

liegen, die vom höheren Standpunkt aus betrachtet bis auf einen Skalar gerade der "Projektor auf die χ-isotypische Komponente der Darstellung L von G über K" ist. Umgekehrt entsteht nach 4.1.15 auch für jedes von Null verschiedene $\alpha = \alpha(x)$ im Bild dieser Abbildung unsere quadratische Erweiterung von K durch Adjunktion der Wurzel α von α^2. Die letzte Aussage des Lemmas schließlich ist evident. □

Beweis des quadratischen Reziprozitätsgesetzes. Wir betrachten nun speziell den p-ten Kreisteilungskörper $\mathbb{Q}(\sqrt[p]{1})$ mit $\sqrt[p]{1} = \zeta$ einer primitiven p-ten Einheitswurzel. Nach 4.5.2 und II.7.3.28 ist seine Galoisgruppe G zyklisch ist von der Ordnung $p-1$, nach 4.6.11 hat sie folglich genau eine Untergruppe vom Index Zwei, die wir im übrigen bereits in 4.5.3 getroffen haben. Der Fixkörper dieser Untergruppe ist nach 4.4.1 eine quadratische Erweiterung von $\mathbb{Q}$, die nach unseren Vorüberlegungen 4.6.14 erzeugt wird von dem nach 3.2.12.4 von Null verschiedenen Element

$$\alpha = \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right) \zeta^a$$

Natürlich gilt nun $\alpha^2 \in \mathbb{Q}$. Wir prüfen durch explizite Rechnung genauer die Formel

$$\alpha^2 = (-1)^{\frac{p-1}{2}} p$$

In der Tat, beachten wir $(\frac{ab^2}{p}) = (\frac{a}{p})$, so ergibt sich durch Substitution von ab für a die zweite Gleichung der Kette

$$\alpha^2 = \sum_{a,b \in \mathbb{F}_p^\times} \left(\frac{ab}{p}\right) \zeta^{a+b} = \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right) \sum_{b \in \mathbb{F}_p^\times} (\zeta^{a+1})^b$$

Bei $a = -1$ ergibt sich ganz rechts der Beitrag $(\frac{-1}{p})(p-1)$. Bei $a \neq -1$ beachten wir, daß für $\eta = \zeta^{a+1}$ wie für jede primitive p-te Einheitswurzel die Relation

$$1 + \eta + \eta^2 + \ldots + \eta^{p-1} = 0$$

erfüllt ist, so daß die Summanden mit $a \neq -1$ jeweils den Beitrag $-(\frac{a}{p})$ liefern. Da nun die Summe der $(\frac{a}{p})$ über alle $a \in \mathbb{F}_p^\times$ verschwindet, liefern alle Summanden mit $a \neq -1$ zusammen den Beitrag $(\frac{-1}{p})$ und wir folgern $\alpha^2 = (\frac{-1}{p})p$. Unsere Formel für α^2 folgt dann aus der Formel

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

aus 4.6.13. Ist p eine ungerade Primzahl und ζ eine primitive p-te Einheitswurzel, so besitzt demnach $(-1)^{\frac{p-1}{2}} p$ eine Quadratwurzel in $\mathbb{Z}[\zeta]$. Das quadratische

Reziprozitätsgesetz ergibt sich nun, indem wir für unsere zweite Primzahl q das Vorzeichen, vermittels dessen ihre Nebenklasse $\bar{q} \in \mathbb{F}_p^\times$ oder vielmehr deren Bild unter dem Isomorphismus

$$\mathbb{F}_p^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$$

aus 4.5.2 auf solch einer Quadratwurzel $\alpha \in \mathbb{Q}(\zeta)$ von $(-1)^{\frac{p-1}{2}}p$ wirkt, auf zwei Weisen berechnen und die Resultate vergleichen. Bezeichne σ_q das Element der Galoisgruppe des Kreisteilungskörpers mit $\sigma_q(\zeta) = \zeta^q$ für eine und jede primitive p-te Einheitswurzel ζ, also $\sigma_q = \sigma_{\bar{q}}$ für $\bar{q} \in \mathbb{F}_p^\times$ die Nebenklasse von q in der weiter vorne eingeführten Notation. Einerseits haben wir nach Konstruktion sicher

$$\sigma_q(\alpha) = \left(\frac{q}{p}\right)\alpha$$

Andererseits gilt für beliebige $c_i \in \mathbb{Z}$ auch $\sigma_q(\sum_{i=0}^{p-1} c_i\zeta^i) = \sum_{i=0}^{p-1} c_i\zeta^{qi}$. Betrachten wir nun den Ring $R = \mathbb{Z}[\zeta]$ und rechnen im Restklassenring R/qR, so erfüllt die darauf induzierte Abbildung nach II.2.4.39 sogar für alle $\alpha \in R$ die Formel

$$\sigma_q(\alpha) \equiv \alpha^q \pmod{qR}$$

Beide Formeln zusammen liefern für unser spezielles α dann

$$\left(\frac{q}{p}\right)\alpha \equiv \alpha^q \pmod{qR}$$

Unser Ring R ist nun offensichtlich eine endlich erzeugte torsionsfreie abelsche Gruppe, insbesondere gilt für unsere zweite Primzahl q notwendig $qR \neq R$ und damit $1 \notin qR$ und dann $qR \cap \mathbb{Z} = q\mathbb{Z}$. Da $\alpha^2 = (-1)^{\frac{p-1}{2}}p$ und damit auch α invertierbar sind in R/qR, folgt

$$\left(\frac{q}{p}\right) \equiv (\alpha^2)^{\frac{q-1}{2}} \equiv p^{\frac{q-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \equiv \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \pmod{qR}$$

Hier sind jedoch beide Seiten ganze Zahlen, also gilt diese Kongruenz auch modulo $q\mathbb{Z}$, und am Anfang und am Ende dieser Kette von Kongruenzen stehen nur die Zahlen ± 1 zur Auswahl, folglich gilt dort sogar Gleichheit. Man überzeugt sich anhand der Definitionen mühelos, daß diese Gleichheit gerade das bedeutet, was wir in Worten als quadratisches Reziprozitätsgesetz formuliert haben. □

4.6.15. Wann 2 ein Quadrat ist modulo einer ungeraden Primzahl p, das sagt uns der folgende "Ergänzungssatz zum quadratischen Reziprozitätsgesetz".

Proposition 4.6.16 (Ergänzungssatz). *Für jede ungerade Primzahl q gilt*

$$\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}} = \begin{cases} 1 & \text{für } q \equiv \pm 1 \pmod 8; \\ -1 & \text{für } q \equiv \pm 3 \pmod 8. \end{cases}$$

Beweis. Wir betrachten die primitive achte Einheitswurzel $\zeta = \exp(\pi\,\mathrm{i}\,/4)$. Wir prüfen $\zeta + \zeta^{-1} = \sqrt{2}$. Sei ε_q das Vorzeichen mit $\sigma_q(\sqrt{2}) = \varepsilon_q\sqrt{2}$. Jetzt rechnen wir im Ring $R = \mathbb{Z}[\zeta]$ und erhalten

$$\varepsilon_q\sqrt{2} = \sigma_q(\sqrt{2}) = \zeta^q + \zeta^{-q} \equiv (\zeta + \zeta^{-1})^q \equiv (\sqrt{2})^q \pmod{qR},$$

also $\varepsilon_q \equiv (\sqrt{2})^{q-1} \equiv 2^{\frac{q-1}{2}} \pmod q$, und damit $\varepsilon_q = (\frac{2}{q})$. Für das Vorzeichen ε_q prüft man andererseits leicht explizit, daß es durch die im Ergänzungssatz behauptete Formel gegeben wird. □

Ergänzung 4.6.17. Will man Legendre-Symbole tatsächlich ausrechnen, so erweist sich deren Erweiterung zu den sogenannten **Jacobi-Symbolen** als praktisch. Man definiert genauer für $a \in \mathbb{Z}$ beliebig und $n \in \mathbb{N}_{\geq 1}$ mit Primfaktorzerlegung $n = p_1 p_2 \ldots p_r$ das Jacobi-Symbol als Produkt von Legendre-Symbolen

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right)$$

Aus den entsprechenden Eigenschaften des Legendre-Symbols folgt, daß auch das Jacobi-Symbol nur von der Restklasse von a modulo n abhängt und daß gilt

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$$

Schließlich folgt aus dem quadaratischen Reziprozitätsgesetz 4.6.8, daß allgemeiner für je zwei ungerade Zahlen $m, n > 1$ das **Reziprozitätsgesetz für Jacobi-Symbole** gilt

$$\left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}}\left(\frac{n}{m}\right)$$

denn auch die Vorzeichen sind multiplikativ in ungeraden m und n, wie man durch Fallunterscheidung prüft. Für jede ungerade Zahl $n > 1$ folgt schließlich aus dem Ergänzungssatz 4.6.16 mühelos der **Ergänzungssatz für Jacobi-Symbole**

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}} = \begin{cases} 1 & \text{für } n \equiv \pm 1 \pmod 8; \\ -1 & \text{für } n \equiv \pm 3 \pmod 8. \end{cases}$$

Für die Primzahlen 1231 und 1549 finden wir so etwa

$$\begin{aligned}
&\left(\tfrac{1231}{1549}\right) = \left(\tfrac{1549}{1231}\right) = \left(\tfrac{318}{1231}\right) = \left(\tfrac{2}{1231}\right)\left(\tfrac{159}{1231}\right) = \left(\tfrac{159}{1231}\right) = -\left(\tfrac{1231}{159}\right) = -\left(\tfrac{118}{159}\right) = \\
&= -\left(\tfrac{2}{159}\right)\left(\tfrac{59}{159}\right) = -\left(\tfrac{59}{159}\right) = -\left(\tfrac{159}{59}\right) = -\left(\tfrac{41}{59}\right) = -\left(\tfrac{59}{41}\right) = -\left(\tfrac{18}{41}\right) = \\
&= -\left(\tfrac{2}{41}\right)\left(\tfrac{9}{41}\right) = -\left(\tfrac{9}{41}\right) = -\left(\tfrac{41}{9}\right) = -\left(\tfrac{5}{9}\right) = -\left(\tfrac{9}{5}\right) = -\left(\tfrac{4}{5}\right) = -\left(\tfrac{2}{5}\right)^2 = -1
\end{aligned}$$

mit unserem Reziprozitätsgesetz und Ergänzungssatz für Jacobi-Symbole. Die Zahl 1231 ist demnach kein quadratischer Rest modulo 1549. Alternativ hätten wir auch den Rest von $1231^{1548/2} = 1231^{774}$ modulo 1548 ausrechnen können. Das dauert so lange auch wieder nicht, da wir zur Beschleunigung der Rechnung 774 in eine Summe von Zweierpotenzen entwickeln können als $774 = 512+256+4+2$, und dann müssen wir nur noch neun Quadrate in $\mathbb{Z}/1549\mathbb{Z}$ berechnen und vier dieser Quadrate in $\mathbb{Z}/1549\mathbb{Z}$ multiplizieren. Ganz so schnell wie obige Rechnung geht das dann aber doch nicht.

Übung 4.6.18. Sei $a \in \mathbb{Z}$ fest vorgegeben. Man zeige: Ob a ein Quadrat ist modulo einer Primzahl q hängt nur von der Restklasse von q modulo $4a$ ab.

Ergänzung 4.6.19. Im Fall $a = -1$ kennen wir das das Resultat der vorhergehenden Übung 4.6.18 im Übrigen bereits aus 2.4.7. In der Sprache der algebraischen Zahlentheorie ist das eine starke Aussage über die Beziehungen zwischen dem "Verzweigungsverhalten der Erweiterung $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$ an verschiedenen Primstellen". Unser Beweis des Reziprozitätsgesetzes, das erst mal den Fall a prim liefert, geht aus vom explizit bekannten Verzweigungsverhalten bei Kreisteilungserweiterungen und folgert das Resultat daraus durch eine Art Galois-Abstieg.

Ergänzende Übung 4.6.20. Ein berühmter **Satz von Kronecker-Weber** besagt, daß jede endliche Galoiserweiterung des Körpers $\mathbb{Q}$ der rationalen Zahlen mit abelscher Galoisgruppe als Unterkörper eines Kreisteilungskörpers realisiert werden kann. Man zeige das für alle quadratischen Erweiterungen von $\mathbb{Q}$.

Ergänzung 4.6.21. Man mag den Satz von Kronecker-Weber interpretieren als eine explizite Beschreibung der "maximalen abelschen Erweiterung" von $\mathbb{Q}$: Sie entsteht durch die Adjunktion aller Einheitswurzeln. **Hilbert's zwölftes Problem** fragt nach einer ähnlich expliziten Beschreibung der "maximalen abelschen Erweiterung" eines beliebigen Zahlkörpers, als da heißt, eines beliebigen Körpers der Charakteristik Null von endlichem Grad über $\mathbb{Q}$.

Übung 4.6.22. Ist 283 ein quadratischer Rest modulo 397? Hinweis: 397 ist eine Primzahl.

4.7 Radikalerweiterungen

Definition 4.7.1. Eine Galoiserweiterung mit zyklischer Galoisgruppe nennt man eine **zyklische Erweiterung**. Eine Galoiserweiterung mit abelscher Galoisgruppe nennt man eine **abelsche Erweiterung**.

4.7.2. Zerfällt das Polynom $X^n - 1$ in einem Körper vollständig in Linearfaktoren, so sagen wir, der besagte Körper **enthalte alle n-ten Einheitswurzeln**. Wir sagen, eine Körpererweiterung L/K **entstehe durch Adjunktion einer n-ten Wurzel** genau dann, wenn gilt $L = K(\alpha)$ für ein $\alpha \in L$ mit $\alpha^n \in K$.

Satz 4.7.3 (**Zyklische Erweiterungen**). *Seien K ein Körper und $n \geq 2$ eine natürliche Zahl derart, daß unser Körper alle n-ten Einheitswurzeln enthält und daß seine Charakteristik n nicht teilt. So gilt:*

1. *Alle zyklischen Erweiterungen von K vom Grad n entstehen durch die Adjunktion einer n-ten Wurzel.*

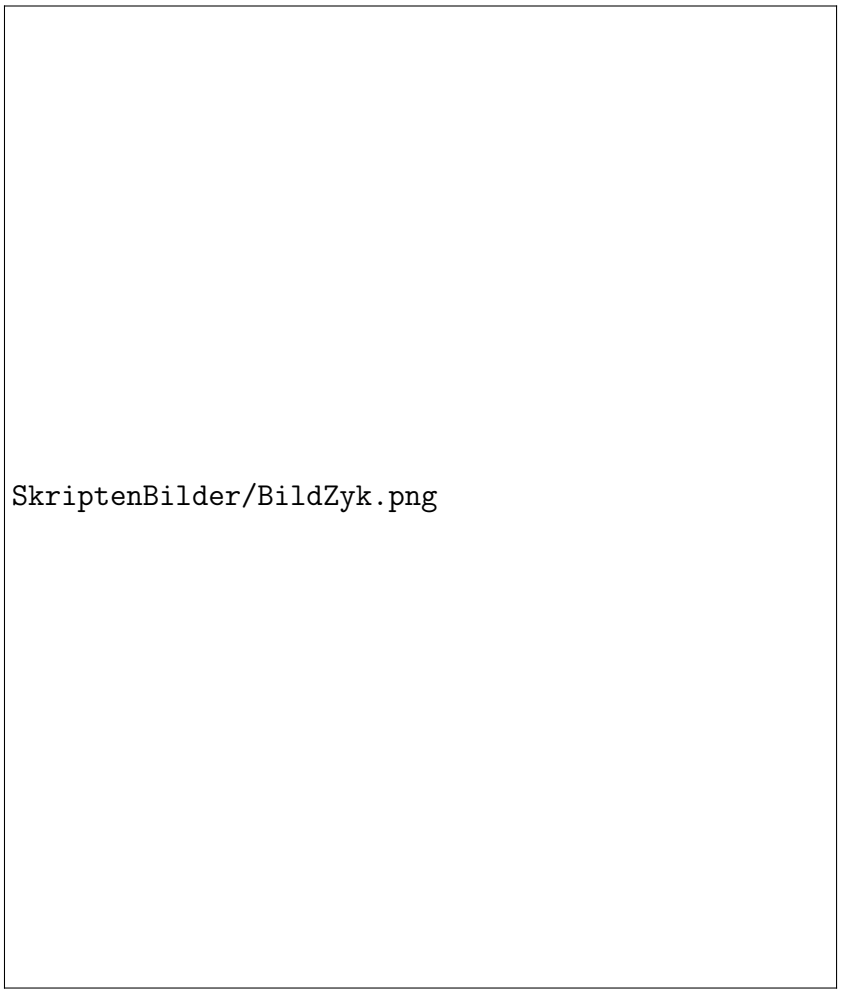
2. *Adjungieren wir zu K eine n-te Wurzel, so erhalten wir eine zyklische Erweiterung, deren Grad n teilt.*

4.7.4. Der Beweis beschreibt im Fall einer zyklischen Erweiterung vom Grad n sogar die Elemente genauer, bei denen die Adjunktion einer n-ten Wurzel unsere Erweiterung liefert: Es handelt sich genau um alle Eigenvektoren eines beliebigen Erzeugers der Galoisgruppe mit einer primitiven n-ten Einheitswurzel als Eigenwert.

4.7.5. Man beachte den fundamentalen Unterschied zwischen der Erweiterung eines Körpers durch n-te Einheitswurzeln und der Erweiterung eines Körpers mit n-ten Einheitswurzeln durch n-te Wurzeln aus von 1 verschiedenen Elementen: Setzen wir der Einfachkeit halber Charakteristik Null voraus, so ist im ersten Fall nach 4.5.2 und 4.7.10 die Ordnung der Galois-Gruppe ein Teiler von $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$, im zweiten Fall jedoch ein Teiler von n.

Beweis. 2. Bezeichne $\mu_n \subset K^\times$ die Gruppe der n-ten Einheitswurzeln. Entsteht $L = K(\alpha)$ durch Adjunktion einer n-ten Wurzel aus $a = \alpha^n$, so sind die Wurzeln des Polynoms $X^n - a$ die $\zeta\alpha$ mit ζ den n-ten Einheitswurzeln, folglich ist unsere Erweiterung Galois. Weiter erhalten wir eine Injektion der Galois-Gruppe in die Gruppe der n-ten Einheitswurzeln, indem wir jedem $\sigma \in \mathrm{Gal}(L/K)$ diejenige Einheitswurzel ζ zuordnen mit $\sigma(\alpha) = \zeta\alpha$. Da nach II.7.3.28 jede endliche Gruppe von Einheitswurzeln zyklisch ist, liefert die Adjunktion n-ter Wurzeln in der Tat zyklische Erweiterungen, deren Ordnung n teilt.

1. Sei umgekehrt L/K eine zyklische Erweiterung vom Grad n. Sei $\sigma \neq \mathrm{id}$ ein Erzeuger der Galoisgruppe. Wir fassen σ auf als eine K-lineare Abbildung $\sigma : L \to L$. Da gilt $\sigma^n = \mathrm{id}$ nach Voraussetzung, sind die Eigenwerte von σ notwendig n-te Einheitswurzeln. Da aus $\sigma(\alpha) = \zeta\alpha$ und $\sigma(\beta) = \eta\beta$ für n-te Einheitswurzeln ζ, η folgt $\sigma(\alpha\beta) = \zeta\eta\alpha\beta$, bilden die Eigenwerte sogar eine Untergruppe $U \subset \mu_n$. Enthielte diese Untergruppe nicht alle n-ten Einheitswurzeln, so gäbe es einen Teiler d von n mit $d \neq n$ derart, daß σ^d als einzigen Eigenwert die 1 hätte. Das kann aber nicht sein, vom höheren Standpunkt aus nach dem Satz von Maschke IV.2.6.1, vom niederen Standpunkt im Fall der Charakteristik Null nach II.6.4.11, elementar kann man auch argumentieren wie folgt: Es wäre



Anschauung für die durch Adjunktion einer dritten Wurzel aus T entstehenden Körpererweiterung des Funktionenkörpers $\mathbb{C}(T)$. Am zweiten Bild zu **??** wird erklärt, wie auch dies Bild zu interpretieren ist. Ich finde, man sieht in diesem Fall auch recht anschaulich, daß die Galoisgruppe zyklisch von der Ordnung drei ist.

ja dann σ^d von der Gestalt $\sigma^d = \mathrm{id} + N$ mit $N \neq 0$ nilpotent, also hätten wir $\sigma^n = \mathrm{id} + (n/d)N + N^2Q(N)$ für ein geeignetes Polynom $Q \in \mathbb{Z}[X]$ und damit

$$(n/d)N = -N^2Q(N)$$

Das ist aber unmöglich für $N \neq 0$ nilpotent, denn bilden wir von beiden Seiten dieser Gleichung Potenzen, so verschwindet die rechte Seite bei einer tieferen Potenz als die linke Seite. Also besteht U aus allen n-ten Einheitswurzeln und es gibt ein von Null verschiedenes $\alpha \in L$ mit $\sigma(\alpha) = \zeta\alpha$ für ζ eine primitive n-ten Einheitswurzel. Wir haben dann notwendig $\sigma(\alpha^n) = \alpha^n$, also $\alpha^n \in K$, aber die Potenzen $\alpha, \alpha^2, \ldots, \alpha^n$ sind linear unabhängig über K als Eigenvektoren zu paarweise verschiedenen Eigenwerten von σ. Es folgt $[K(\alpha) : K] = n$ und damit $L = K(\alpha)$. □

Ergänzende Übung 4.7.6. Sei $n \geq 1$ und K ein Körper, der alle n-ten Einheitswurzeln besitzt und dessen Charakteristik n nicht teilt. Gegeben $a \in K$ ist das Polynom $X^n - a$ irreduzibel in $K[X]$ genau dann, wenn a für keinen Teiler $d > 1$ von n eine d-te Wurzel in K besitzt.

Korollar 4.7.7 (Adjunktion primer Wurzeln). *Sei p eine Primzahl und K ein Körper einer Charakteristik $\mathrm{char}\, K \neq p$, der alle p-ten Einheitswurzeln enthält. Genau dann ist eine echte Erweiterung unseres Körpers Galois vom Grad p, wenn sie durch Adjunktion einer p-ten Wurzel entsteht.*

Beweis. Eine Galoiserweiterung von Primzahlordnung ist notwendig zyklisch. Das Korollar folgt damit aus 4.7.3. □

Definition 4.7.8. Sind in einem großen Körper zwei Teilkörper K, L gegeben, so bezeichnet (KL) den von K und L in unserem großen Körper erzeugten Teilkörper, und nennt diesen Körper das **Kompositum** von K und L.

4.7.9. Für das Kompositum ist die abkürzende Notation $(KL) = KL$ üblich. Ich verwende hier etwas pedantisch die Notation (KL), da ja KL in unseren Konventionen I.3.1.2.6 a priori nur die Menge aller Produkte bedeutet und man oft runde Klammern als Symbol für die "Erzeugung als Körper" verwendet.

Satz 4.7.10 (Translationssatz der Galoistheorie). *Seien in einem großen Körper zwei Teilkörper K, L gegeben. Ist $K \supset (K \cap L)$ eine endliche Galoiserweiterung, so ist auch $(KL) \supset L$ eine endliche Galoiserweiterung und die Restriktion liefert einen Isomorphismus von Galoisgruppen*

$$\mathrm{Gal}((KL)/L) \xrightarrow{\sim} \mathrm{Gal}(K/K \cap L)$$

4.7.11. Insbesondere gilt dieser Situation $[K : K \cap L] = [(KL) : L]$. Ohne die Galois-Bedingung gilt das im Allgemeinen nicht. Als Gegenbeispiel betrachte man in den komplexen Zahlen die von zwei verschiedenen dritten Wurzeln aus 2 über $\mathbb{Q}$ erzeugten Teilkörper K und L. Da jeder von ihnen nur zwei Teilkörper hat, muß hier gelten $K \cap L = \mathbb{Q}$. Ihr Kompositum (KL) hat Grad 6 über $\mathbb{Q}$ und damit Grad 2 über K und L.

Ergänzung 4.7.12. Der obige Translationssatz gilt auch ohne die Annahme, unsere Erweiterung sei endlich. Sogar wenn wir nur $K \supset (K \cap L)$ normal annehmen, folgt bereits $(KL) \supset L$ normal und die Restriktion liefert einen Isomorphismus von Galoisgruppen. Wir zeigen das in **??**.

Beweis. Mit $K/(K \cap L)$ ist auch $(KL)/L$ erzeugt von endlich vielen separablen Elementen bzw. ein Zerfällungskörper. Also ist $(KL)/L$ Galois und L ist nach 4.1.13 der Fixkörper der Galoisgruppe, in Formeln $L = (KL)^G$ für $G = \mathrm{Gal}((KL)/L)$. Da K normal ist über $(K \cap L)$, stabilisieren alle Körperautomorphismen von (KL) über L den Unterkörper K, und die durch Restriktion gegebene Abbildung res zwischen den Galoisgruppen ist offensichtlich injektiv. Der Fixkörper des Bildes von res ist aber genau $K \cap L$, und das zeigt mit 4.1.11 die Bijektivität von res. □

Definition 4.7.13. Sei L/K eine Körpererweiterung. Wir nennen L eine **Radikalerweiterung** von K genau dann, wenn es eine Körperkette

$$K = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_r = L$$

gibt derart, daß der nächstgrößere Körper jeweils entsteht durch Adjunktion einer Wurzel, daß es also in Formeln jeweils $\alpha_i \in K_i$ und $n_i \geq 2$ gibt derart, daß gilt $\alpha_i^{n_i} \in K_{i-1}$ und $K_i = K_{i-1}(\alpha_i)$.

Bemerkung 4.7.14. "Radikal" ist der lateinische Ausdruck für "Wurzel". Unsere Radikalerweiterungen würde man also auf Deutsch bezeichnen als "Erweiterungen, die durch sukzessives Wurzelziehen entstehen".

Definition 4.7.15. Sei M/K eine Körpererweiterung. Wir sagen, ein Element $\alpha \in M$ läßt sich **darstellen durch Radikale über** K genau dann, wenn sich $K(\alpha)$ in eine Radikalerweiterung von K einbetten läßt.

Beispiel 4.7.16. Die folgende reelle Zahl läßt sich darstellen durch Radikale über dem Körper $\mathbb{Q}$ der rationalen Zahlen:

$$\frac{\sqrt[7]{\sqrt[5]{6}+3}+13}{\sqrt[2]{3}+8} - \sqrt[17]{19876} + \sin(\pi/7)$$

Definition 4.7.17. Sei K ein Körper und $P \in K[X]$ ein Polynom. Wir sagen, die Gleichung $P(X) = 0$ läßt sich **auflösen durch Radikale** genau dann, wenn sich alle Nullstellen des Polynoms P in seinem Zerfällungskörper durch Radikale über K darstellen lassen. Ist unser Polynom irreduzibel, so ist es offensichtlich auch gleichbedeutend, daß sich *eine* Nullstelle durch Radikale über K darstellen läßt.

Bemerkung 4.7.18. Eine Gruppe G heißt nach 1.4.11 **auflösbar** genau dann, wenn es eine Folge von Untergruppen $G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_r = 1$ gibt mit G_i normal in G_{i-1} und G_{i-1}/G_i abelsch für $1 \leq i \leq r$.

Satz 4.7.19 (Auflösbarkeit von Gleichungen durch Radikale). *Sei K ein Körper der Charakteristik $\operatorname{char} K = 0$ und $P \in K[X]$ ein Polynom. So sind gleichbedeutend:*

1. *Die Gleichung $P(X) = 0$ läßt sich auflösen durch Radikale.*
2. *Die Galoisgruppe des Zerfällungskörpers von P über K ist auflösbar.*

Beweis. Das folgt mit 1.4.14 und der Galoiskorrespondenz sofort aus der anschließenden Proposition, angewandt auf den Zerfällungskörper von P. □

Proposition 4.7.20. *Sei K ein Körper der Charakteristik $\operatorname{char} K = 0$ und sei L/K eine Körpererweiterung von K. So sind gleichbedeutend:*

1. *Die Erweiterung L läßt sich einbetten in eine Radikalerweiterung des Körpers K.*
2. *Die Erweiterung L läßt sich einbetten in eine endliche Galoiserweiterung des Körpers K mit auflösbarer Galoisgruppe.*

Beweis. $2 \Rightarrow 1$. Sei ohne Beschränkung der Allgemeinheit L/K eine endliche Galoiserweiterung mit auflösbarer Galoisgruppe $G = \operatorname{Gal}(L/K)$. So gibt es eine Folge von Untergruppen

$$G = G_0 \supset G_1 \supset \ldots \supset G_r = 1$$

mit G_i normal in G_{i-1} und G_{i-1}/G_i zyklisch von Primzahlordnung für $1 \leq i \leq r$. Die zugehörige Kette von Fixkörpern ist eine Kette von zyklischen Erweiterungen von Primzahlordnung

$$K = K_0 \subset K_1 \subset \ldots \subset K_r = L$$

Adjungieren wir eine primitive $|G|$-te Einheitswurzel ζ, so erhalten wir nach dem Translationssatz 4.7.10 wieder eine Kette

$$K = K_0 \subset K_0(\zeta) \subset K_1(\zeta) \subset \ldots \subset K_r(\zeta) = L(\zeta)$$

von Galoiserweiterungen. Nach unserem Satz über Adjunktion primer Wurzeln ensteht hier jede Stufe durch Adjunktion einer geeigneten Wurzel aus der vorherigen Stufe. Mithin läßt sich L in eine Radikalerweiterung von K einbetten, nämlich in die Radikalerweiterung $L(\zeta)$.

$1 \Rightarrow 2$. Sei ohne Beschränkung der Allgemeinheit L/K eine Radikalerweiterung. Offensichtlich können wir L auch erhalten, indem wir sukzessive Wurzeln von Primzahlordnung $\sqrt[p_i]{a_i}$ adjungieren, für geeignete Primzahlen p_i. Es gibt also eine Körperkette

$$K = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_r = L$$

sowie geeignete $\alpha_i \in K_i$ und Primzahlen p_i derart, daß für alle $i \geq 1$ gilt $K_i = K_{i-1}(\alpha_i)$ und $\alpha_i^{p_i} \in K_{i-1}$. Ist n das Produkt dieser p_i und adjungieren wir zu L eine primitive n-te Einheitswurzel ζ, so ist im Körperturm

$$K = K_0 \subset K_0(\zeta) \subset K_1(\zeta) \subset \ldots \subset K_r(\zeta) = L(\zeta)$$

jeder Schritt eine abelsche Erweiterung. Vergrößern wir nun $L(\zeta)$ zu einer normalen Erweiterung N/K und betrachten darin das Kompositum $M \subset N$ aller $\varphi(L(\zeta))$ mit $\varphi \in \mathrm{Ring}^K(L(\zeta), N)$, so ist M eine Galoiserweiterung von K und es gibt einen Körperturm

$$K = M_0 \subset M_1 \subset M_2 \subset \ldots \subset M_t = M$$

in dem jede Stufe eine abelsche Erweiterung ist: Um solch einen Körperturm anzugeben, zählen wir unsere φ auf als $\varphi_1, \ldots, \varphi_m$, beginnen mit $M_1 = M_0(\zeta)$ und adjungieren der Reihe nach $\varphi_1(\alpha_1)$, $\varphi_1(\alpha_2), \ldots$, $\varphi_1(\alpha_r)$, $\varphi_2(\alpha_1)$, $\varphi_2(\alpha_2)$, $\ldots, \varphi_2(\alpha_r), \ldots$, $\varphi_m(\alpha_1)$, $\varphi_m(\alpha_2), \ldots$, $\varphi_m(\alpha_r)$. Die Galoiskorrespondenz zeigt dann, daß die Galoisgruppe $\mathrm{Gal}(M/K)$ auflösbar ist. □

Proposition 4.7.21. *Hat ein irreduzibles Polynom fünften Grades aus $\mathbb{Q}[X]$ genau drei reelle und zwei komplexe Nullstellen, so ist seine Galoisgruppe die volle symmetrische Gruppe $\mathcal{S}_5$ und ist damit nicht auflösbar.*

Beweis. Die komplexe Konjugation τ vertauscht zwei Nullstellen und läßt die übrigen fest. Da die Galoisgruppe G transitiv auf der 5-elementigen Menge der Nullstellen operiert, teilt nach der Bahnformel 5 die Gruppenordnung und es gibt nach 1.5.6 ein $g \in G$ von der Ordnung $\mathrm{ord}\, g = 5$. Man sieht etwa mit II.2.10.10, daß g und τ schon ganz $\mathcal{S}_5$ erzeugen. □

Beispiel 4.7.22. Das Polynom $X(X^2+4)(X^2-4) = X^5 - 16X$ hat genau drei reelle Nullstellen und Extrema bei $X = \pm 2/\sqrt[4]{5}$ mit Werten $\pm 32(\frac{1}{5} - 1)1/\sqrt[4]{5}$, die im Absolutbetrag größer sind als zwei. Das Polynom $X^5 - 16X + 2$ hat also

ebenfalls genau drei reelle und zwei komplexe Nullstellen, und es ist darüber hinaus irreduzibel in $\mathbb{Q}[X]$ nach dem Eisensteinkriterium 2.6.2. Seine Galoisgruppe ist nach 4.7.21 folglich nicht auflösbar, und damit kann nach 4.7.19 die Gleichung $X^5 - 16X + 2 = 0$ nicht durch Radikale gelöst werden.

Beispiel 4.7.23. Das Polynom $X^5 - 2$ in $\mathbb{Q}[X]$ ist irreduzibel nach dem Eisensteinkriterium 2.6.2. Es ist jedoch durchaus auflösbar durch Radikale.

4.8 Lösung kubischer Gleichungen

4.8.1. Jetzt interessieren wir uns für **kubische Gleichungen**, also Gleichungen der Gestalt

$$x^3 + ax^2 + bx + c = 0$$

Ihre Galoisgruppen sind auflösbar als Untergruppen von $\mathcal{S}_3$, also müssen sich kubische Gleichungen zumindest in Charakteristik Null durch Radikale lösen lassen. Um explizite Lösungsformeln anzugeben, bringen wir zunächst durch die Substitution $x = y - a/3$ den quadratischen Term zum Verschwinden und gehen über zu einer Gleichung der Gestalt $y^3 + py + q = 0$. Für die Lösung derartiger Gleichungen gibt der folgende Satz eine explizite Formel.

Satz 4.8.2. *Gegeben komplexe Zahlen p, q erhält man genau die Lösungen der Gleichung $y^3 + py + q = 0$, indem man in der* **Cardano'schen Formel**

$$y_{1/2/3} = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

bei beiden Summanden dieselbe Quadratwurzel fest wählt und dann die beiden Kubikwurzeln so zieht, daß ihr Produkt gerade $-p/3$ ist.

4.8.3. Dasselbe gilt sogar für jeden beliebigen algebraisch abgeschlossenen Körper einer von zwei und drei verschiedenen Charakteristik. Dieser Trick war schon bei den Italienern im 16. Jahrhundert bekannt und wurde von den Experten sorgsam geheimgehalten. Selbst wenn alle drei Nullstellen unserer kubischen Gleichung reell sind, ist es nicht möglich, unser Lösungsverfahren ohne die Verwendung der komplexen Zahlen anzuwenden. Diese schlagende Anwendung der komplexen Zahlen war der Ausgangspunkt ihres Siegeszugs in der höheren Mathematik. Die Bemerkung 4.9.8 aus dem anschließenden Abschnitt zeigt, daß der Übergang zu komplexen Zahlen hier wirklich notwendig und nicht etwa nur unserer Ungeschicklichkeit geschuldet ist.

Beweis. Daß wir auf diese Weise wirklich nur Lösungen unserer Gleichung erhalten, kann man unschwer nachrechnen. Daß wir alle Lösungen erhalten, folgt

auch recht schnell: Stimmen zwei derartige Lösungen überein, sagen wir $u+v = \zeta u + \zeta^{-1}v$ für verträgliche Wahlen u und v der beiden Kubikwurzeln und eine primitive dritte Einheitswurzel ζ, so folgern wir $v = \zeta u$, damit das Verschwinden der Diskriminante $27q^2 + 4p^3$, und damit gibt es auch nur höchstens zwei Lösungen nach 2.7.16. Stimmen alle drei so konstruierten Lösungen überein, so folgt weiter $u = v = 0$ und $q = p = 0$ und unsere Gleichung hat in der Tat als einzige Lösung $y = 0$. □

4.8.4. Wie wir sehen, ist es nicht schwer, die Cardano'sche Formel nachzuprüfen. Ich will nun aber erklären, wie man durch Galois-Theorie auf diese Formel geführt wird. Sei dazu k ein Körper einer von Zwei und Drei verschiedenen Charakteristik, der eine nichttriviale dritte Einheitswurzel ζ enthalten möge. Wir bilden den Funktionenkörper

$$K = k('p, q) = \operatorname{Quot} k['p, q]$$

in zwei algebraisch unabhängigen Veränderlichen p und q. Unser Polynom $Y^3 + pY + q$ ist dann nach 2.5.13 irreduzibel in $K[Y]$. Alternativ kann man auch direkt bemerken, daß nach 2.5.9 jede Faktorisierung von einer Faktorisierung im Polynomring $k['p, q, Y]$ herkommen müßte, in der wir $p = q$ setzen könnten und einen Widerspruch zum Eisensteinkriterium 2.6.3 erhielten. Ist L/K ein Zerfällungskörper dieses Polynoms, so schreiben wir

$$Y^3 + pY + q = (Y - \alpha)(Y - \beta)(Y - \gamma)$$

mit $\alpha, \beta, \gamma \in L$ und erhalten

$$\begin{aligned} \alpha + \beta + \gamma &= 0 \\ \alpha\beta + \beta\gamma + \gamma\alpha &= p \\ -\alpha\beta\gamma &= q \quad = \quad \alpha^2\beta + \beta^2\alpha \end{aligned}$$

Da die Diskriminante $4p^3 + 27q^2$ aus 2.7.16 in unserem Fall nicht verschwindet, sind die drei Nullstellen verschieden und unsere Erweiterung ist Galois. Die Galoisgruppe von L/K muß treu und transitiv operieren als eine Gruppe von Permutationen der Menge $\{\alpha, \beta, \gamma\}$ der drei Wurzeln. Damit kommen für diese Galoisgruppe nur die Gruppe $\mathcal{S}_3$ aller Permutationen und die Gruppe A_3 aller geraden Permutationen in Betracht. Der Fixkörper des Normalteilers A_3 der geraden Permutationen enthält das Element

$$E = (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha) = -2\alpha^3 - 3\alpha^2\beta + 3\alpha\beta^2 + 2\beta^3$$

und nach 2.7.16 oder auch elementarer Rechnung ist sein Quadrat bis auf ein Vorzeichen die Diskriminante

$$E^2 = -4p^3 - 27q^2$$

Ist die Charakteristik unseres Körpers nicht gerade Zwei, so ist $-4p^3-27q^2$ nach 2.5.16 in $K=k(p,q)$ kein Quadrat und wir folgern $[K(E):K]=2$. Da nun unsere Erweiterung L/K höchstens Grad 6 haben kann und da L über dem Fixkörper der geraden Permutationen notwendig Grad drei hat, muß $K(E)$ bereits dieser Fixkörper sein und $L/K(E)$ ist eine Galoiserweiterung mit der Galoisgruppe A_3. Sei nun $\sigma\in G$ der Erzeuger dieser Galoisgruppe mit $\sigma(\alpha)=\beta$, $\sigma(\beta)=\gamma$ und $\sigma(\gamma)=\alpha$. Nach 4.7.4 entsteht dann L aus $K(E)$ durch Adjunktion eines Eigenvektors von σ zu einem von 1 verschiedenen Eigenwert. Hier benötigen wir unsere Voraussetzung, daß es in k nichttriviale dritte Einheitswurzeln gibt, und damit ist insbesondere auch der Fall der Charakteristik drei ausgeschlossen. Die dritte Potenz eines solchen Eigenvektors liegt in $K(E)$, so daß L aus $K(E)$ entsteht durch Adjunktion einer Kubikwurzel. Ist $\zeta\in k$ eine nichttriviale dritte Einheitswurzel, so liegt zum Beispiel

$$\begin{aligned} u &= \alpha+\zeta\sigma(\alpha)+\zeta^2\sigma^2(\alpha)\\ &= (1-\zeta^2)\alpha+(\zeta-\zeta^2)\beta \end{aligned}$$

im Eigenraum $\mathrm{Eig}(\sigma;\zeta^2)$ und ist nicht Null, da sonst gälte $\beta\in k\alpha$ im Widerspruch zu $\sigma(\alpha)=\beta$. Ebenso erzeugt

$$\begin{aligned} v &= \alpha+\zeta^2\sigma(\alpha)+\zeta\sigma^2(\alpha)\\ &= (1-\zeta)\alpha+(\zeta^2-\zeta)\beta \end{aligned}$$

den Eigenraum $\mathrm{Eig}(\sigma;\zeta)$ als $K(E)$-Vektorraum und die 1 erzeugt als $K(E)$-Vektorraum den Eigenraum $\mathrm{Eig}(\sigma;1)$. Die drei Elemente $u,v,1$ bilden also eine $K(E)$-Basis von L und wir müssen unsere drei Wurzeln linear aus ihnen kombinieren können. In der Tat erhalten wir unmittelbar $u+v=3\alpha$ und dann durch Teilen durch Drei und Anwenden von σ

$$\alpha=\frac{u}{3}+\frac{v}{3}\qquad \beta=\zeta^2\frac{u}{3}+\zeta\frac{v}{3}\qquad \gamma=\zeta\frac{u}{3}+\zeta^2\frac{v}{3}$$

Die dritten Potenzen von u und von v müssen nun wie gesagt in $K(E)$ liegen, also als K-Linearkombinationen von 1 und E zu schreiben sein. Um besagte dritte Potenzen explizit darzustellen, zerlegen wir sie unter dem Element τ der Galoisgruppe, das α und β vertauscht, in Eigenvektoren: Schreiben wir $2v^3=(v^3+\tau(v^3))+(v^3-\tau(v^3))$, so muß offensichtlich der erste Summand zu K gehören und der zweite zu KE. Nun können wir ja unsere obige Gleichung auch umformen zu $v=(1-\zeta)(\alpha-\zeta\beta)$. Packen wir der Einfachkeit der Rechnung halber den Faktor $(1-\zeta)$ noch auf die andere Seite und setzen $\tilde v=(1-\zeta)^{-1}v=(\alpha-\zeta\beta)$,

so erhalten wir

$$\begin{aligned}
\tilde{v}^3 &= +\alpha^3 - 3\zeta\alpha^2\beta + 3\zeta^2\alpha\beta^2 - \beta^3 \\
\tau(\tilde{v})^3 &= -\alpha^3 + 3\zeta^2\alpha^2\beta - 3\zeta\alpha\beta^2 + \beta^3 \\
\tilde{v}^3 + \tau(\tilde{v})^3 &= 3(\zeta^2-\zeta)(\alpha^2\beta + \alpha\beta^2) && = 3(\zeta^2-\zeta)q \\
\tilde{v}^3 - \tau(\tilde{v})^3 &= 2\alpha^3 - 3(\zeta+\zeta^2)\alpha^2\beta + 3(\zeta+\zeta^2)\alpha\beta^2 - 2\beta^3 \\
&= 2\alpha^3 + 3\alpha^2\beta - 3\alpha\beta^2 - 2\beta^3 && = -E \\
2\tilde{v}^3 &= && = 3(\zeta^2-\zeta)q - E
\end{aligned}$$

und wegen $(1-\zeta)^3 = 3(\zeta^2-\zeta)$ und $(\zeta^2-\zeta)^2 = \zeta+\zeta^2-2 = -3$ schließlich

$$\left(\frac{v}{3}\right)^3 = -\frac{q}{2} + \frac{(\zeta-\zeta^2)E}{18}$$

Genauso liefert Ersetzen von ζ durch ζ^2 in obiger Rechnung auch

$$\left(\frac{u}{3}\right)^3 = -\frac{q}{2} - \frac{(\zeta-\zeta^2)E}{18}$$

und es folgt, daß die beiden Ausdrücke

$$-\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}$$

genau $\left(\frac{v}{3}\right)^3$ und $\left(\frac{u}{3}\right)^3$ liefern. Unsere Lösung α hat also die Gestalt

$$\alpha = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

Wenn wir andererseits die beiden kubischen Wurzeln so ziehen, daß ihr Produkt gerade $-p/3$ ist, so erhalten wir auch stets Lösungen.

4.8.5. Haben wir statt dem Funktionenkörper $K = k('p, q)$ einen beliebigen Körper K einer Charakteristik $\operatorname{char} K \neq 2, 3$ mit nichttrivialen dritten Einheitswurzeln vor uns, so kann obiges Argument in verschiedener Weise zusammenbrechen: Unser Polynom muß nicht irreduzibel sein, und wenn es irreduzibel ist, könnte seine Galoisgruppe nur aus den drei geraden Permutationen der drei Nullstellen bestehen. In diesen Fällen funktioniert das obige Argument nur noch in mehr oder weniger stark modifizierter Form. Es scheint mir jedoch einigermaßen klar, daß unsere für allgemeines p, q hergeleiteten Formeln ihre Gültigkeit behalten sollten, "was immer man für p und q einsetzt, solange dabei nicht Nullen in Nennern auftreten". In unserem Fall haben wir das ja sogar in 4.8.3 bereits explizit geprüft. Für eine formalere Begründung muß ich Sie auf spezialisiertere Vorlesungen verweisen.

Übung 4.8.6. Ein irreduzibles Polynom dritten Grades der Gestalt $Y^3 + pY + q$ mit Koeffizienten in einem Körper k der Charakteristik $\operatorname{char} k \neq 2$ hat genau dann die Galoisgruppe $\mathcal{S}_3$ über k, wenn $-4p^3 - 27q^2$ kein Quadrat in k ist. In unserer Terminologie ist $-4p^3 - 27q^2$ das Negative der Diskriminante unseres Polynoms, aber hier sind auch andere Konventionen verbreitet.

Beispiel 4.8.7. Das Polynom $X^3 - 2$ hat nach die Galoisgruppe $\mathcal{S}_3$ über $\mathbb{Q}$, denn $-108 = (-27)4$ ist kein Quadrat in $\mathbb{Q}$. Dasselbe Polynom hat jedoch Galoisgruppe A_3 über $\mathbb{Q}(\sqrt[3]{1})$ nach unserem Satz über Radikalerweiterungen 4.7.3. Damit alles zusammenpaßt, muß -108 ein Quadrat im dritten Kreisteilungskörper $\mathbb{Q}(\sqrt[3]{1})$ sein. Zum Glück stimmt das auch, für ζ eine primitive dritte Einheitswurzel gilt nämlich $(\zeta - \zeta^{-1})^2 = -3$.

4.9 Einheitswurzeln und der casus irreduzibilis*

4.9.1. Die Tabelle

	sin	cos
π	0	-1
$\pi/2$	1	0
$\pi/3$	$\sqrt{3}/2$	1/2
$\pi/4$	$1/\sqrt{2}$	$1/\sqrt{2}$
$\pi/5$	$\sqrt{5-\sqrt{5}}/2\sqrt{2}$	$(\sqrt{5}+1)/4$
$\pi/6$	1/2	$\sqrt{3}/2$
$\pi/7$	?	?
$\pi/8$	$\sqrt{\frac{1}{2}-\sqrt{2}}$	$\sqrt{\frac{1}{2}+\sqrt{2}}$
$\pi/9$	?	?
$\pi/10$	$(\sqrt{5}-1)/4$	$\sqrt{5+\sqrt{5}}/2\sqrt{2}$
$\pi/11$	?	?

aus **??** zeigt einige $n \geq 1$, für die $\sin(\pi/n)$ und $\cos(\pi/n)$ in geschlossener Form als "reelle algebraische Ausdrücke" dargestellt werden können, ohne daß wir bei der Berechnung des besagten Ausdrucks den Körper der reellen Zahlen verlassen müßten, und auch einige Fragezeichen für Fälle, in denen keine derartige Darstellung zur Verfügung steht. Wir zeigen im Folgenden, daß das nicht etwa an unserer Ungeschicklichkeit liegt, sondern daß es derartige reelle Darstellungen für die meisten n schlicht nicht gibt. Diese Aussage gilt es zunächst einmal zu präzisieren.

Definition 4.9.2. Sei $F \subset E$ eine Körpererweiterung. Wir bezeichnen als **Radikalabschluß von** F **in** E den kleinsten Zwischenkörper $R \subset E$ derart, daß für alle $p \geq 1$ gilt $(x^p \in R) \Rightarrow (x \in R)$, und notieren ihn

$$R = \mathrm{rad}(F \subset E)$$

Beispiel 4.9.3. Die folgende reelle Zahl gehört zum Radikalabschluß des Körpers $\mathbb{Q}$ der rationalen Zahlen im Körper $\mathbb{R}$ der reellen Zahlen:

$$\frac{\sqrt[7]{\sqrt[5]{6}+3}+13}{\sqrt[2]{3}+8} - \sqrt[17]{19876}$$

Korollar 4.9.4. *Genau dann gehört* $\sin(\pi/n)$ *zum Radikalabschluß der rationalen Zahlen in den reellen Zahlen, wenn das regelmäßige* n*-Eck konstruierbar alias* $\varphi(n)$ *eine Zweierpotenz ist.*

Beweis. Sicher liegt $\sin(\pi/n)$ in einem Kreisteilungskörper. Liegt $\sin(\pi/n)$ auch im Radikalabschluß $\mathrm{rad}(\mathbb{Q} \subset \mathbb{R})$ der rationalen in den reellen Zahlen, so folgt aus dem anschließenden Satz 4.9.6 von Rost mit der in 4.9.5 eingeführten Notation "quad" für den "quadratischen Abschluß" sofort $\sin(\pi/n) \in \mathrm{quad}(\mathbb{Q} \subset \mathbb{R})$. Damit ist $\sin(\pi/n)$ aber nach 3.3.2 konstruierbar und damit dann unschwer auch das regelmäßige n-Eck. Der Beweis der Gegenrichtung bleibe dem Leser überlassen. □

Definition 4.9.5. Sei $F \subset E$ eine Körpererweiterung. Wir bezeichnen als **quadratischen Abschluß von** F **in** E den kleinsten Zwischenkörper $Q \subset E$ mit $(x^2 \in Q) \Rightarrow (x \in Q)$ und notieren ihn

$$Q = \mathrm{quad}(F \subset E)$$

Satz 4.9.6 (Markus Rost). *Der Radikalabschluß der rationalen Zahlen in den reellen Zahlen trifft jeden Kreisteilungskörper nur innerhalb des quadratischen Abschlusses der rationalen Zahlen in den reellen Zahlen. Für jedes* $n \in \mathbb{N}$ *gilt also in Formeln*

$$\mathrm{rad}(\mathbb{Q} \subset \mathbb{R}) \cap \mathbb{Q}(\sqrt[n]{1}) \quad \subset \quad \mathrm{quad}(\mathbb{Q} \subset \mathbb{R})$$

Ergänzung 4.9.7. Für jeden Teilkörper $K \subset \mathbb{R}$ und jedes $n \geq 1$ gilt allgemeiner $\mathrm{rad}(K \subset \mathbb{R}) \cap K(\sqrt[n]{1}) \subset \mathrm{quad}(K \subset \mathbb{R})$. Der Beweis ist im wesentlichen derselbe.

4.9.8. Der Satz von Rost zeigt auch, daß $\cos(2\pi/7)$ nicht zum Radikalabschluß von $\mathbb{Q}$ in $\mathbb{R}$ gehören kann. In der Tat gehört diese reelle Zahl zu einem Kreisteilungskörper und müßte nach dem Satz von Rost anderfalls sogar zum quadratischen Abschluß von $\mathbb{Q}$ in $\mathbb{R}$ gehören. Das steht jedoch im Widerspruch zu unserer

Erkenntnis, daß das regelmäßige Siebeneck nicht mit Zirkel und Lineal konstruiert werden kann. Weiter ist $\cos(2\pi/7)$ nach 4.1.21 auch eine von drei reellen Nullstellen des Polynoms $X^3 + X^2 - 2X - 1$. Wir sehen also, daß kubische Gleichungen mit rationalen Koeffizienten, selbst wenn sie drei reelle Nullstellen haben, im allgemeinen nicht durch "algebraische Rechenoperationen im Rahmen der reellen Zahlen" gelöst werden können. Der Übergang ins Komplexe oder alternativ die Verwendung trigonometrischer Funktionen zu ihrer Lösung "durch Radikale" ist in anderen Worten unumgänglich. Lateinisch spricht man bei reellen Gleichungen dritten Grades dieser Art vom **casus irreducibilis**. Im übrigen ist $\cos(2\pi/7)$ ein Erzeuger des Schnitts des siebten Kreisteilungskörpers mit der reellen Achse, dieser Schnitt muß Grad $6/2 = 3$ über $\mathbb{Q}$ haben, und besagtes Polynom ist gerade das Minimalpolynom von $\cos(2\pi/7)$ über $\mathbb{Q}$.

Beweis. Wir halten eine natürliche Zahl $n \geq 1$ für den folgenden Beweis fest. Um unseren Satz zu zeigen, reicht es sicher nachzuweisen, daß für jeden Teilkörper $L \subset \mathbb{R}$ mit der Eigenschaft

$$L \cap \mathbb{Q}(\sqrt[n]{1}) \quad \subset \quad \mathrm{quad}(\mathbb{Q} \subset \mathbb{R})$$

auch der durch Adjunktion einer primen reellen Wurzel x aus einem Element von L entstehende Teilkörper $L(x) \subset \mathbb{R}$ diese Eigenschaft hat, daß also für beliebiges $x \in \mathbb{R}$ und p prim mit $x^p = a \in L^\times$ unsere obige Inklusion auch die Inklusion

$$L(x) \cap \mathbb{Q}(\sqrt[n]{1}) \quad \subset \quad \mathrm{quad}(\mathbb{Q} \subset \mathbb{R})$$

impliziert. Wir unterscheiden zwei Fälle. Im Fall $[L(x) : L] = q < p$ folgt aus unseren Annahmen bereits $L(x) = L$. In der Tat haben wir ja

$$\det_L(x|L(x))^p = \det_L(x^p|L(x)) = a^q$$

Es gibt also $c \in L$ mit $c^p = a^q$. Schreiben wir $1 = \alpha p + \beta q$, so folgt $a = a^{\alpha p+\beta q} = (c^\beta a^\alpha)^p$ und a hat bereits eine p-te Wurzel $y \in L$, woraus wegen $L \subset \mathbb{R}$ und $x \in \mathbb{R}$ folgt $y = \pm x$ und $L(x) = L$. Es bleibt also nur noch, den Fall $[L(x) : L] = p$ zu diskutieren. Dazu müssen wir etwas weiter ausholen. Bezeichne $S := \mathbb{Q}(\sqrt[n]{1}) \cap \mathbb{R}$ den "reellen Teil" des n-ten Kreisteilungskörpers und $T := \mathbb{Q}(\sqrt[n]{1}) \cap \mathrm{quad}(\mathbb{Q} \subset \mathbb{R})$ den "reell-quadratwurzligen Teil" des n-ten Kreisteilungskörpers. Für jeden Teilkörper $K \subset \mathbb{R}$ ist $K \cap \mathbb{Q}(\sqrt[n]{1}) \subset \mathrm{quad}(\mathbb{Q} \subset \mathbb{R})$ offensichtlich gleichbedeutend zu $K \cap S \subset T$. Es gilt also für jeden Teilkörper $L \subset \mathbb{R}$ und jede Primzahl p und jedes $x \in \mathbb{R}$ mit $x^p \in L$ und $[L(x) : L] = p$ zu zeigen

$$L \cap S \subset T \quad \Rightarrow \quad L(x) \cap S \subset T$$

Unter der Annahme $L(x) \cap S = L \cap S$ ist das eh klar. Sonst erhalten wir mit $(L(x) \cap S)/(L \cap S)$ eine nichttriviale Galoiserweiterung, denn das sind beides

Zwischenkörpern einer endlichen abelschen Erweiterung, und nach dem Translationssatz 4.7.10 ist dann auch $((L(x) \cap S)L)/L$ eine nichttriviale Galoiserweiterung. Da $L(x)/L$ Primzahlgrad hat und folglich keine echten Zwischenkörper zuläßt, folgern wir $(L(x) \cap S)L = L(x)$, und $L(x)/L$ ist mithin selbst eine Galoiserweiterung vom Grad p. Das Polynom $X^p - a$ ist dann notwendig das Minimalpolynom von x über L, und da jede Galoiserweiterung normal ist, müssen alle seine Nullstellen auch zu $L(x)$ gehören, also alle ζx für ζ eine beliebige p-te Einheitswurzel. Damit müssen aber alle p-ten Einheitswurzeln zu $L(x)$ gehören, also zu $\mathbb{R}$, und das gilt nur im Fall $p = 2$. Mithin sind wir in diesem Fall, und durch das Rückverfolgen unserer Argumente erhalten wir

$$[(L(x) \cap S) : (L \cap S)] = 2$$

Der Körper $L(x) \cap S$ entsteht also aus dem Teilkörper $L \cap S \subset T$ durch Adjunktion einer Quadratwurzel. Folglich liegt $L(x) \cap S$ in der Tat bereits selbst im reellquadratwurzligen Teil T des n-ten Kreisteilungskörpers. □

Kapitel IV

Darstellungen und Moduln

Hier geht es hauptsächlich um Darstellungen endlicher Gruppen und die Verallgemeinerung der Theorie von Vektorräumen über Körpern zur Theorie von Moduln über nicht notwendig kommutativen Ringen. Für Verbesserungen danke ich Frau Noemi Joosten, Frau Natascha Moser, Frau Bettina Eiche.

Inhalt

1 Darstellungen und Moduln

1.1 Definitionen und Grundlagen

Definition 1.1.1. Eine **Darstellung**, englisch und französisch **representation**, einer Gruppe G über einem Körper k ist ein Paar (V, ρ) bestehend aus einem k-Vektorraum V und einem Gruppenhomomorphismus

$$\rho : G \to \mathrm{GL}(V)$$

1.1.2. Oft bezeichnen wir eine Darstellung abkürzend mit demselben Symbol wie den zugrundeliegenden Vektorraum. Gegeben eine Darstellung V einer Gruppe G bezeichnet dann ρ_V den zugehörigen Gruppenhomomorphismus $\rho_V : G \to \mathrm{GL}(V)$. In derselben Weise definiert man auch allgemeiner den Begriff der **Darstellung eines Monoids** über einem Körper oder, noch allgemeiner, über einem Ring k.

1.1.3. Im Fall $V = k^n$ ist $\mathrm{GL}(V) = \mathrm{GL}(n; k)$ die Gruppe der invertierbaren $n \times n$-Matrizen mit Einträgen in k. Ist unser Gruppenhomomorphismus $\rho : G \to \mathrm{GL}(V)$ dann auch noch injektiv, so "stellt ρ die abstrakte Gruppe G dar als eine konkrete Gruppe von Matrizen", daher die Bezeichnung als "Darstellung". So könnte zum Beispiel die zweielementige Gruppe dargestellt werden, indem man ihr nichttriviales Element als Punktspiegelung auf der Ebene operieren läßt, oder als Spiegelung an einer Achse in der Ebene, oder als Punktspiegelung auf dem Raum, oder als Spiegelung an einer Ebene im Raum, oder auch als Drehung mit dem Winkel $180°$ um eine Achse. Das Symbol ρ ist ein "rho", das Analogon für unser "r" im griechischen Alphabet. Es steht für "representation". Das folgende Lemma erklärt, in welchem Sinn eine Darstellung einer Gruppe G nichts anderes ist als eine Operation von G auf einem Vektorraum "durch lineare Abbildungen".

Übung 1.1.4. Sei G eine Gruppe und k ein Körper und V ein k-Vektorraum. So induziert die Bijektion $\mathrm{Ens}(G, \mathrm{Ens}(V, V)) \xrightarrow{\sim} \mathrm{Ens}(G \times V, V)$ aus I.2.2.26 eine Bijektion

$$\left\{ \begin{array}{c} \text{Darstellungen} \\ G \to \mathrm{GL}(V) \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{c} G\text{-Operationen } G \times V \to V \\ \text{durch } k\text{-lineare Abbildungen} \end{array} \right\}$$

wobei wir mit einer "G-Operation durch k-lineare Abbildungen" eine G-Operation $G \times V \to V$ im Sinne von II.8.1.1 meinen mit der Eigenschaft, daß gilt $g(v+w) = gv + gw$ und $g(\lambda v) = \lambda(gv) \quad \forall g \in G, \lambda \in k$ und $v, w \in V$. Analoges gilt allgemeiner auch für Darstellungen von Monoiden über Ringen.

Beispiel 1.1.5. Jeder Vektorraum V wird eine Darstellung seiner Automorphismengruppe $G = \mathrm{GL}(V)$ vermittels $\rho = \mathrm{id}$. Diese Darstellung heißt die **Standarddarstellung von** $\mathrm{GL}(V)$.

Beispiel 1.1.6. Jeder Vektorraum V wird eine Darstellung einer beliebigen Gruppe G vermittels der trivialen Operation $\rho(g) = \mathrm{id}_V \quad \forall g \in G$.

Beispiel 1.1.7. Ist K/k eine Körpererweiterung, so ist K eine Darstellung über k der Galoisgruppe $\mathrm{Gal}(K/k)$.

Beispiel 1.1.8. Eine Darstellung (V, ρ) der Gruppe $\mathbb{Z}$ anzugeben bedeutet nach I.3.3.12 nichts anderes, als einen Automorphismus $A \in \mathrm{GL}(V)$ eines Vektorraums V anzugeben, nämlich dem Automorphismus $A = \rho(1)$.

Beispiel 1.1.9. Wir untersuchen nun die endlichdimensionalen Darstellungen der Gruppe $\mathbb{Z}/2\mathbb{Z}$. Eine solche Darstellung ist ja nichts anderes als ein endlichdimensionaler Vektorraum V mit einem Endomorphismus $A : V \to V$ derart, daß gilt $A^2 = \mathrm{id}_V$. Wir unterscheiden zwei Fälle.

$\mathrm{char}\, k \neq 2$: In diesem Fall ist V die direkte Summe $V = V^+ \oplus V^-$ der Eigenräume von A zu den Eigenwerten ± 1, für alle $v \in V$ gilt nämlich

$$v = \frac{1}{2}(v + Av) + \frac{1}{2}(v - Av)$$

$\mathrm{char}\, k = 2$: In diesem Fall hat A nur den Eigenwert 1, in einer geeigneten Basis von V hat also A eine Matrix in Jordan'scher Normalform, und aus $A^2 = \mathrm{id}_V$ folgt, daß hier nur Jordanblöcke der Größen eins und zwei möglich sind.

Um die Analoga dieser Erkenntnisse für eine beliebige Gruppe G formulieren zu können, bauen wir zunächst unseren Begriffsapparat weiter aus.

Definition 1.1.10. Seien V, W Darstellungen einer Gruppe G über einem festen Körper k. Ein **Homomorphismus von Darstellungen** ist eine k-lineare Abbildung $f : V \to W$ derart, daß gilt $f(gv) = gf(v)$ für alle $v \in V$, $g \in G$. Ein **Isomorphismus von Darstellungen** ist ein bijektiver Homomorphismus. Gibt es einen Isomorphismus zwischen zwei Darstellungen V und W, so schreiben wir auch $V \cong W$ und sagen, V und W seien **isomorph**.

Definition 1.1.11. Gegeben Darstellungen V, W einer Gruppe G über einem Körper k definieren wir ihre **direkte Summe** als den Vektorraum $V \oplus W$ mit der Operation $g(v, w) = (gv, gw)$. Ähnlich definieren wir auch direkte Summen von endlich oder sogar unendlich vielen Darstellungen. Die direkte Summe von n Kopien einer Darstellung V kürzen wir ab mit V^n. Für den Fall $n = 0$ vereinbaren wir $V^0 = 0$.

Beispiel 1.1.12. Nun können wir die obigen Erkenntnisse wie folgt formulieren:

$\mathrm{char}\, k \neq 2$: Bezeichnet k_+ bzw. k_- die triviale bzw. die nichttriviale eindimensionale Darstellung von $\mathbb{Z}/2\mathbb{Z}$, so ist jede endlichdimensionale Darstellung von $\mathbb{Z}/2\mathbb{Z}$ über k isomorph zu genau einer Darstellung der Gestalt $k_+^n \oplus k_-^m$ für $n, m \in \mathbb{N}$.

$\operatorname{char} k = 2$: Bezeichnet k bzw. P die triviale Darstellung bzw. eine zweidimensionale Darstellung mit nichttrivialer Operation von $\mathbb{Z}/2\mathbb{Z}$, bei der also das nichtneutrale Element durch einen Jordanblock der Größe zwei mit Eigenwert Eins operiert, so ist jede endlichdimensionale Darstellung von $\mathbb{Z}/2\mathbb{Z}$ über k isomorph zu genau einer Darstellung der Gestalt $k^n \oplus P^m$ für $n, m \in \mathbb{N}$.

Von den in 1.1.3 diskutierten Fällen wäre in dieser Notation die Punktspiegelung auf der Ebene $\mathbb{R}^2_-$, die Spiegelung an einer Achse $\mathbb{R}_+ \oplus \mathbb{R}_-$, die Punktspiegelung im Raum $\mathbb{R}^3_-$, die Spiegelung an einer Ebene $\mathbb{R}^2_+ \oplus \mathbb{R}_-$, und die Drehung mit dem Winkel $180°$ um eine Achse $\mathbb{R}_+ \oplus \mathbb{R}^2_-$.

1.1.13. Wir wollen nun ähnliche Aussagen auch für allgemeinere Gruppen formulieren und bauen dazu unseren Begriffsapparat noch weiter aus.

Definition 1.1.14. Sei G eine Gruppe.

1. Eine Teilmenge $W \subset V$ einer Darstellung V von G heißt eine **Unterdarstellung** genau dann, wenn W ein unter G stabiler Untervektorraum ist, in Formeln $g \in G, w \in W \Rightarrow gw \in W$.

2. Eine Darstellung V von G heißt **irreduzibel** oder **einfach** genau dann, wenn V nicht der Nullraum ist, aber 0 und V die einzigen Unterdarstellungen von V sind.

3. Eine Darstellung V von G heißt **unzerlegbar** genau dann, wenn V nicht der Nullraum ist und es keine zwei von Null verschiedenen Unterdarstellungen $W_1, W_2 \subset V$ gibt mit $V = W_1 \oplus W_2$.

4. Eine Darstellung V von G heißt **zyklisch** genau dann, wenn es einen Vektor $v \in V$ gibt, dessen Bahn bereits die ganze Darstellung als Vektorraum erzeugt, in Formeln $\langle Gv \rangle = V$. Solch ein Vektor heißt dann ein **zyklischer Vektor**.

1.1.15. Zum Beispiel ist jede eindimensionale Darstellung irreduzibel. Unsere Darstellung P von 1.1.12 ist zwar unzerlegbar, aber nicht irreduzibel. Wir formulieren nun ein nächstes Ziel.

Proposition 1.1.16. *Eine endliche Gruppe hat über jedem Körper bis auf Isomorphismus höchstens soviele irreduzible Darstellungen wie Elemente. Bezeichnet also* $\operatorname{irr}_k G$ *die Menge der Isomorphieklassen irreduzibler Darstellungen einer Gruppe* G *über einem Körper* k*, so gilt in Formeln stets*

$$|\operatorname{irr}_k G| \leq |G|$$

1.1.17. Zum Beweis der Proposition 1.1.16 entwickeln wir im Folgenden allgemeine Begriffe und Methoden, die Ihnen auch in anderem Kontext ständig begegnen werden. Wir beweisen sie dann als Satz 1.4.20.

Ergänzung 1.1.18. Bereits für die Klein'sche Vierergruppe gibt es über dem Körper mit zwei Elementen unzerlegbare Darstellungen beliebig großer Dimension, siehe [Ben91], 4.3. Die Proposition gilt also nicht mehr, wenn wir darin "irreduzibel" durch "unzerlegbar" ersetzen.

Übung 1.1.19. Man zeige, daß gegeben eine Primzahl p jede p-Gruppe über einem Körper der Charakteristik p bis auf Isomorphismus nur eine einzige einfache Darstellung besitzt. Hinweis: Man beginne mit dem Fall zyklischer Gruppen und verwende dann III.1.4.10.

Übung 1.1.20. Gegeben ein Gruppenhomomorphismus $H \to G$ können wir jede Darstellung V von G zurückziehen zu einer Darstellung $\operatorname{res}_G^H V$ von H. Man zeige, daß wir beim Zurückziehen mit einem inneren Automorphismus $G \to G$ eine zur ursprünglichen Darstellung isomorphe Darstellung erhalten.

Ergänzung 1.1.21. Stabilisiert eine endliche Untergruppe der Automorphismengruppe eines endlichdimensionalen reellen Vektorraums ein Gitter, so nennt man sie **kristallographisch**. Gleichbedeutend ist nach 1.1.22 die Forderung, daß sie bezüglich einer geeigneten Basis durch Matrizen mit rationalen Einträgen dargestellt wird.

Ergänzende Übung 1.1.22. Gegeben eine endlichdimensionale Darstellung V einer endlichen Gruppe über $\mathbb{Q}$ gibt es stets eine $\mathbb{Z}$**-Form**, als da heißt ein unter G stabiles Gitter $V_\mathbb{Z} \subset V$.

Übung 1.1.23. Gegeben eine Darstellung (V, ρ) einer Gruppe G über einem Körper k erhalten wir eine Darstellung (V^*, ρ^*) auf dem Dualraum durch die Vorschrift $\rho^*(g) = (\rho(g^{-1}))^\top$. Sie heißt die **kontragrediente Darstellung** zur Darstellung (V, ρ). Man zeige, daß eine endlichdimensionale Darstellung einfach ist genau dann, wenn die zugehörige kontragrediente Darstellung einfach ist. Man gebe ein Beispiel für eine eindimensionale Darstellung, die nicht zu ihrer kontragredienten Darstellung isomorph ist.

Übung 1.1.24. Die Dimension einer zyklischen und erst recht einer irreduziblen Darstellung ist beschränkt durch die Kardinalität der dargestellten Gruppe.

Übung 1.1.25. Man zeige, daß die Quaternionen aufgefaßt als reeller Vektorraum eine irreduzible Darstellung der achtelementigen Quaternionengruppe aus III.1.5.15 bilden.

Übung 1.1.26. Wieviele Unterdarstellungen hat die Darstellung $\mathbb{R}_+ \oplus \mathbb{R}_-$ der Gruppe $\mathbb{Z}/2\mathbb{Z}$? Ist sie zyklisch? Was ist die Dimension des Raums der Homomorphismen von dieser Darstellung zu sich selber?

Übung 1.1.27. Man gebe alle Unterdarstellungen der Darstellung $\mathbb{R}_+^2 \oplus \mathbb{R}_-$ der Gruppe $\mathbb{Z}/2\mathbb{Z}$ an. Ist diese Darstellung zyklisch? Was ist die Dimension des Raums der Homomorphismen von dieser Darstellung zu sich selber?

Übung 1.1.28. Man bestimme die Dimension des Raums der Homomorphismen von Darstellungen $(\mathbb{R}_+^n \oplus \mathbb{R}_-^m) \to (\mathbb{R}_+^a \oplus \mathbb{R}_-^b)$.

1.2 Moduln über Ringen

Definition 1.2.1. Sei R ein Ring. Ein **R-Modul** ist Paar bestehend aus einer abelschen Gruppe $(M, +)$ und einer Abbildung

$$\begin{array}{ccc} R \times M & \to & M \\ (r, m) & \mapsto & rm \end{array}$$

derart, daß für alle $r, s \in R$ und $m, n \in M$ die folgenden Identitäten gelten:

$$\begin{array}{rcl} r(m+n) & = & (rm) + (rn) \\ (r+s)m & = & (rm) + (sm) \\ r(sm) & = & (rs)m \\ 1m & = & m \end{array}$$

Beispiel 1.2.2. Ist R ein Körper, so nennt man einen R-Modul meist einen R-Vektorraum. Der Ring R selbst ist in offensichtlicher Weise ein R-Modul. Dasselbe gilt für R^n. Weitere Beispiele kommen später.

1.2.3. Wir vereinbaren auch in diesem Kontext die Regel "Punkt vor Strich". Wie bei Vektorrämen zeigt man für alle $m \in M$ die Formel $0m = 0$, genauer $0_R m = 0_M$, und folgert $(-1)m = -m$.

1.2.4. Arbeitet man mit der alternativen Konvention, nach der Ringe nicht notwendig unitär zu sein brauchen, so ist die dritte Bedingung nicht mehr sinnvoll und wird weggelassen. Unsere Moduln würde man in diesen Konventionen als "unitäre Moduln über einem unitären Ring" bezeichnen.

1.2.5. Gegeben eine abelsche Gruppe M bilden wir wie in II.2.4.4 den Ring $\operatorname{Ab} M$ aller Gruppenhomomorphismen $\varphi : M \to M$, den sogenannten **Endomorphismenring von** M. Seine Addition ist die Addition von Abbildungen, $(\varphi+\psi)(m) = \varphi(m) + \psi(m)$, die Multiplikation ist die Verknüpfung von Abbildungen, $\varphi\psi = \varphi \circ \psi$, und das Einselement ist die Identität $\mathrm{id} : M \to M$.

Übung 1.2.6. Gegeben eine abelsche Gruppe M und ein Ring R induziert die kanonische Identifikation $\operatorname{Ens}(R \times M, M) \xrightarrow{\sim} \operatorname{Ens}(R, \operatorname{Ens}(M, M))$ aus I.2.2.26 eine Bijektion

$$\left\{ \begin{array}{c} \text{Strukturen als } R\text{-Modul} \\ \text{auf der abelschen Gruppe } M \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{c} \text{Ringhomomorphismen} \\ R \to \operatorname{Ab} M \end{array} \right\}$$

Im Fall eines Körpers war das bereits Übung II.2.4.21.

1.2.7. In diesem Sinne ist eine R-Modulstruktur auf einer abelschen Gruppe M also "dasselbe" wie ein Ringhomomorphismus $R \to \operatorname{Ab} M$. Für jeden Ring E gibt es nun genau einen Ringhomomorphismus $\mathbb{Z} \to E$. Jede abelsche Gruppe M trägt also genau eine $\mathbb{Z}$-Modulstruktur. Wir können diese $\mathbb{Z}$-Modulstruktur auch explizit beschreiben, für $a \in \mathbb{N}$ ist eben notwendig $1m = m$, also $2m = (1+1)m = m + m$, induktiv $(a+1)m = am + m$, und dann $(-a)m = (-1)am = -(am)$.

Ergänzung 1.2.8. Sei Ω eine Menge. Unter einem **Ω-Modul** versteht man manchmal eine abelsche Gruppe M mitsamt einer Abbildung $\Omega \to \operatorname{Ab}(M)$ unserer Menge Ω in den Endomorphismenring der abelschen Gruppe M. Das ist nun allerdings nichts anderes als ein Modul in unserem bisherigen Sinne über dem "nichtkommutativen Polynomring über $\mathbb{Z}$ in durch Ω indizierten Variablen", den wir in der Notation aus **??** etwa $\operatorname{Ring}^{\uparrow} \Omega$ notieren könnten. Insofern bringt uns dieses Konzept nichts Neues und alles, was wir im folgenden zu Moduln über Ringen zeigen, gilt a forteriori auch für Moduln über Mengen.

1.2.9. Ist $\varphi : R \to S$ ein Ringhomomorphismus, so wird jeder S-Modul und insbesondere auch S selbst ein R-Modul vermittels der Operation $rm = \varphi(r)m$. Dies Verfahren heißt **Restriktion der Skalare**, und zwar selbst dann, wenn $\varphi : R \to S$ nicht die Inklusion eines Teilrings ist. Zum Beispiel ist für jedes Ideal $\mathfrak{a} \subset R$ der Quotient $R/\mathfrak{a}$ ein R-Modul in natürlicher Weise.

Übung 1.2.10. Gegeben eine abelsche Gruppe M und ein Körper k haben wir natürliche Bijektionen

$$\begin{array}{ccc}
\left\{\begin{array}{c}\text{Strukturen als } k[X]\text{-Modul}\\ \text{auf der abelschen Gruppe } M\end{array}\right\} & \xrightarrow{\sim} & \left\{\begin{array}{c}\text{Ringhomomorphismen}\\ k[X] \to \operatorname{Ab} M\end{array}\right\} \\
 & & \wr\downarrow \\
\left\{\begin{array}{c}\text{Paare } (\psi, A) \text{ bestehend aus}\\ \text{einer } k\text{-Vektorraumstruktur}\\ \psi : k \times M \to M\\ \text{auf der abelschen Gruppe } M\\ \text{und einem Endomorphismus}\\ A \in \operatorname{End}_k(M)\end{array}\right\} & \xrightarrow{\sim} & \left\{\begin{array}{c}\text{Paare } (\varphi, A) \text{ bestehend aus}\\ \text{einem Ringhomomorphismus}\\ \varphi : k \to \operatorname{Ab} M\\ \text{und einem mit seinem Bild}\\ \text{kommutierenden Element}\\ A \in \operatorname{Ab} M\end{array}\right\}
\end{array}$$

Genauer liefert 1.2.6 die obere horizontale Bijektion und II.2.5.4 die vertikale Bijektion. In diesem Sinne ist also ein $k[X]$-Modul "dasselbe" wie ein k-Vektorraum mit einem k-linearen Endomorphismus.

Definition 1.2.11. Gegeben k ein Ring und G eine Gruppe definieren wir den **Gruppenring**

$$kG$$

der Gruppe G über k wie folgt: Als abelsche Gruppe ist kG wie in **??** die Menge aller Abbildungen $f : G \to k$, die nur an endlich vielen Stellen von Null verschiedene Werte annehmen. So eine Abbildung schreiben wir als eine formale Linearkombination $\sum f(g)g$ von Elementen aus G mit Koeffizienten aus k. Die Multiplikation $*$ in kG, manchmal auch **Konvolution** oder **Faltung** genannt, erklären wir durch die Vorschrift

$$\left(\sum_{g\in G} a_g g\right) * \left(\sum_{h\in G} b_h h\right) = \sum_{x\in G}\left(\sum_{gh=x} a_g b_h\right) x$$

wo die innere Summe rechts über alle Paare $(g,h) \in G\times G$ laufen soll mit $gh = x$. Offensichtlich erhalten wir so einen Ring mitsamt einem Ringhomomorphismus $k \hookrightarrow kG$, $a \mapsto ae$ für $e \in G$ das neutrale Element und mitsamt einem Monoidhomomorphismus $G \to kG$, $g \mapsto 1g$ von unserer Gruppe in ihren Gruppenring mit der Multiplikation als Verknüpfung. Ist k ein Körper, so ist dieser Monoidhomomorphismus, wenn wir ihn als eine durch G indizierte Familie von Elementen von kG auffassen, offensichtlich eine Basis von kG über k. Für Ringe gilt dasselbe mit dem auf Moduln erweiterten Basisbegriff aus 1.5.6. Wir schreiben meist kurz $ae = a$ und $1g = g$, auch wenn wir Elemente des Gruppenrings meinen, und notieren die Faltung oft ohne $*$ schlicht durch Hintereinanderschreiben. Häufig wird der Gruppenring auch $k[G]$ notiert.

1.2.12. Die eben eingeführte Notation für Gruppenringe ist nur im Fall multiplikativ notierter Gruppen praktisch: Im Fall additiv notierter Gruppen wäre bereits der Ausdruck $g+h$ zweideutig, es könnte damit entweder die Summe in der Gruppe $1(g+h)$ oder die Summe im Gruppenring $1g + 1h$ gemeint sein. Aus diesem Grund schreibt man im Fall additiv notierter Gruppen Elemente des Gruppenrings lieber in der Form $\sum f(g)\,\mathrm{e}^g$, wobei die Notation e^g nur eine rein formale Bedeutung hat. Dann gilt etwa im Gruppenring $\mathrm{e}^{g+h} = \mathrm{e}^g\,\mathrm{e}^h \neq \mathrm{e}^g + \mathrm{e}^h$ und man kann wieder ganz intuitiv rechnen.

1.2.13. Wir erhalten einen Isomorphismus $k\mathbb{Z} \xrightarrow{\sim} k[X,X^{-1}]$ zwischen dem Gruppenring der Gruppe $\mathbb{Z}$ über einem Ring k und dem Ring $k[X,X^{-1}]$ der Laurentpolynome mit Koeffizienten in k durch die Vorschrift $\sum a_n\,\mathrm{e}^n \mapsto \sum a_n X^n$. Allgemeiner kann man in derselben Weise auch für jedes Monoid G den **Monoidring** kG einführen und erhält analog einen Ringisomorphismus $k\mathbb{N} \xrightarrow{\sim} k[X]$.

Übung 1.2.14. Gegeben ein Ringhomomorphismus $\varphi : k \to R$ und ein Monoid G und Monoidhomomorphismus $\psi : G \to (R,\cdot)$ mit der Eigenschaft $\varphi(a)\psi(g) = \psi(g)\varphi(a)\ \forall a \in k,\ g \in G$ gibt es genau einen Ringhomomorphismus $kG \to R$, der φ und ψ fortsetzt.

Übung 1.2.15. Diese Übung ist grundlegend für die in diesem Text vorgesehene Entwicklung der Darstellungstheorie endlicher Gruppen. Sei G eine Gruppe oder

allgemeiner ein Monoid und k ein Körper oder allgemeiner ein Ring und M eine abelsche Gruppe. Das Einschränken einer Abbildung $kG \times M \to M$ zu Abbildungen $k \times M \to M$ und $G \times M \to M$ liefert dann die vertikale Bijektion im Diagramm

$$\begin{array}{c}
\left\{\begin{array}{c} kG\text{-Modulstrukturen} \\ kG \times M \to M \\ \text{auf der abelschen Gruppe } M \end{array}\right\} \\
\downarrow \wr \\
\left\{\begin{array}{c} k\text{-Modulstrukturen} \\ k \times M \to M \\ \text{auf der abelschen Gruppe } M \\ \text{zusammen mit } G\text{-Operation} \\ G \times M \to M \\ \text{durch } k\text{-lineare Abbildungen} \end{array}\right\} \xrightarrow{\sim} \left\{\begin{array}{c} k\text{-Modulstrukturen} \\ k \times M \to M \\ \text{auf der abelschen Gruppe } M \\ \text{zusammen mit einem} \\ \text{Monoidhomomorphismus} \\ G \to \mathrm{End}_k(M) \end{array}\right\}
\end{array}$$

wobei die horizontale Bijektion wie so oft schon wieder einmal von unserer Bijektion $\mathrm{Ens}(G \times M, M) \xrightarrow{\sim} \mathrm{Ens}(G, \mathrm{Ens}(M, M))$ aus I.2.2.26 herkommt und $\mathrm{End}_k(M)$ das multiplikative Monoid des Rings $\mathrm{End}_k(M)$ meint, den wir erst in 1.3.2 einführen werden. In diesem Sinne ist eine Darstellung einer Gruppe G über k also "dasselbe" wie ein kG-Modul. Wir werden einen guten Teil der Darstellungstheorie von Gruppen aus der Spezialisierung von Resultaten für Moduln über Ringen erhalten, die hinwiederum durch die Methoden der linearen Algebra für Moduln über Körpern alias Vektorräume motiviert werden.

Übung 1.2.16. Man zeige, daß es für jeden Ring k und $G = \{e, g\}$ eine zweielementige Gruppe genau einen Ringisomorphismus $k[X]/\langle X^2 - 1\rangle \xrightarrow{\sim} kG$ gibt mit $\bar{X} \mapsto g$. Man folgere aus dem abstrakten chinesischen Restsatz weiter für k einen Körper mit $\mathrm{char}\, k \neq 2$ einen Isomorphismus $k[X]/\langle X^2 - 1\rangle \xrightarrow{\sim} k \times k$.

Übung 1.2.17. Gegeben Ringe $R_1, \ldots, R_n$ mit Produkt $R = R_1 \times \ldots \times R_n$ erhalten wir für jede abelsche Gruppe M eine Bijektion

$$\left\{\begin{array}{c} \text{Strukturen auf } M \\ \text{als } R\text{-Modul} \end{array}\right\} \xrightarrow{\sim} \left\{\begin{array}{c} \text{Zerlegungen } M = M_1 \oplus \ldots \oplus M_n \text{ mit} \\ \text{jeweils einer } R_i\text{-Modulstruktur auf } M_i \end{array}\right\}$$

indem wir in R die Elemente $\mathrm{e}_i = (0, \ldots, 1, \ldots, 0)$ mit einer 1 an der i-ten Stelle und Nullen sonst betrachten und in M die Untergruppen $M_i := e_i M$ nehmen und sie mit der hoffentlich offensichtlichen von der R-Modulstruktur auf M induzierten Struktur eines R_i-Moduls versehen.

Übung 1.2.18. Man zeige, daß der Gruppenring der Gruppe $\mathbb{Z}/n\mathbb{Z}$ über einem Körper k isomorph ist zum Quotienten $k[X]/\langle X^n - 1\rangle$ des Polynomrings. Im Fall, daß $X^n - 1$ über k in Linearfaktoren zerfällt, zeige man weiter, daß die

einfachen Darstellungen alle eindimensional sind und daß ihre Isomorphieklassen parametrisiert werden durch die Wurzeln dieses Polynoms. Unter der Annahme, daß zusätzlich das Bild von n in k nicht verschwindet, zeige man weiter, daß dieser Gruppenring auch isomorph ist zum Produkt $k \times \ldots \times k$ von n Kopien des Körpers k. Im Fall $k = \mathbb{C}$ liefert etwa die diskrete Fouriertransformation aus **??** einen derartigen Isomorphismus.

1.3 Homomorphismen, Untermoduln, Quotienten

Definition 1.3.1. Eine Abbildung $f : M \to N$ von einem R-Modul in einen weiteren heißt **R-linear** oder ein **R-Modulhomomorphismus** genau dann, wenn gilt $f(m + m') = f(m) + f(m')$ und $f(rm) = rf(m) \quad \forall m, m' \in M, r \in R$.

Definition 1.3.2. Die Menge aller Homomorphismen von einem R-Modul M in einen R-Modul N schreiben wir auch $\mathrm{Hom}_R(M, N)$. Sie bildet eine Untergruppe von $\mathrm{Ens}(M, N)$. Ein bijektiver Homomorphismus heißt ein **Isomorphismus** von R-Moduln. Gibt es einen Isomorphismus zwischen zwei R-Moduln M und N, so schreiben wir auch $M \cong M$ und sagen, M und N seien **isomorph**. Ein Homomorphismus von einem Modul zu sich selbst heißt ein **Endomorphismus** unseres Moduls. Die Menge aller Endomorphismen des R-Moduls M notiert man $\mathrm{End}_R(M)$. Sie bildet unter der Verknüpfung als Multiplikation einen Ring.

Lemma 1.3.3. *Die R-Modulhomomorphismen von einem Ring R, aufgefaßt als R-Modul, zu einem beliebigen weiteren R-Modul werden parametrisiert durch die Elemente des besagten R-Moduls. Für jeden R-Modul M ist genauer die Abbildung*

$$\begin{array}{ccc} M & \to & \mathrm{Hom}_R(R, M) \\ m & \mapsto & (r \mapsto rm) \end{array}$$

ein Isomorphismus von abelschen Gruppen mit Inversem $\varphi \mapsto \varphi(1)$.

Beweis. Dem Leser überlassen. □

Übung 1.3.4. Man zeige: Ist R ein Ring und $e \in R$ ein idempotentes Element und M ein R-Modul, so induziert das Auswerten bei e eine Bijektion $\mathrm{Hom}_R(Re, M) \xrightarrow{\sim} eM$.

Definition 1.3.5. Eine Teilmenge $N \subset M$ eines R-Moduls M heißt ein **Untermodul** genau dann, wenn N eine Untergruppe ist und es gilt $m \in N, r \in R \Rightarrow rm \in N$.

1.3.6. Die Untermoduln eines kommutativen Rings sind genau seine Ideale. Jeder Schnitt von Untermoduln ist wieder ein Untermodul. Ist $T \subset M$ eine Teilmenge

eines Moduls M, so heißt der kleinste Untermodul von M, der T enthält, auch der **von T erzeugte Untermodul** und wir bezeichnen ihn mit $\langle T\rangle_R$ oder abkürzend mit $\langle T\rangle$. Man kann diesen Untermodul beschreiben als die Menge aller Linearkombinationen

$$\{r_1t_1 + \ldots r_st_s \mid s \geq 0,\ r_i \in R,\ t_i \in T\}$$

wobei die leere Linearkombination mit $s = 0$ für die Null in M stehen möge. Ein Modul, der von einer endlichen Teilmenge erzeugt wird, heißt **endlich erzeugt**. Ein Modul, der von einem einzigen Element erzeugt wird, heißt ein **zyklischer Modul**.

1.3.7. Das Bild eines Untermoduls unter einem Modulhomomorphismus ist wieder ein Untermodul. Dasselbe gilt für das Urbild eines Untermoduls. Insbesondere sind Bild und Kern eines Modulhomomorphismus stets Untermoduln.

Ergänzende Übung 1.3.8. In einem endlich erzeugten Modul umfaßt jedes Erzeugendensystem ein endliches Erzeugendensystem.

Proposition 1.3.9 (über Quotientenmoduln). *Sei M ein R-Modul und $N \subset M$ ein Untermodul.*

1. *Es gibt genau eine Struktur eines R-Moduls auf der Quotientengruppe M/N derart, daß die Projektion $\mathrm{can} : M \twoheadrightarrow M/N$ ein Homomorphismus von R-Moduln ist.*
2. *Jeder Homomorphismus von R-Moduln $\varphi : M \to M'$ mit $\varphi(N) = 0$ faktorisiert in eindeutiger Weise über M/N, es gibt also zu φ genau einen R-Modulhomomorphismus $\tilde{\varphi} : M/N \to M'$ mit $\varphi = \tilde{\varphi} \circ \mathrm{can}$.*

Beweis. Dem Leser überlassen. □

Übung 1.3.10. Sei R ein Ring und $\mathfrak{a} \subset R$ ein Ideal und M ein R-Modul. Bezeichne $\mathfrak{a}M \subset M$ den Untermodul, der von allen Elementen am mit $a \in \mathfrak{a}$ und $m \in M$ erzeugt wird, und der bei sorgfältigerer Notation eigentlich $\langle \mathfrak{a}M\rangle$ notiert werden müßte. Man zeige, daß die Operation von R auf $M/\mathfrak{a}M$ in natürlicher Weise faktorisiert über $R/\mathfrak{a}$, so daß also $M/\mathfrak{a}M$ in natürlicher Weise ein $R/\mathfrak{a}$-Modul wird.

Übung 1.3.11. Gegeben ein R-Modul M wird M ein Modul über seinem Endomorphismenring $\mathrm{End}_R(M)$ vermittels der Vorschrift $fm = f(m)$ für $f \in \mathrm{End}_R(M)$ und $m \in M$.

Übung 1.3.12. Gegeben Moduln M_i über Ringen R_i kann man das Produkt M der M_i in offensichtlicher Weise mit der Struktur eines Moduls über dem Produkt R der R_i versehen. Ergibt sich in derselben Weise ein R-Modul N als das Produkt gewisser R_i-Moduln N_i, so haben wir einen kanonischen Isomorphismus

$$\mathrm{Hom}_R(M, N) \xrightarrow{\sim} \prod_i \mathrm{Hom}_{R_i}(M_i, N_i)$$

1.4 Einfache Moduln und Kompositionsreihen

Definition 1.4.1. Ein Modul heißt **einfach** genau dann, wenn er nicht Null ist, aber außer sich selbst und Null keine Untermoduln hat.

Beispiele 1.4.2. Die einfachen Moduln über einem Körper oder allgemeiner einem Schiefkörper sind genau die eindimensionalen Vektorräume. Jeder Vektorraum ist einfach als Modul über seinem Endomorphismenring.

Übung 1.4.3. Die einfachen $\mathbb{Z}$-Moduln sind genau die zyklischen abelschen Gruppen von Primzahlordnung. Allgemeiner sind alle einfachen Moduln über einem Ring isomorph zu einem Quotienten des besagten Rings nach einem maximalen Linksideal. Ist der Ring kommutativ, so kann man besagtes Linksideal aus dem Modul zurückgewinnen als seinen Annulator. Genauer ist dann der Quotient unseres Rings nach unserem maximalen Ideal bereits ein Körper, vergleiche **??**, und unser einfacher Modul ist ein eindimensionaler Vektorraum über diesem Körper. Bei nichtkommutativen Ringen können die Quotienten nach verschiedenen maximalen Linksidealen jedoch durchaus als Moduln isomorph sein: Man denke etwa an den Matrizenring $\mathrm{M}(r \times r; k)$ mit Einträgen in einem Körper k und den einfachen Modul k^r dieses Rings: Hier sind ja die Annulatoren verschiedener von Null verschiedener Elemente im allgemeinen durchaus verschiedene Linksideale.

Satz 1.4.4 (Existenz von maximalen Idealen). *In jedem von Null verschiedenen Ring gibt es mindestens ein maximales Ideal. Allgemeiner läßt sich in einem beliebigen Ring jedes Ideal, das nicht der ganze Ring ist, vergrößern zu einem maximalen Ideal unseres Rings.*

Beweis. Sei R unser Ring und $\mathfrak{a} \neq R$ unser Ideal. Wir betrachten das System aller Ideale von R, die $\mathfrak{a}$ enthalten und nicht ganz R sind oder, gleichbedeutend, nicht die 1 von R enthalten. Dieses System von Mengen ist offensichtlich nicht leer und stabil unter aufsteigenden Vereinigungen. Jetzt folgt der Satz aus dem Zorn'schen Lemma in der Gestalt **??**. □

Übung 1.4.5. In jedem Ring läßt sich auch jedes echte Links- bzw. Rechtsideal vergrößern zu einem maximalen echten Links- bzw. Rechtsideal. Genau dann ist ein Linksideal maximal, wenn der Quotient danach ein einfacher Modul ist. Jeder von Null verschiedene Modul über einem Ring besitzt einen einfachen Subquotienten. Insbesondere besitzt jeder von Null verschiedene Ring mindestens einen einfachen Modul.

Übung 1.4.6. Warum kann man nicht mit demselben Argument zeigen, daß jede Gruppe eine maximale echte Untergruppe besitzt? Man zeige auch, daß die additive Gruppe $\mathbb{Q}$ keine maximale echte Untergruppe besitzt.

Übung 1.4.7. Jeder endlich erzeugte und von Null verschiedene Modul besitzt einen einfachen Quotienten. Hinweis: 1.4.5. Der $\mathbb{Z}$-Modul $\mathbb{Q}$ besitzt als $\mathbb{Z}$-Modul weder einfache Untermoduln noch einfache Quotienten. Als $\mathbb{Q}$-Modul ist $\mathbb{Q}$ dahingegen einfach.

Übung 1.4.8. Ist k ein algebraisch abgeschlossener Körper, so ist jeder einfache $k[X]$-Modul eindimensional und isomorph zu $k[X]/\langle X-\lambda\rangle$ für genau ein $\lambda \in k$.

1.4.9. Der Hilbert'sche Nullstellensatz **??** besagt, daß alle einfachen Moduln über einem Polynomring in endlich vielen Variablen mit Koeffizienten in einem Körper endlichdimensional sind über besagtem Körper. Ist der Körper algebraisch abgeschlossen, so sind sie sogar eindimensional, das folgt dann aus 1.4.11.

Lemma 1.4.10. *Seien R ein Ring, E, E' einfache R-Moduln und M ein beliebiger R-Modul. So gilt:*

1. *Jeder Homomorphismus $E \to M$ ist injektiv oder Null.*
2. *Jeder Homomorphismus $M \to E'$ ist surjektiv oder Null.*
3. *Jeder Homomorphismus $E \to E'$ ist bijektiv oder Null.*
4. *Der Endomorphismenring $\operatorname{End}_R E$ ist ein Schiefkörper.*

Beweis. $\ker(E \to M)$ und $\operatorname{im}(M \to E')$ sind Untermoduln von E bzw. von E' und sind folglich Null oder ganz E bzw. ganz E'. □

Korollar 1.4.11. *Sei R ein kommutativer Ring, der einen algebraisch abgeschlossenen Körper k als Teilring hat. So ist ein einfacher R-Modul, der endlichdimensional ist als k-Vektorraum, notwendig eindimensional als k-Vektorraum.*

Beweis. Die Multiplikation mit einem beliebigen Element $r \in R$ besitzt notwendig einen Eigenwert, und der zugehörige Eigenraum ist ein von Null verschiedener Untermodul, also der ganze Modul. Also operiert jedes $r \in R$ durch einen Skalar, und dann kann unser Modul nur einfach sein, wenn er eindimensional ist. □

Definition 1.4.12. Gegeben ein Modul M über einem Ring R definieren wir seine **Länge**

$$l_R(M) = l(M) \in \mathbb{N} \sqcup \{\infty\}$$

als das Supremum über alle n derart, daß es in M eine echt absteigende Kette von Untermoduln gibt der Gestalt $M = M_n \supsetneq M_{n-1} \supsetneq \ldots \supsetneq M_0 = 0$, die also salopp gesprochen in n echten Schritten vom ganzen Modul zum Nullmodul führt.

Beispiel 1.4.13. Ist k ein Körper, so ist die Länge eines k-Moduls genau die Dimension des fraglichen k-Vektorraums.

1.4.14. Bei einer endlichen echt absteigenden Kette maximal möglicher Länge ist natürlich stets M_i/M_{i-1} einfach für $1 \leq i \leq n$. Offensichtlich hat ein Modul die Länge Null genau dann, wenn er der Nullmodul ist, und die Länge Eins genau dann, wenn er einfach ist.

Definition 1.4.15. Sei R ein Ring und M ein R-Modul. Eine **Kompositionsreihe von** M ist eine endliche Kette von Untermoduln

$$M = M_r \supset M_{r-1} \supset \ldots \supset M_0 = 0$$

derart, daß M_i/M_{i-1} einfach ist für $1 \leq i \leq r$. Der Modul M_i/M_{i-1} heißt dann der **i-te Subquotient** unserer Kompositionsreihe. Gegeben ein Modul M über einem Ring erklären wir seine **Kompositionslänge**

$$\lambda_R(M) = \lambda(M) \in \mathbb{N} \sqcup \{\infty\}$$

wie folgt: Besitzt unser Modul eine Kompositionsreihe, so sei $\lambda(M)$ die kleinstmögliche Länge einer Kompositionsreihe von M. Besitzt unser Modul keine Kompositionsreihe, so sagen wir, seine Kompositionslänge sei unendlich und schreiben $\lambda(M) = \infty$.

Satz 1.4.16 (Jordan-Hölder). *Die Länge und die Kompositionslänge stimmen für jeden Modul überein. Weiter haben je zwei Kompositionsreihen eines Moduls dieselbe Länge und bis auf Reihenfolge isomorphe Subquotienten.*

1.4.17. In Formeln ausgedrückt besagt der zweite Teil: Sind $M = M_r \supset \ldots \supset M_0 = 0$ und $M = N_s \supset \ldots \supset N_0 = 0$ zwei Kompositionsreihen eines Moduls M, so gilt $r = s$ und es gibt eine Permutation $\sigma \in \mathcal{S}_r$ mit $N_i/N_{i-1} \cong M_{\sigma(i)}/M_{\sigma(i)-1}$ für alle i. Diese Subquotienten oder genauer ihre Isomorphieklassen heißen die **Kompositionsfaktoren** unseres Moduls endlicher Länge M, und unser Satz sagt auch, daß jeder Kompositionsfaktor mit einer wohlbestimmten Vielfachheit auftritt. Gegeben ein einfacher Modul L notiert man die Vielfachheit von L als Kompositionsfaktor von M meist

$$[M : L]$$

Beweis. Die erste Aussage unseres Satzes behauptet in Formeln $l(M) = \lambda(M)$. Offensichtlich ist a priori nur die Abschätzung $l(M) \geq \lambda(M)$. Als nächstes zeigen wir nun, daß für jeden Modul M endlicher Kompositionslänge und jeden von Null verschiedenen Untermodul $N \subset M$ gilt

$$\lambda(M/N) < \lambda(M)$$

Sei in der Tat $M = M_r \supset \ldots \supset M_0 = 0$ eine Kompositionsreihe von M und $N \subset M$ ein Untermodul. Wir betrachten den Quotienten $\bar{M} = M/N$ und die Bilder $\bar{M}_i$ der M_i in $\bar{M}$ und erhalten kurze exakte Sequenzen

$$M_i \cap N/M_{i-1} \cap N \hookrightarrow M_i/M_{i-1} \twoheadrightarrow \bar{M}_i/\bar{M}_{i-1}$$

durch explizites Nachdenken oder formales Anwenden des Neunerlemmas II.9.2.13 auf das kommutative Diagramm

$$\begin{array}{ccccc} M_{i-1} \cap N & \hookrightarrow & M_i \cap N & \twoheadrightarrow & M_i \cap N/M_{i-1} \cap N \\ \downarrow & & \downarrow & & \downarrow \\ M_{i-1} & \hookrightarrow & M_i & \twoheadrightarrow & M_i/M_{i-1} \\ \downarrow & & \downarrow & & \downarrow \\ \bar{M}_{i-1} & \hookrightarrow & \bar{M}_i & \twoheadrightarrow & \bar{M}_i/\bar{M}_{i-1} \end{array}$$

Gilt $N \neq 0$, so kann nicht $M_i \cap N = M_{i-1} \cap N$ gelten für alle i. Zu jeder Kompositionsreihe von M haben wir also eine echt kürzere Kompositionsreihe von $\bar{M} = M/N$ konstruiert und erkennen damit, daß in der Tat aus $\lambda(M) < \infty$ und $N \neq 0$ folgt $\lambda(M/N) < \lambda(M)$. Man sieht so, daß die Länge einer beliebigen echt absteigenden Kette von Untermoduln eines Moduls endlicher Kompositionslänge M nach oben beschränkt ist durch eben diese Kompositionslänge $\lambda(M)$ und folgert sofort $l(M) \leq \lambda(M)$. Im Fall $\lambda(M) = \infty$ ist das eh klar und so ergibt sich schließlich für jeden Modul M die Gleichheit

$$l(M) = \lambda(M)$$

Daß je zwei Kompositionsreihen dieselbe Länge haben, folgt sofort. Ist weiter N einfach, so gibt es oben genau einen Index j mit

$$M_j \cap N = N \text{ aber } M_{j-1} \cap N = 0$$

Für diesen Index haben wir $M_j/M_{j-1} \cong N$ und $\bar{M}_j/\bar{M}_{j-1} = 0$, wohingegen für die anderen Indizes $i \neq j$ gilt $M_i/M_{i-1} \cong \bar{M}_i/\bar{M}_{i-1}$. Nun folgt der Rest des Satzes mit Induktion. □

Korollar 1.4.18. *Gegeben $M \supset N$ ein Modul mit einem Untermodul gilt in $\mathbb{N} \sqcup \{\infty\}$ die Gleichheit $l(M) = l(M/N) + l(N)$.*

Beweis. Für jeden Untermodul $N \subset M$ sind die Ungleichungen

$$\begin{aligned} l(M) &\geq l(M/N) + l(N) \\ \lambda(M) &\leq \lambda(M/N) + \lambda(N) \end{aligned}$$

offensichtlich. Da nach dem Satz aber die Länge und die Kompositionslänge übereinstimmen, folgt die Behauptung. □

Korollar 1.4.19. *Sei R ein Ring, der einen Körper k als Teilring hat. Ist R endlichdimensional als Linksmodul über k, so gibt es bis auf Isomorphismus höchstens $\dim_k R$ einfache R-Moduln.*

Beweis. Natürlich ist R von endlicher Länge als R-Modul und es gilt sogar $l(R) \leq \dim_k R$. Jeder einfache R-Modul ist aber ein Quotient von R und taucht also in einer und damit in jeder Kompositionsreihe von R als Subquotient auf. □

Satz 1.4.20. *Eine endliche Gruppe hat über jedem Körper höchstens soviele Isomorphieklassen von irreduziblen Darstellungen, wie sie Elemente hat.*

Beweis. Bezeichnet G unsere endliche Gruppe und k unseren Körper, so behaupten wir in Formeln, daß es bis auf Isomorphismus höchstens $|G|$ irreduzible Darstellungen von G über k gibt. Um das zu zeigen, fassen wir unsere Darstellungen mit 1.2.15 als Moduln über dem Gruppenring kG auf, und der Satz folgt dann aus Korollar 1.4.19. □

Übung 1.4.21. Der Quotient eines Moduls nach einem maximalen echten Untermodul ist stets ein einfacher Modul.

Übung 1.4.22. Der einzige einfache Modul über dem Endomorphismenring eines endlichdimensionalen Vektorraums ist der besagte Vektorraum selber, bis auf Isomorphismus.

Ergänzende Übung 1.4.23. Ein Modul heißt **artinsch** nach dem Mathematiker Emil Artin genau dann, wenn jede absteigende Folge von Untermoduln stationär wird. Man sagt dann auch, unser Modul "erfülle die absteigende Kettenbedingung". Man zeige, daß ein Modul artinsch ist genau dann, wenn er endliche Länge hat.

1.4.24. Auf Englisch spricht man von der **descending chain condition** oder kurz **dcc** oder auch von **artinian modules**. Darin liegt eine gewisse Ironie der Geschichte, Emil Artin war nämlich armenischen Ursprungs und seine Familie hatte ihren Familiennamen Artinian extra zu Artin eingedeutscht. Wichtiger als die artinschen Moduln sind die sogenannten "noetherschen" Moduln, die die analoge "aufsteigende Kettenbedingung" erfüllen, vergleiche 1.7.12.

Ergänzung 1.4.25. Eine Variante zum hier gewählten Zugang zum Satz von Jordan-Hölder findet man etwa in [JS06]: Man zeigt wie dort ausgeführt ohne große Schwierigkeiten, daß je zwei endliche Filtrierungen eines Moduls durch das Einfügen geeigneter weiterer Untermoduln so verfeinert werden können, daß die Subquotienten der beiden so enstehenden Filtrierungen bis auf Reihenfolge isomorph sind.

1.5 Summen und Produkte von Moduln

1.5.1. Die folgenden Konstruktionen verallgemeinern unsere Konstruktionen im Fall von Vektorräumen aus II.6.2.

Definition 1.5.2. Gegeben eine Familie $(M_\lambda)_{\lambda\in\Lambda}$ von Moduln über einem Ring R bilden wir zwei neue R-Moduln, das **Produkt** $\prod M_\lambda$ und die **direkte Summe** oder kurz **Summe** $\bigoplus M_\lambda$ durch die Regeln

$$\begin{aligned}\textstyle\prod_{\lambda\in\Lambda} M_\lambda &= \{(m_\lambda)_{\lambda\in\Lambda} \mid m_\lambda \in M_\lambda\}\\ \textstyle\bigoplus_{\lambda\in\Lambda} M_\lambda &= \{(m_\lambda)_{\lambda\in\Lambda} \mid m_\lambda \in M_\lambda, \text{ nur endlich viele } m_\lambda \text{ sind nicht null}\}\end{aligned}$$

mit der offensichtlichen komponentenweisen Addition und Multiplikation mit Skalaren aus R.

1.5.3. Für eine endliche Familie von Moduln $M_1, \ldots, M_s$ stimmen die direkte Summe und das Produkt überein. Wir benutzen dann alternativ die Notationen

$$M_1 \times \ldots \times M_s = M_1 \oplus \ldots \oplus M_s$$

1.5.4. Das Produkt bzw. die Summe sind das Produkt bzw. Koprodukt in der Kategorie der R-Moduln im Sinne unserer allgemeinen Definitionen II.10.4.1 bzw. II.10.4.7. Ausformuliert bedeutet das: Die offensichtlichen Einbettungen und Projektionen sind Homomorphismen

$$\mathrm{in}_\lambda : M_\lambda \hookrightarrow \bigoplus_{\lambda\in\Lambda} M_\lambda \qquad \text{bzw.} \qquad \mathrm{pr}_\lambda : \prod_{\lambda\in\Lambda} M_\lambda \twoheadrightarrow M_\lambda$$

und ist M ein weiterer R-Modul, so induzieren die durch Vorschalten der in_λ bzw. Nachschalten der pr_λ gegebenen Abbildungen Bijektionen

$$\begin{aligned}\mathrm{Hom}_R(\textstyle\bigoplus_{\lambda\in\Lambda} M_\lambda, M) &\xrightarrow{\sim} \textstyle\prod_{\lambda\in\Lambda} \mathrm{Hom}_R(M_\lambda, M)\\ f &\mapsto (f\circ \mathrm{in}_\lambda)_{\lambda\in\Lambda}\end{aligned}$$

$$\begin{aligned}\mathrm{Hom}_R(M, \textstyle\prod_{\lambda\in\Lambda} M_\lambda) &\xrightarrow{\sim} \textstyle\prod_{\lambda\in\Lambda} \mathrm{Hom}_R(M, M_\lambda)\\ f &\mapsto (\mathrm{pr}_\lambda \circ f)_{\lambda\in\Lambda}\end{aligned}$$

1.5.5. Gegeben eine Familie $(M_\lambda)_{\lambda\in\Lambda}$ von Untermoduln eines Moduls M bezeichnet man den von ihrer Vereinigung erzeugten Untermodul auch als ihre **Summe** und notiert ihn $\sum_{\lambda\in\Lambda} M_\lambda$. Diese Summe kann auch interpretiert werden als das Bild eines natürlichen Homomorphismus $\bigoplus_{\lambda\in\Lambda} M_\lambda \to M$ von der direkten Summe nach M. Ist dieser Homomorphismus injektiv, so sagen wir, die "Summe der Untermoduln M_λ sei direkt" und schreiben statt $\sum_{\lambda\in\Lambda} M_\lambda$ auch $\bigoplus_{\lambda\in\Lambda} M_\lambda$.

1.5.6. Auch bei Moduln über Ringen nennt man eine Familie $(m_\lambda)_{\lambda\in\Lambda}$ **linear unabhängig** genau dann, wenn nur die triviale (endliche) Linearkombination verschwindet, wenn also für eine Familie $(r_\lambda)_{\lambda\in\Lambda}$ von Elementen unseres Rings mit nur endlich vielen von Null verschiedenen Mitgliedern gilt

$$\sum_{\lambda\in\Lambda} r_\lambda m_\lambda = 0 \quad \Rightarrow \text{ alle } r_\lambda \text{ sind null}$$

Ein linear unabhängiges Erzeugendensystem heißt wie bei Vektorräumen eine **Basis**, und wie dort erklären wir die Begriffsvarianten einer **Basis als Teilmenge**, einer **Basis als Familie**, und einer **angeordneten Basis**. Allerdings besitzen keineswegs alle Moduln eine Basis, wie man das von Vektorräumen gewohnt ist. Die Moduln, die eine Basis besitzen, nennt man **freie Moduln**.

Beispiel 1.5.7. $\mathbb{Z}/5\mathbb{Z}$ ist kein freier $\mathbb{Z}$-Modul, aber durchaus ein freier Modul über dem Ring $\mathbb{Z}/5\mathbb{Z}$.

Beispiel 1.5.8. Für jede Menge Λ ist der Modul

$$R\Lambda := \{f : \Lambda \to R \mid f(\lambda) = 0 \text{ für fast alle } \lambda\}$$

frei, denn die Abbildungen, die an einer Stelle den Wert 1 annehmen und sonst den Wert Null, bilden eine Basis. Nach unseren Definitionen ist umgekehrt eine Familie $(m_\lambda)_{\lambda\in\Lambda}$ in einem Modul M eine Basis genau dann, wenn die Abbildung $R\Lambda \to M$ mit $(r_\lambda) \mapsto \sum r_\lambda m_\lambda$ ein Isomorphismus ist.

Übung 1.5.9. Jeder Modul ist Quotient eines freien Moduls.

1.5.10. Für beliebige Ringe R folgt aus $R^n \cong R^m$ im allgemeinen keineswegs $n = m$. Das einfachste Gegenbeispiel ist der Nullring, und das ist nach 1.5.11 auch das einzige kommutative Gegenbeispiel. Unter den nicht kommutativen Ringen gibt es jedoch auch interessantere Gegenbeispiele. Betrachten wir etwa zu einem beliebigen Körper den freien Vektorraum V über der Menge $\mathbb{N}$, so gibt es einen Isomorphismus $V \xrightarrow{\sim} V \oplus V$, und für den Endomorphismenring $R = \operatorname{End} V$ erhalten wir einen Isomorphismus von R-Moduln $R \cong R^2$ als die Verknüpfung $R = \operatorname{End} V \cong \operatorname{Hom}(V \oplus V, V) \cong R \oplus R$.

Übung 1.5.11. Gegeben ein kommutativer von Null verschiedener Ring R folgt aus $R^n \cong R^m$ schon $n = m$. Hinweis: Man benutze 1.3.10 und wähle mit 1.4.5 ein maximales Ideal $\mathfrak{a} \subset R$, so daß $R/\mathfrak{a}$ nach **??** ein Körper ist. Ein alternativer Beweis, der ohne das Zorn'sche Lemma auskommt, wird in 1.6.8 gegeben.

Übung 1.5.12. Gegeben Moduln $M_1, \ldots, M_m$ und $N_1, \ldots, N_n$ über einem Ring R haben wir eine natürliche Identifikation

$$\operatorname{Hom}_R(M_1 \oplus \ldots \oplus M_m, N_1 \oplus \ldots \oplus N_n) \xrightarrow{\sim} \prod_{i,j} \operatorname{Hom}_R(M_j, N_i)$$

1.5.13. Wir werden die Elemente einer endlichen direkten Summe oft als Spaltenvetoren von Elementen der Summanden auffassen und die Homomorphismen zwischen direkten Summen als Matrizen von Homomorphismen zwischen den Summanden. Das erlaubt uns, die Komposition solcher Homomorphismen mit dem Formalismus der Matrixmultiplikation zu berechnen.

Übung 1.5.14. Gegeben eine Familie von Moduln M_{ij} mit $i \in I, j \in J$ haben wir stets eine kanonische Injektion $\bigoplus_i (\prod_j M_{ji}) \to \prod_j (\bigoplus_i M_{ji})$, die im allgemeinen aber kein Isomorphismus ist.

Lemma 1.5.15 (Verallgemeinerte Hauptraumzerlegung). *Gegeben ein Modul M über einem Kring R und ein maximales Ideal $\chi \in \operatorname{Max} R$ setze man $M_\chi = \{m \in M \mid \chi^k m = 0 \text{ für } k \gg 0\}$. Mit dieser Notation liefern die Inklusionen eine Einbettung*

$$\bigoplus_{\chi \in \operatorname{Max} R} M_\chi \hookrightarrow M$$

und das Bild dieser Einbettung ist die Vereinigung aller Untermoduln endlicher Länge.

1.5.16. Im Spezialfall eines Polynomrings in einer Veränderlichen über einem algebraisch abgeschlossenen Körper k ist das die Hauptraumzerlegung II.6.3.12, vergleiche auch II.6.3.17. Unter der Bijektion $k \xrightarrow{\sim} \operatorname{Max}(k[X])$, $\lambda \mapsto \langle X - \lambda \rangle$ entspricht genauer die Hauptraumzerlegung des durch Multiplikation mit X gegebenen Endomorphismus des k-Vektorraums M genau der Zerlegung in der Proposition.

Beweis. Wäre die Summe der M_χ nicht direkt, so wäre auch schon eine endliche Teilsumme nicht direkt und wir hätten etwa eine endliche direkte Teilsumme $M_\nu \oplus \ldots \oplus M_\mu$, die von einem weiteren M_χ nichttrivial geschnitten wird. Wegen $(M \oplus N)_\chi = M_\chi \oplus N_\chi$ hätten wir dann $\mu \neq \chi$ mit $M_\mu \cap M_\chi \neq 0$. Das ist aber absurd, da gilt $R = \chi + \mu$, also $1 = a + b$ mit $a \in \chi$, $b \in \mu$, also für alle n auch $1 = (a+b)^{2n} = c + d$ mit $c \in \chi^n$, $d \in \mu^n$, und damit $1m = 0$ für alle $m \in M_\mu \cap M_\chi$. Die Summe ist also direkt und es reicht, wenn wir für M von endlicher Länge $M = \sum M_\chi$ zeigen. Unter dieser Annahme ist klar, daß wir paarweise verschiedene $\chi_1, \ldots, \chi_r \in \operatorname{Max} R$ finden können und $n \in \mathbb{N}$ mit

$$(\chi_1 \ldots \chi_r)^n M = 0$$

Der chinesische Restsatz III.2.2.4 liefert dann einen Isomorphismus

$$R/(\chi_1 \ldots \chi_r)^n \xrightarrow{\sim} R/\chi_1^n \times \ldots \times R/\chi_r^n$$

den wir benutzen können, um unser M aufzufassen als einen Modul über dem Produktring. Die Elemente e_i in diesem Produktring mit einem einzigen Eintrag

1 an der i-ten Stelle und Nullen sonst haben als Elemente der rechten Seite die Eigenschaft $\chi_i^n e_i = 0$ und für alle $m \in M$ gehört $m = e_1 m + \ldots + e_r m$ folglich zur Summe der M_χ. □

Übung 1.5.17. Man bestimme die verallgemeinerte Hauptraumzerlegung von $\mathbb{Z}/1000\mathbb{Z}$.

1.6 Matrizenrechnung

Definition 1.6.1. Sei R ein Ring. Ein **R-Rechtsmodul** ist ein Paar bestehend aus einer abelschen Gruppe $(M, +)$ mitsamt einer Abbildung $M \times R \to M, (m, r) \mapsto mr$ derart, daß gilt für alle $m, n \in M$ und $r, s \in R$:

$$\begin{array}{rcl} (m+n)r & = & mr + nr \\ m(r+s) & = & mr + ms \\ m(rs) & = & (mr)s \\ m1 & = & m \end{array}$$

1.6.2. Unsere R-Moduln aus Definition 1.2.1 nennt man manchmal auch genauer **Linksmoduln**. Um den Unterschied klar zu machen, definieren wir für jeden Ring $R = (R, +, \cdot)$ den **opponierten Ring** $R^{\mathrm{opp}} = (R, +, *)$ als die abelsche Gruppe R mit der "vertauschten" Multiplikation $r * s = sr$ für $r, s \in R$. Man prüft ohne Schwierigkeiten, daß ein R-Rechtsmodul dasselbe ist wie ein R^{opp}-Linksmodul, alias eine abelsche Gruppe M mitsamt einem Ringhomomorphimus $R^{\mathrm{opp}} \to \operatorname{End} M$. Insbesondere braucht man bei kommutativen Ringen zwischen Rechtsmoduln und Linksmoduln keinen Unterschied zu machen.

1.6.3. Für R-Rechtsmoduln M, N nennen wir einen Homomorphismus von abelschen Gruppen $f : M \to N$ mit $f(mr) = f(m)r \; \forall m \in M, r \in R$ auch einen **Homomorphismus von R-Rechtsmoduln** und bezeichnen die Menge aller Homomorphimen von R-Rechtsmoduln mit

$$\operatorname{Hom}_{-R}(M, N)$$

Genau wie bei Körpern haben wir auch bei Ringen R eine natürliche Bijektion

$$\begin{array}{rccc} M: & \operatorname{Hom}_{-R}(R^n, R^m) & \xrightarrow{\sim} & \mathrm{M}(m \times n; R) \\ & f & \mapsto & [f] \end{array}$$

wo die Spalten der Matrix $M(f) = [f] = (a_{ij})$ die Bilder unter f der Vektoren $\mathrm{e}_1, \ldots, \mathrm{e}_n$ der Standardbasis des R^n sind, in Formeln $f(\mathrm{e}_j) = (a_{1j}, \ldots, a_{mj})$ für $1 \leq j \leq n$. Die inverse Abbildung ordnet jeder Matrix A die R-rechtslineare Abbildung $x \mapsto Ax$ zu, wo wir die Elemente $x \in R^n$ bzw. $Ax \in R^m$ als Spaltenmatrizen auffassen. Wie bei Körpern entspricht die Matrixmultiplikation der Verknüpfung von Abbildungen, in Formeln $[f \circ g] = [f] \circ [g]$, und f ist ein Isomorphismus genau dann, wenn seine Matrix $[f]$ invertierbar ist.

1.6.4. Gegeben R-Rechtsmoduln M, N mit angeordneten Basen $\mathcal{A}, \mathcal{B}$ erhalten wir genau wie bei Körpern auch bei Ringen R eine natürliche Bijektion

$$\begin{array}{ccc} \mathrm{Hom}_{-R}(M,N) & \xrightarrow{\sim} & \mathrm{M}(m\times n;R) \\ f & \mapsto & {}_{\mathcal{B}}[f]_{\mathcal{A}} \end{array}$$

und nennen wieder ${}_{\mathcal{B}}[f]_{\mathcal{A}}$ die **darstellende Matrix der Abbildung f in Bezug auf die Basen $\mathcal{A}$ und $\mathcal{B}$**. Die Formel ${}_{\mathcal{C}}[g\circ f]_{\mathcal{A}} = {}_{\mathcal{C}}[g]_{\mathcal{B}} \circ {}_{\mathcal{B}}[f]_{\mathcal{A}}$ gilt entsprechend.

Übung 1.6.5. Gegeben ein Ring R liefert die durch Rechtsmultiplikation gegebene Abbildung aus 1.3.3 einen Ringisomorphismus $R^{\mathrm{opp}} \xrightarrow{\sim} \mathrm{End}_R(R)$ und die durch Linksmultiplikation gegebene Abbildung einen Ringisomorphismus $R \xrightarrow{\sim} \mathrm{End}_{-R}(R)$.

1.6.6. Ich erinnere an die Definition der Determinante quadratischer Matrizen mit Einträgen in einem kommutativen Ring durch die Leibnizformel II.3.1.1, an die Multiplikationsformel $\det(AB) = (\det A)(\det B)$ aus II.3.4.1 und daran, daß eine quadratische Matrix nach II.3.4.13 genau dann invertierbar ist, wenn ihre Determinante eine Einheit in fraglichen kommutativen Ring ist.

Ergänzung 1.6.7. Die Leibnizformel ist zwar auch für nichtkommutative Ringe noch sinnvoll, aber die Formel $\det(AB) = (\det A)(\det B)$ ist dann nicht mehr richtig, und deshalb sind Determinanten in der Allgemeinheit nichtkommutativer Ringe nicht mehr von Nutzen.

Proposition 1.6.8. *Ist R ein kommutativer Ring und nicht der Nullring, so folgt aus der Existenz eines Isomorphismus von Moduln $R^n \cong R^m$ bereits $n = m$.*

1.6.9. Ein alternativer Beweis wird in Übung 1.5.11 skizziert. Ein Gegenbeispiel für nichtkommutative Ringe erklärt 1.5.10.

Beweis. Ein Isomorphismus $R^n \cong R^m$ wird notwendig beschrieben durch Matrizen A und B. Wäre $n \neq m$, so wären unsere Matrizen nicht quadratisch. Hat ohne Beschränkung der Allgemeinheit A mehr Zeilen als Spalten und ergänzen wir unsere Matrizen durch Nullen zu quadratischen Matrizen $\tilde{A}$ und $\tilde{B}$, so gilt immer noch $\tilde{A}\tilde{B} = I$ mit I der Einheitsmatrix, im Widerspruch zu $\det \tilde{A} = 0$. □

1.6.10. Ist M ein endlich erzeugter freier Modul über einem kommutativen Ring $R \neq 0$, so heißt die Zahl $n \in \mathbb{N}$ mit $M \cong R^n$ auch der **Rang** von M. Das Beispiel **??** zeigt, daß man über nichtkommutativen Ringen im allgemeinen nicht mehr sinnvoll vom Rang eines freien Moduls reden kann.

Ergänzende Übung 1.6.11. Für jeden Ring R und jede natürliche Zahl $n \geq 1$ liefert die Zuordnung $M \mapsto M^n$ eine Äquivalenz von Kategorien

$$R\text{-Mod} \xrightarrow{\sim} \mathrm{M}(n\times n;R)\text{-Mod}$$

In anderen Worten ist jeder Modul über $S = \mathrm{M}(n \times n; R)$ isomorph zu einem Modul der Gestalt M^n mit $M \in R\text{-Mod}$ und unsere Zuordnung induziert Bijektionen $\mathrm{Hom}_R(M,N) \xrightarrow{\sim} \mathrm{Hom}_S(M^n, N^n)$. Etwas allgemeiner ist für jeden freien R-Rechtsmodul V mit Endomorphismenring $E = \mathrm{End}_{-R}(V)$ die Zuordnung $M \mapsto V \otimes_R M$ eine Äquivalenz von Kategorien $R\text{-Mod} \xrightarrow{\sim} E\text{-Mod}$. Diese Aussagen sind im übrigen Spezialfälle unserer allgemeinen Überlegungen **??**.

Ergänzung 1.6.12. Es gibt Schiefkörper $K \subset L$ derart, daß L über K endlich erzeugt ist als Linksmodul, nicht aber als Rechtsmodul. Die Frage nach einem solchen Beispiel war lange als **Artin's Problem** bekannt. Eine explizite Konstruktion kann man in [Coh95] finden.

1.7 Noethersche Moduln und Ringe

Definition 1.7.1. Ein Modul über einem Ring heißt **noethersch** genau dann, wenn alle seine Untermoduln endlich erzeugt sind. Mit gemeint ist die Forderung, daß unser Modul selbst endlich erzeugt sein soll.

Definition 1.7.2. Ein Ring heißt **linksnoethersch** bzw. **rechtsnoethersch** genau dann, wenn er noethersch ist als Links- bzw. Rechtsmodul über sich selbst, und **noethersch** genau dann, wenn er linksnoethersch und rechtsnoethersch ist.

Beispiel 1.7.3. Ein Vektorraum über einem Körper k ist noethersch als k-Modul genau dann, wenn er endlichdimensional ist. Jeder Hauptidealring ist noethersch.

Beispiel 1.7.4. Der Polynomring $R = \mathbb{Z}[T_1, T_2, \ldots]$ in abzählbar vielen Variablen ist nicht noethersch, denn das von allen T_i erzeugte Ideal ist nicht endlich erzeugt. Um das zu sehen, zeigt man diese Aussage vielleicht noch leichter für den Quotienten dieses Ideals nach dem von allen T_iT_j erzeugten Unterideal.

Proposition 1.7.5. *Jeder Quotient und jeder Untermodul eines noetherschen Moduls ist noethersch. Besitzt ein Modul M einen noetherschen Untermodul M' derart, daß auch der Quotient M/M' noethersch ist, so ist bereits M selbst noethersch.*

1.7.6. Für diejenigen Leser, die mit exakten Sequenzen vertraut sind, können wir die Proposition auch wie folgt formulieren: Ist $M' \hookrightarrow M \twoheadrightarrow M''$ eine kurze exakte Sequenz von Moduln über einem Ring, so ist M noethersch genau dann, wenn M' und M'' noethersch sind.

Beweis. Der erste Teil bleibt dem Leser überlassen. Wir müssen im zweiten Teil zeigen, daß jeder Untermodul $U \subset M$ endlich erzeugt ist. Nach Annahme ist aber $\bar{U} \subset M/M'$ endlich erzeugt, wir finden also Elemente $u_1, \ldots, u_r \in U$, deren Bilder $\bar{U}$ erzeugen. Ganz genauso ist $U \cap M'$ endlich erzeugt, sagen wir von $v_1, \ldots, v_s \in U$, und dann sieht man leicht, daß die $u_1, \ldots, u_r, v_1, \ldots, v_s$ ganz U erzeugen. □

Übung 1.7.7. Jeder Quotient eines linksnoetherschen Rings ist linksnoethersch. Jeder Quotient eines rechtsnoetherschen Rings ist rechtsnoethersch. Jeder Quotient eines noetherschen Rings ist noethersch.

Satz 1.7.8. *Ein Modul über einem noetherschen Ring ist noethersch genau dann, wenn er endlich erzeugt ist.*

Beweis. Ein noetherscher Modul ist immer endlich erzeugt. Ist umgekehrt M endlich erzeugt, so ist M ein Quotient von R^n, und für R noethersch ist auch R^n noethersch nach 1.7.5. □

Beispiel 1.7.9. Dieser Satz zeigt insbesondere, daß jede Untergruppe einer endlich erzeugten abelschen Gruppe endlich erzeugt ist. In der Tat ist ja eine abelsche Gruppe dasselbe wie ein $\mathbb{Z}$-Modul, und $\mathbb{Z}$ ist ein Hauptidealring, also noethersch.

Satz 1.7.10 (Hilbert'scher Basissatz). *Ist R ein linksnoetherscher Ring, so ist auch der Polynomring $R[T]$ über R linksnoethersch. Dasselbe gilt auch für rechtsnoethersch und noethersch.*

Beweis. Sei $I \subset R[T]$ ein Linksideal. Wir betrachten das Linksideal $\mathfrak{a} \subset R$, das erzeugt wird von den Leitkoeffizienten aller Polynome aus I. Da R noethersch ist, gibt es endlich viele Polynome $f_1, \ldots, f_t \in I$, deren Leitkoeffizienten das Linksideal $\mathfrak{a} \subset R$ erzeugen. Sei m das Maximum der Grade der f_i. Gegeben $h \in I$ mit $\deg h \geq m$ finden wir offensichtlich $p_i \in R[T]$ derart, daß

$$h - (p_1 f_1 + \ldots + p_t f_t)$$

echt kleineren Grad hat als h. Induktiv finden wir dann sogar p_i derart, daß diese Differenz echt kleineren Grad hat als m. Die Polynome aus $R[T]$ vom Grad $< m$ und dann auch die Polynome aus I vom Grad $< m$ bilden aber einen endlich erzeugten R-Modul, und wählen wir Erzeuger $g_1, \ldots, g_r$ dieses R-Moduls, so erzeugen offensichtlich $f_1, \ldots, f_t, g_1, \ldots, g_r$ unser Linksideal I über $R[T]$. □

1.7.11. Insbesondere ist also ein Polynomring $K[T_1, \ldots, T_n]$ in endlich vielen Variablen über einem Körper K noethersch.

Lemma 1.7.12. *Für einen Modul sind gleichbedeutend:*

1. *Unser Modul ist noethersch, als da heißt, jeder Untermodul ist endlich erzeugt.*

2. *Jedes nichtleere System von Untermoduln unseres Moduls besitzt ein maximales Element.*

3. *Jede aufsteigende Folge $M_0 \subset M_1 \subset \ldots$ von Untermoduln unseres Moduls wird stationär.*

1.7.13. Ein Ring ist insbesondere linksnoethersch genau dann, wenn jede aufsteigende Folge von Linksidealen stationär wird.

Beweis. $(1) \Rightarrow (3)$: Sei M unser Modul. Ist jeder Untermodul von M endlich erzeugt, so auch die Vereinigung $\bigcup_{i=0}^{\infty} M_i$ über unsere aufsteigende Folge von Untermoduln. Es gibt also ein j derart, daß alle Erzeuger dieser Vereinigung schon in M_j liegen, und dann gilt notwendig $M_j = M_{j+1} = \ldots = \bigcup_{i=0}^{\infty} M_i$.

$(3) \Rightarrow (1)$: Ist ein Untermodul $N \subset M$ nicht endlich erzeugt, so finden wir induktiv eine Folge $m_0, m_1, \ldots$ in N derart, daß für jedes $i \geq 0$ das i-te Folgenglied m_i nicht im Erzeugnis der vorhergehenden $m_0, m_1, \ldots, m_{i-1}$ liegt. Die $M_i = \langle m_0, m_1, \ldots, m_i \rangle$ bilden dann eine aufsteigende Folge von Untermoduln von M, die nicht stationär wird.

$(2) \Leftrightarrow (3)$: Offensichtlich besitzt in einer partiell geordneten Menge jede nichtleere Teilmenge mindestens ein maximales Element genau dann, wenn jede monoton wachsende Folge in unserer Menge stationär wird. Diese Erkenntnis gilt es anzuwenden auf das System alias die Menge aller Untermoduln unseres Moduls. □

1.8 Moduln über Hauptidealringen

Satz 1.8.1 (Elementarteilersatz). *Sei f ein Homomorphismus zwischen zwei freien Moduln endlichen Ranges über einem Kring, in dem jedes Ideal ein Hauptideal ist. So gilt:*

1. *Es gibt angeordnete Basen $\mathcal{A}, \mathcal{B}$ unserer Moduln, derart, daß die darstellende Matrix $D := {}_{\mathcal{B}}[f]_{\mathcal{A}}$ eine (nicht notwendig quadratische) Diagomalmatrix ist, deren vordere Diagonaleinträge jeweils die hinteren teilen, in Formeln $d_{11}|d_{22}|\ldots|d_{rr}$ für r das Minimum der beiden Ränge.*

2. *Ist unser Kring zusätzlich ein Integritätsbereich, so sind die Diagonaleinträge d_{ii} einer derartigen darstellenden Matrix durch die Abbildung f wohlbestimmt bis auf Multiplikation mit Einheiten.*

1.8.2. Den Körperfall kennen wir bereits aus II.1.10.11, den Fall des Hauptidealrings $\mathbb{Z}$ aus II.7.4.11, den Fall eines Polynomrings aus II.7.4.22.

1.8.3. Nach unserer Definition III.2.3.9 ist ein Hauptidealring ein kommutativer Integritätsbereich, in dem jedes Ideal ein Hauptideal ist. Wir können unseren Satz auch verstehen als die Beschreibung eines Systems von Repräsentanten für die

Bahnen der offensichtlichen Wirkung der Gruppe $\mathrm{GL}(n;R) \times \mathrm{GL}(m;R)$ auf der Menge $\mathrm{M}(n \times m;R)$ für Hauptidealringe R.

Beweis. Wir dürfen $E = R^m$ und $F = R^n$ annehmen. Die Abbildung f wird beschrieben durch eine Matrix $A \in \mathrm{M}(n \times m;R)$ und es gilt, invertierbare Matrizen $P \in \mathrm{M}(n \times n;R)$ und $Q \in \mathrm{M}(m \times m;R)$ zu finden derart, daß $PAQ = D$ diagonal ist von der gewünschten Form. Für eine Matrix A bezeichne $\langle A \rangle \subset R$ das von den Einträgen von A erzeugte Ideal. Sicher gilt $\langle XA \rangle \subset \langle A \rangle$ für jede Matrix X, also $\langle XA \rangle = \langle A \rangle$ für X invertierbar. Ebenso gilt $\langle AY \rangle \subset \langle A \rangle$ für jede Matrix Y und $\langle AY \rangle = \langle A \rangle$ für Y invertierbar. Wir geben im folgenden ein Verfahren an, das im Fall $\langle a_{11} \rangle \neq \langle A \rangle$ invertierbare Matrizen X und Y liefert derart, daß der obere linke Eintrag von XAY ein echt größeres Ideal erzeugt als a_{11}. Mit Induktion finden wir dann sogar $\tilde{X}$ und $\tilde{Y}$ invertierbar derart, daß der obere linke Eintrag von $\tilde{X}A\tilde{Y}$ das Ideal $\langle \tilde{X}A\tilde{Y} \rangle = \langle A \rangle$ erzeugt, d.h. daß er alle Einträge von $\tilde{X}A\tilde{Y}$ teilt. Da nun Zeilen- und Spaltenoperationen auch durch Multiplikation mit invertierbaren Matrizen von links bzw. rechts gegeben werden, finden wir dann sogar invertierbare Matrizen $\hat{X}, \hat{Y}$ derart, daß $\hat{X}A\hat{Y}$ außer einem Eintrag $a_{11} = d_{11}$ in der oberen linken Ecke nur Nullen in der ersten Zeile und erste Spalte stehen hat und daß zusätzlich gilt $\langle d_{11} \rangle = \langle A \rangle$. Dann können wir aber den Beweis beenden mit einer offensichtlichen Induktion. Es bleibt, das versprochene Verfahren anzugeben. Wir unterscheiden drei Fälle.

(i) Falls a_{11} nicht alle Elemente der ersten Zeile teilt, sagen wir a_{11} teilt nicht a_{12}, so betrachten wir das Ideal $\langle a_{11}, a_{12} \rangle$ und wählen dafür einen Erzeuger d. Wir können nun schreiben $d = xa_{11} + ya_{12}$ sowie zusätzlich $a_{11} = d\lambda, a_{12} = d\mu$ und folgern $1 = x\lambda + y\mu$. Jetzt beachten wir

$$\left(\begin{array}{cc|c} a_{11} & a_{12} & * \\ * & * & \\ \hline * & & * \end{array}\right) \left(\begin{array}{cc|c} x & -\mu & 0 \\ y & \lambda & \\ \hline 0 & & I \end{array}\right) = \left(\begin{array}{cc|c} d & * & * \\ * & * & \\ \hline * & & * \end{array}\right)$$

mit I der Einheitsmatrix und haben schon gewonnen.

(ii) Falls a_{11} nicht alle Elemente der ersten Spalte teilt, gehen wir analog vor.

(iii) Teilt a_{11} alle Elemente der ersten Zeile und der ersten Spalte, so finden wir schon mal invertierbare X, Y derart, daß XAY außer einem Eintrag a_{11} in der oberen linken Ecke nur Nullen in der ersten Zeile und der ersten Spalte stehen hat. Unter der Annahme $\langle a_{11} \rangle \neq \langle A \rangle$ kann aber a_{11} nicht alle Einträge von A teilen. Addieren wir nun eine geeignete Zeile zur ersten Zeile, so landen wir im Fall (i) und haben wieder gewonnen.

Damit haben wir das versprochene Verfahren angegeben und Teil 1 ist gezeigt.

2. Wir zeigen nun die Eindeutigkeit der Diagonaleinträge bis auf Einheiten. Dazu betrachten wir für $i \geq 1$ das von allen Determinanten von $(i \times i)$-Untermatrizen von A erzeugte Ideal $J_i(A)$. Ist X eine weitere Matrix, so gilt $J_i(XA) \subset J_i(A)$, denn die Zeilen von XA sind Linearkombinationen von Zeilen von A. Insbesondere gilt also $J_i(XA) = J_i(A)$ für invertierbares X und ebenso $J_i(AY) = J_i(A)$ für invertierbares Y. Es folgt sofort, daß $J_i(A)$ das vom Produkt $d_{11}d_{22}\cdots d_{ii}$ erzeugte Ideal ist, in Formeln $J_i(A) = \langle d_{11}d_{22}\cdots d_{ii}\rangle$, und im nullteilerfreien Fall folgt daraus dann die Eindeutigkeit der d_{ii} bis auf Einheiten. □

1.8.4. Wir geben nun zwei Formen der Klassifikation endlich erzeugter Moduln über Hauptidealringen an. Wenden wir diese Klassifikationen an auf den Hauptidealring $\mathbb{Z}$, so erhalten wir die Klassifikation der endlich erzeugten abelschen Gruppen II.7.4.2 und II.7.4.3 vom Beginn der Vorlesung. Wenden wir unsere Sätze an auf einen Polynomring über einem algebraisch abgeschlossenen Körper, so ergibt sich die Jordan'sche Normalform II.6.5.6, wie als Korollar 1.8.10 ausgeführt wird.

Satz 1.8.5 (Klassifikation durch Idealketten). *Ist M ein endlich erzeugter Modul über einem Hauptidealring R, so gibt es genau eine aufsteigende Kette $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \ldots \subset \mathfrak{a}_s \subset R$ von Idealen von R mit $\mathfrak{a}_s \neq R$ und*

$$M \cong R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_s$$

Der Nullmodul wird abgedeckt durch den Fall $s = 0$.

1.8.6. Ist R ein faktorieller Ring, so nennen wir die Potenzen irreduzibler Elemente von R auch die **Primpotenzen** von R. Jede Primpotenz q hat also die Form $q = p^e$ mit p irreduzibel und $e \geq 1$. Wir verwenden diesen Begriff bei der Darstellung einer zweiten Klassifikation derselben Objekte.

Ergänzung 1.8.7. Die Existenz ist mir auch klar für Kringe, in denen jedes Ideal ein Hauptideal ist. Aber wie steht es in dieser Allgemeinheit mit der Eindeutigkeit?

Satz 1.8.8 (Klassifikation durch Multimengen von Primpotenzen). *Ist M ein endlich erzeugter Modul über einem Hauptidealring R, so gibt es $r \in \mathbb{N}$ und Primpotenzen $q_1, \ldots, q_t \in R$ derart, daß gilt*

$$M \cong R^r \times R/q_1R \times \ldots \times R/q_tR$$

Hier ist r wohlbestimmt und die q_i sind wohlbestimmt bis auf Einheiten und Reihenfolge. Der Nullmodul wird abgedeckt durch den Fall $r = t = 0$.

1.8.9. Der Beweis beider Sätze ist mutatis mutandis derselbe wie der Beweis ihrer als II.7.4.2 und II.7.4.3 diskutierten Spezialisierungen für den Hauptidealring $\mathbb{Z}$ der ganzen Zahlen.

Beweis von 1.8.5. Gegeben ein Erzeugendensystem $g_1, \ldots, g_n$ von M erklären wir durch die Vorschrift $(a_1, \ldots, a_n) \mapsto a_1 g_1 + \ldots + a_n g_n$ einen surjektiven Modulhomomorphismus

$$R^n \twoheadrightarrow M$$

Dessen Kern ist nach 1.7.8 ein endlich erzeugter R-Modul K, für den wir wieder einen surjektiven Homomorphismus $R^m \twoheadrightarrow K$ finden können. Mit der Komposition $R^m \twoheadrightarrow K \hookrightarrow R^n$ als erster Abbildung entsteht so eine im Sinne von II.7.5.2 exakte Sequenz von R-Moduln

$$R^m \to R^n \to M \to 0$$

Nach 1.6.3 sind die Homomorphismen $R^m \to R^n$ genau die Multiplikationen von links mit $(n \times m)$-Matrizen mit Einträgen in R. Weiter überlegt man sich, daß auch in dieser Situation die Verknüpfung von Homomorphismen der Multiplikation von Matrizen entspricht. Bezeichnet nun A die Matrix unserer Abbildung $R^m \to R^n$ und wählen wir P und Q wie im Elementarteilersatz oder vielmehr dem Beginn seines Beweises, so ergibt sich ein kommutatives Diagramm von R-Moduln

$$\begin{array}{ccc} R^m & \xrightarrow{A\circ} & R^n \\ {\scriptstyle Q\circ}\uparrow\wr & & \wr\downarrow{\scriptstyle P\circ} \\ R^m & \xrightarrow{D\circ} & R^n \end{array}$$

für eine nicht notwendigerweise quadratische Diagonalmatrix D mit Einträgen $d_1|d_2|\ldots|d_r$ für $r = \min(m,n)$. Bilden wir nun andererseits das Produkt der exakten Sequenzen $R \xrightarrow{d_i} R \to R/\langle d_i\rangle \to 0$ für $1 \leq i \leq r$ mit $m-r$ Kopien der exakten Sequenzen $R \to 0 \to 0 \to 0$ im Fall $m > n$ bzw. $n-r$ Kopien der exakten Sequenzen $0 \to R \xrightarrow{\mathrm{id}} R \to 0$ im Fall $n > m$, so erhalten wir mit II.7.5.6 die untere Horizontale in einem kommutativen Diagramm mit exakten Zeilen

$$\begin{array}{ccccccc} R^m & \xrightarrow{A\circ} & R^n & \longrightarrow & M & \longrightarrow & 0 \\ {\scriptstyle Q\circ}\uparrow\wr & & \wr\downarrow{\scriptstyle P\circ} & & & & \downarrow \\ R^m & \xrightarrow{D\circ} & R^n & \longrightarrow & R/\langle d_1\rangle \times \ldots \times R/\langle d_r\rangle \times R^{n-r} & \longrightarrow & 0 \end{array}$$

Damit liefert II.7.5.5 oder vielmehr eine offensichtliche Variante dieses Resultats für Moduln einen Isomorphismus $M \xrightarrow{\sim} R/\langle d_1\rangle \times \ldots \times R/\langle d_r\rangle \times R^{n-r}$. Lassen wir von unserer Folge $d_1|d_2|\ldots|d_r$ alle Einheiten vorne weg und ergänzen am Ende $(n-r)$ Nullen und drehen die Nummerierung um, so erhalten wir eine Folge $a_s|\ldots|a_1$ derart, daß die von ihren Gliedern erzeugten Ideale eine Kette bilden wie im Satz 1.8.5 gefordert, und die Existenz dort ist gezeigt. Um die Eindeutigkeit zu zeigen bemerken wir, daß für jeden endlich erzeugten R-Modul M und jedes

irreduzible Element p und alle $n \geq 1$ der Quotient $p^{n-1}M/p^nM$ nach 1.3.10 ein endlichdimensionaler Vektorraum über dem Restklassenring $R/\langle p\rangle$ ist, der hinwiederum nach III.2.3.27 ein Körper sein muß. Wir notieren seine Dimension

$$D_p^n(M) := \dim_{R/\langle p\rangle}(p^{n-1}M/p^nM)$$

Man folgert unmittelbar $D_p^n(M \times N) = D_p^n(M) + D_p^n(N)$ für je zwei endlich erzeugte R-Moduln M und N. Für zyklische R-Moduln $M \cong R/aR$ behaupten wir nun

$$D_p^n(R/aR) \quad = \quad \begin{cases} 1 & p^n \text{ teilt } a; \\ 0 & \text{sonst.} \end{cases}$$

In der Tat ist das klar für $a = p^m$, für a teilerfremd zu p ist es eh klar, und mit dem chinesischen Restsatz III.2.2.4 folgt es im allgemeinen. Für eine Zerlegung $M \cong R/\langle d_1\rangle \times \ldots \times R/\langle d_s\rangle$ wie in 1.8.5 finden wir also

$$D_p^n(M) = |\{i \mid p^n \text{ teilt } d_i\}|$$

Die Zahl der Nullen unter unseren d_i wird damit für jedes p gegeben durch die Formel $|\{i \mid d_i = 0\}| = \lim_{n\to\infty} D_p^n(M)$, und welche Potenz von jedem irreduziblen Element p in jedem von Null verschiedenen d_i stecken muß, kann man offensichtlich an den Zahlen $D_p^n(M)$ auch ablesen. Folglich hängen die Ideale $\langle d_i\rangle$ nur von M und nicht von der gewählten Zerlegung ab. □

Beweis. Aus 1.8.5 folgt sofort die Existenzaussage in Satz 1.8.8, indem wir im Fall $\mathfrak{a}_i \neq 0$ einen Erzeuger d_i von $\mathfrak{a}_i$ als Produkt von paarweise teilerfremden Primpotenzen $d_i = q_1 \ldots q_k$ schreiben und mit dem chinesischen Restsatz zerlegen

$$R/\mathfrak{a}_i \cong R/q_1R \times \ldots \times R/q_kR$$

Für die Eindeutigkeit argumentieren wir wie im vorhergehenden Beweis: Für $M \cong R^r \times R/q_1R \times \ldots \times R/q_tR$ wie in 1.8.8 finden wir diesmal

$$D_p^n(M) = r + |\{i \mid p^n \text{ teilt } q_i\}|$$

Wenden wir diese Erkenntnis an auf alle irreduziblen Elemente p, so folgt die im Satz behauptete Eindeutigkeit ohne weitere Schwierigkeiten: Die Zahl der Primpotenzen q_i, die bis auf eine Einheit p^n sind, muß nämlich bei jeder Zerlegung gerade $D_p^n(M) - D_p^{n+1}(M)$ sein, und den Rang r des freien Anteils können wir als die auch von allen Wahlen unabhängige Zahl $r = \lim_{n\to\infty} D_p^n(M)$ beschreiben, für jedes irreduzible Element p. □

Korollar 1.8.10 (Jordan'sche Normalform). *Sei V ein endlichdimensionaler Vektorraum über einem algebraisch abgeschlossenen Körper k und sei $A : V \to$*

V eine lineare Abbildung. So gibt es eine Basis von V derart, daß die Matrix von A bezüglich dieser Basis blockdiagonal ist, wobei die Blöcke konstant sind auf der Diagonale, konstant Eins auf der ersten oberen Nebendiagonale, und Null an allen anderen Stellen.

Bemerkung 1.8.11. Das ist genau Satz II.6.5.6 aus der linearen Algebra.

Beweis. Mithilfe von 1.2.10 fassen wir V als $k[X]$-Modul auf und mit 1.8.8 finden wir einen Isomorphismus von $k[X]$-Moduln

$$V \cong k[X]/\langle (X-\lambda_1)^{n_1}\rangle \times \ldots \times k[X]/\langle (X-\lambda_t)^{n_t}\rangle$$

Wählen wir auf der rechten Seite im Summanden $k[X]/\langle (X-\lambda)^n\rangle$ als angeordnete Basis die Nebenklassen von $(X-\lambda)^{n-1}, \ldots, (X-\lambda)$ und 1, so erhält man die Matrix der Multiplikation mit X, indem man zunächst die Matrix der Multiplikation mit $(X-\lambda)$ berechnet und dann die Diagonalmatrix λI addiert. So erkennt man dann leicht, daß die Matrix der Multiplikation mit X die gewünschte Form hat. □

1.8.12. Auf ähnliche Weise erhält man auch Normalformen für die Matrizen von Endomorphismen über nicht notwendig algebraisch abgeschlossenen Körpern, wie in den folgenden Übungen ausgeführt wird.

Übung 1.8.13. Jedes normierte Polynom $P \in k[X]$ ist bis auf Vorzeichen das charakteristische Polynom der k-linearen Abbildung $(X\cdot) : k[X]/\langle P\rangle \to k[X]/\langle P\rangle$. Hat unser Polynom die Gestalt $P = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$, so bilden die Nebenklassen von $1, X, \ldots, X^{n-1}$ eine angeordnete Basis des Quotienten, und in Bezug auf diese Basis hat die durch Multiplikation mit X gegebene k-lineare Abbildung die in nebenstehender Abbildung angegebene Matrix. Hinweis: Eine Methode ist die explizite Berechnung mithilfe der Determinante. Alternativ mag man k algebraisch abgeschlossen annehmen und sich mithilfe des chinesischen Restsatzes auf den Fall zurückziehen, daß P eine Potenz eines linearen Polynoms ist.

Ergänzende Übung 1.8.14. Sei $A : V \to V$ ein Endomorphismus eines endlichdimensionalen Vektorraums über einem Körper k. Man zeige: Genau dann hat A das charakteristische Polynom P, wenn es eine Faktorisierung $P = Q_1 \ldots Q_r$ gibt derart, daß der (V, A) entsprechende $k[X]$-Modul isomorph ist zu

$$k[X]/\langle Q_1\rangle \times \ldots \times k[X]/\langle Q_r\rangle$$

Man nutze diese Erkenntnis, um einen alternativen Beweis des Satzes von Cayley-Hamilton II.3.5.21 zu geben. Hinweis: 1.8.13 und 1.8.5 oder 1.8.8. In anderen

Illustration zu 1.8.13

Worten kann das Aufmultiplizieren einer endlichen Multimenge von Null verschiedener Polynome bis auf eine multiplikative Konstante aus $k^\times$ demnach geschrieben werden als die Verknüpfung

$$\begin{array}{ccc}
\{Q_1,\ldots,Q_r\} & \in & \left\{ \begin{array}{c} \text{endliche Multimengen} \\ \text{von Polynomen aus } k[X]\backslash 0 \end{array} \right\} \\
\downarrow & & \downarrow \\
k[X]/\langle Q_1\rangle \times \ldots \times k[X]/\langle Q_r\rangle & \in & \left\{ \begin{array}{c} \text{endlichdimensionale} \\ k[X]\text{-Moduln} \end{array} \right\} \\
& & \downarrow \\
(V,A) & \in & \left\{ \begin{array}{c} \text{endlichdimensionale} \\ k\text{-Vektorräume } V \\ \text{mit Endomorphismus} \end{array} \right\} \\
\downarrow & & \downarrow \\
\chi_A & \in & k[X]
\end{array}$$

mit unserer Entsprechung $M \mapsto (M,(X\cdot))$ aus 1.2.10 als mittlerem Pfeil.

Ergänzende Übung 1.8.15. Sei $A : V \to V$ ein Endomorphismus eines Vektorraums über einem Körper k. Man zeige: Genau dann entspricht (V,A) einem $k[X]$-Modul der Gestalt $k[X]/\langle P\rangle$ für ein Polynom $P \in k[X]$, wenn es einen Vektor $v \in V$ gibt derart, daß die $A^i v$ den Vektorraum V erzeugen. Ein derartiger Vektor heißt auch ein **zyklischer Vektor**.

Ergänzende Übung 1.8.16. Sei $A : V \to V$ ein Endomorphismus eines endlichdimensionalen Vektorraums über einem Körper k. Man zeige: Kommen im charakteristischen Polynom χ_A von A keine k-irreduziblen Faktoren mehrfach vor, so entspricht (V,A) dem $k[X]$-Modul $k[X]/\langle\chi_A\rangle$.

2 Darstellungstheorie endlicher Gruppen

2.1 Halbeinfache Moduln und Ringe

Definition 2.1.1. Ein Modul heißt **halbeinfach** genau dann, wenn er die Summe seiner einfachen Untermoduln ist, in anderen Worten also das Erzeugnis der Vereinigung seiner einfachen Untermoduln. Ein Ring heißt **halbeinfach** genau dann, wenn er halbeinfach ist als Linksmodul über sich selber.

2.1.2. Aus dem Satz über die Struktur halbeinfacher Ringe 2.1.20 wird folgen, daß ein Ring halbeinfach ist genau dann, wenn der opponierte Ring halbeinfach ist. Jeder Vektorraum alias Modul über einem Körper ist halbeinfach nach 1.4.2. Der Gruppenring einer endlichen Gruppe über einem Körper oder sogar Schiefkörper, dessen Charakteristik die Gruppenordnung nicht teilt, ist halbeinfach nach dem Satz von Maschke 2.6.1. Unter einem **einfachen Ring** verstehen wir dahingegen einen Ring, der nicht Null ist und außer Null und dem ganzen Ring keine weiteren zweiseitigen Ideale besitzt. Diese Terminologie ist mit der eben in 2.1.1 eingeführten Terminologie nicht gut verträglich, da einfache Ringe keineswegs halbeinfach als Linksmodul zu sein brauchen. Ein einfacher Ring R ist vielmehr einfach als Modul über dem Produktring $R \times R^{\mathrm{opp}}$, dessen Operation auf R dabei durch simultane Links- und Rechtsmultiplikation zu verstehen ist. Zum Beispiel erhält man einen einfachen Ring, wenn man den Quotienten des Endomorphismenrings eines Vektorraums abzählbarer Dimension nach dem Ideal aller Endomorphismen endlichen Ranges betrachtet, wie der Leser zur Übung selbst prüfen mag. Dieser Ring E ist jedoch als Linksmodul über sich selber mit denselben Argumenten wie in 1.5.10 isomorph zu E^2, folglich kann er nach 2.1.8 nicht halbeinfach sein. In der Literatur wird auch oft unter einem "einfachen Ring" das verstanden, was in der hier gewählten Terminologie als ein "halbeinfacher einfacher Ring" zu bezeichnen ist.

Ergänzende Übung 2.1.3. Gegeben $m \geq 1$ ist $\mathbb{Z}/m\mathbb{Z}$ ein halbeinfacher $\mathbb{Z}$-Modul genau dann, wenn kein Primfaktor in m mehrfach vorkommt.

Ergänzende Übung 2.1.4. Ein $\mathbb{C}[X]$-Modul M ist halbeinfach genau dann, wenn der durch Multiplikation mit X gegebene Endomorphismus des $\mathbb{C}$-Vektorraums M diagonalisierbar ist, als da heißt, wenn M eine Basis aus Eigenvektoren besitzt. Dasselbe gilt im Fall von $k[X]$-Moduln für jeden algebraisch abgeschlossenen Körper k. Hinweis: 1.4.8. Ist k ein vollkommener Körper und $\bar{k}$ ein algebraischer Abschluß, so ist ein $k[X]$-Modul halbeinfach genau dann, wenn der durch Erweiterung der Skalare entstehende $\bar{k}[X]$-Modul halbeinfach ist. Ist k nicht vollkommen, so gilt das nicht mehr.

2.1.5. Zwei Untermoduln $U, D \subset M$ eines Moduls heißen **komplementär** und wir schreiben $M = U \oplus D$ genau dann, wenn die Addition einen Isomorphismus

$U \oplus D \xrightarrow{\sim} M$ liefert. Dafür hinreichend und notwendig ist, daß sowohl gilt $U \cap D = 0$ als auch $U + D = M$. Wir sagen in dem Fall auch, M sei die **direkte Summe** von U und D und D sei ein **Komplement** von U in M. Analoge Begriffsbildungen benutzen wir auch für beliebige Familien von Untermoduln eines Moduls.

Proposition 2.1.6 (Charakterisierung halbeinfacher Moduln). *Sei R ein Ring und M ein R-Modul. So sind gleichbedeutend:*

1. *M ist halbeinfach alias die Summe seiner einfachen Untermoduln;*
2. *M ist eine direkte Summe von einfachen Untermoduln;*
3. *Jeder Untermodul von M besitzt ein Komplement in M.*

Beweis. $2 \Rightarrow 1$: Das ist klar.

$1 \Rightarrow 3$: Sei $M = \sum_{i \in I} M_i$ das Erzeugnis einer Familie von einfachen Untermoduln $M_i \subset M$ und sei $U \subset M$ der Untermodul, für den wir ein Komplement suchen. Gegeben $J \subset I$ setzen wir $M_J = \sum_{i \in J} M_i$. Ist I endlich, so finden wir natürlich unter allen Teilmengen $J \subset I$ mit $M_J \cap U = 0$ eine bezüglich Inklusion maximale Teilmenge. Ist I unendlich, so folgt die Existenz eines solchen maximalen J mit dem Zorn'schen Lemma. In jedem Fall behaupten wir für solch ein maximales J, daß gilt $M_J \oplus U = M$. In der Tat, aus $M_J + U \neq M$ folgt, daß es ein $i \in I$ gibt mit $M_i \not\subset (M_J + U)$, also $M_i \cap (M_J + U) = 0$ da M_i einfach ist. Dann folgt aber $(M_i + M_J) \cap U = 0$ und J war nicht maximal.

$3 \Rightarrow 2$: Wir bemerken zunächst, daß sich die Eigenschaft 3 auf Untermoduln vererbt: Sind nämlich $U \subset N \subset M$ Untermoduln und ist V ein Komplement von U in M, so ist notwendig $V \cap N$ ein Komplement von U in N. Jetzt finden wir mithilfe des Zorn'schen Lemmas eine maximale Menge von einfachen Untermoduln derart, daß ihre Summe in M direkt ist. Wäre diese Summe S nicht ganz M, so fänden wir ein von Null verschiedenes Komplement D von S in M. In diesem Komplement D gäbe es einen von Null verschiedenen zyklischen Untermodul $Z \subset D$, und der hätte nach 1.4.7 seinerseits einen einfachen Quotienten $Z \twoheadrightarrow Q$. Nun hat diese Surjektion einen Kern $K \subset Z$ und der hat ein Komplement $F \subset Z$, und wegen mit $F \cong Q$ ist F einfach. Das aber steht im Widerspruch zur Maximalität von S. □

2.1.7. Beim Nachweis der Implikation $1 \Rightarrow 3$ im vorhergehenden Beweis hätten wir natürlich auch gleich mit der Familie aller einfachen Untermoduln arbeiten können. Ich hoffe jedoch, daß man anhand des oben gegebenen Arguments besser nachvollziehen kann, in welchen Fällen das Zorn'sche Lemma wirklich benötigt wird.

Übung 2.1.8. Jeder halbeinfache Ring zerfällt als Linksmodul über sich selber in eine direkte Summe von endlich vielen einfachen Untermoduln. Hinweis: Man betrachte die zu einer Zerlegung in eine direkte Summe gehörige Zerlegung der Eins.

Korollar 2.1.9. *Jeder Quotient und jeder Untermodul eines halbeinfachen Moduls ist halbeinfach.*

Beweis. Natürlich ist jeder Quotient eine Summe einfacher Untermoduln und ist damit halbeinfach nach 2.1.6. Weiter besitzt nach 2.1.6 jeder Untermodul ein Komplement und ist damit auch isomorph zu einem Quotienten unseres Moduls, nämlich zu dem Quotienten nach besagtem Komplement. Alternativ kann man sich daran erinnern, daß wir beim Beweis von $3 \Rightarrow 1$ in 2.1.6 bereits gezeigt hatten, daß sich die Eigenschaft 3 auf Untermoduln vererbt. □

Übung 2.1.10. Man zeige, daß jeder Linksmodul über einem halbeinfachen Ring halbeinfach ist.

Definition 2.1.11. Sei R ein Ring und M ein R-Modul. Gegeben ein einfacher R-Modul E notieren wir $M_E \subset M$ die Summe aller zu E isomorphen Untermoduln von M und nennen sie die **isotypische Komponente von** M **vom Typ** E.

Satz 2.1.12 (Zerlegung in isotypische Komponenten). *Sei R ein Ring, M ein halbeinfacher R-Modul und $\operatorname{irr}(R)$ ein Repräsentantensystem für die Isomorphieklassen einfacher R-Moduln. So zerfällt M als die direkte Summe seiner isotypischen Komponenten*

$$M = \bigoplus_{E \in \operatorname{irr}(R)} M_E$$

Beweis. Da M nach Annahme halbeinfach ist, muß nur gezeigt werden, daß die Summe der isotypischen Komponenten direkt ist, daß also gilt

$$M_E \cap \sum_{F \neq E} M_F = 0$$

für alle E. Dazu hinwiederum brauchen wir nur zu zeigen, daß jeder einfache Untermodul einer Summe von einfachen Untermoduln zu einem der Summanden isomorph ist. Da aber besagte Summe halbeinfach ist, ist unser einfacher Untermodul auch ein Quotient dieser Summe und damit notwendig auch ein Quotient eines Summanden. □

2.1.13. Das Erzeugnis der Vereinigung aller einfachen Untermoduln eines Moduls M heißt der **Sockel von** M und wird notiert $\operatorname{soc} M$. Der Sockel ist natürlich der größte halbeinfache Untermodul.

Übung 2.1.14. Jeder Homomorphismus von Moduln erhält die isotypischen Komponenten. Eine Sequenz $M' \to M \to M''$ von halbeinfachen Moduln ist exakt genau dann, wenn für alle einfachen Moduln die induzierte Sequenz $M'_E \to M_E \to M''_E$ exakt ist.

Übung 2.1.15. Man gebe einen halbeinfachen $\mathbb{Z}$-Modul mit genau tausend Elementen an.

Ergänzende Übung 2.1.16. Man bestimme die isotypischen Komponenten des $\mathbb{Z}$-Moduls $\mathbb{Z}/30\mathbb{Z}$.

Ergänzende Übung 2.1.17. Man erkläre, inwiefern die Zerlegung eines halbeinfachen Moduls in isotypische Komponenten die Eigenraumzerlegung eines Vektorraums unter einem diagonalisierbaren Endomorphismus verallgemeinert. Hinweis: 2.1.4.

Ergänzende Übung 2.1.18. Man zeige: Besitzt ein einfacher Ring ein Linksideal, das als Linksmodul einfach ist, so ist unser Ring bereits halbeinfach.

Ergänzende Übung 2.1.19. Jeder Ring $\mathrm{M}(n \times n; D)$ von endlichen quadratischen Matrizen mit Koeffizienten in einem Schiefkörper D und $n \geq 1$ ist einfach, und jeder halbeinfache einfache Ring ist isomorph zu einem derartigen Matrizenring für genau ein n und einen bis auf Isomorphismus wohlbestimmten Schiefkörper D. Das fragliche n heißt dann der **Goldie-Rang** unseres halbeinfachen einfachen Rings. Hinweis: 2.1.8, 2.1.6, 2.1.12, 1.6.5, 1.5.13. Wer spickeln will, kann auch in 2.1.20 nachsehen.

Satz 2.1.20 (Struktur halbeinfacher Ringe). *1. Jeder halbeinfache Ring besitzt bis auf Isomorphismus nur endlich viele einfache Moduln.*

2. *Der opponierte Ring eines halbeinfachen Rings ist stets auch wieder halbeinfach.*

3. *Jeder einfache Modul über einem halbeinfachen Ring ist endlichdimensional als Modul über dem Schiefkörper seiner Endomorphismen.*

4. *Ist $L_1, \ldots, L_r$ ein Vertretersystem für die Isomorphieklassen einfacher Moduln eines halbeinfachen Rings R und sind $D_i = \mathrm{End}_R L_i$ ihre Endomorphismenringe, so liefert die kanonische Abbildung einen Ringisomorphismus*

$$R \xrightarrow{\sim} (\mathrm{End}_{D_1} L_1) \times \ldots \times (\mathrm{End}_{D_r} L_r)$$

2.1.21. Die D_i müssen natürlich Schiefkörper sein. Umgekehrt zeigt man unschwer, daß jedes endliche Produkt von Matrizenringen über Schiefkörpern ein halbeinfacher Ring ist.

Beweis. Jeder halbeinfache Ring besitzt nach 2.1.8 bis auf Isomorphismus nur endlich viele einfache Moduln und zerfällt sogar in eine endliche direkte Summe von einfachen Moduln. Ist $L_1, \ldots, L_r$ ein Vertretersystem für die Isomorphieklassen einfacher Moduln und m_i deren jeweilige Vielfachheit, so haben wir also einen Isomorphismus von R-Linksmoduln $R \cong L_1^{m_1} \oplus \ldots \oplus L_r^{m_r}$. Sind $D_i = \operatorname{End}_R L_i$ die Endomorphismenringe unserer einfachen Moduln, so erhalten wir nach 1.6.5 und offensichtlichen Überlegungen Ringisomorphismen

$$R^{\mathrm{opp}} \xrightarrow{\sim} \operatorname{End}_R R \xleftarrow{\sim} \mathrm{M}(m_1 \times m_1; D_1) \times \ldots \times \mathrm{M}(m_r \times m_r; D_r)$$

Jeder halbeinfache Ring ist also isomorph zu einem endlichen Produkt von Ringen endlicher quadratischer Matrizen mit Einträgen in Schiefkörpern. Umgekehrt kann man auch leicht zeigen, daß alle Ringe dieser Gestalt halbeinfach sind. Insbesondere ist der opponierte Ring eines halbeinfachen Rings stets wieder halbeinfach. Nun ist nach 1.6.11 klar, daß gegeben ein Schiefkörper D und eine natürliche Zahl $m \geq 1$ jeder einfache Modul des Matrizenrings $\mathrm{M}(m \times m; D)$ isomorph ist zum Modul D^m von Spaltenmatrizen und jeder einfache Rechtsmodul isomorph zum Modul $\mathrm{M}(1 \times m; D)$ von Zeilenmatrizen, dessen Endomorphismenring hinwiederum D selber ist, nun aber durch Linksmultiplikation wirkend. Das zeigt die vorletzte Aussage. Die letzte Aussage folgt dann unmittelbar. □

2.2 Das Lemma von Schur

Satz 2.2.1 (Schur's sches Lemma). *Eine endlichdimensionale irreduzible Darstellung einer Gruppe über einem algebraisch abgeschlossenen Körper besitzt außer den Skalaren keine Endomorphismen.*

Beweis. Sei G unsere Gruppe, k unser algebraisch abgeschlossener Körper und V unsere endlichdimensionale irreduzible Darstellung. Der Satz behauptet in Formeln

$$k \xrightarrow{\sim} \operatorname{Mod}_k^G V$$

Nach Annahme gilt $V \neq 0$. Jedes $\varphi \in \operatorname{Mod}_k^G V$ besitzt also einen Eigenwert, sagen wir λ, und der zugehörige Eigenraum ist offensichtlich eine von Null verschiedene Unterdarstellung als Kern von $\varphi - \lambda \operatorname{id}$. Also muß dieser Kern schon ganz V sein und wir folgern $\varphi = \lambda \operatorname{id}$. □

Beispiel 2.2.2. Die Gruppe G der vierten Einheitswurzeln in $\mathbb{C}$ operiert durch Multiplikation auf dem $\mathbb{R}$-Vektorraum $\mathbb{C}$ und macht diesen zu einer irreduziblen Darstellung $V = \mathbb{C}$ von G über $k = \mathbb{R}$. Dennoch haben wir in diesem Fall $k \neq \operatorname{Mod}_k^G V$. Das steht nicht in Widerspruch zu unserem Satz, da $k = \mathbb{R}$ nicht algebraisch abeschlossen ist.

Beispiel 2.2.3. Ist $k \subset L$ ein Körpererweiterung, so wird $V = L$ eine irreduzible Darstellung der Gruppe $G = L^\times$ über k. In diesem Fall haben wir offensichtlich $\mathrm{End}_{kG} V = L$ und im allgemeinen kann natürlich $k \neq L$ gelten selbst wenn k algebraisch abgeschlossen ist, zum Beispiel mit $L = k(X)$. Das steht jedoch auch nicht in Widerspruch zu unserem Satz, da unter der Voraussetzung k algebraisch abgeschlossen notwendig gilt $\dim_k L = \infty$.

Übung 2.2.4. Sei R ein Ring und $k \subset R$ ein algebraisch abgeschlossener Körper derart, daß gilt $ar = ra \ \forall a \in k, r \in R$. So gilt für jeden einfachen R-Modul M, der endlichdimensional ist als k-Vektorraum, notwendig $k \xrightarrow{\sim} \mathrm{End}_R M$.

Übung 2.2.5. Jede endlichdimensionale irreduzible Darstellung einer abelschen Gruppe über einem algebraisch abgeschlossenen Körper ist eindimensional. Hinweis: Jedes Gruppenelement operiert in diesem Fall durch einen Endomorphismus unserer Darstellung.

2.2.6. Die nun folgenden Verallgemeinerungen sind für die Darstellungstheorie endlicher Gruppen ohne Bedeutung. Ihr Beweis benötigt stärkere Resultate der Mengenlehre.

Satz 2.2.7 (Schur'sches Lemma). *Sei R ein Ring und $k \subset R$ ein algebraisch abgeschlossener Körper mit $ar = ra \ \forall a \in k, r \in R$. So liefert für jeden einfachen R-Modul E, dessen Dimension als k-Vektorraum echt kleiner ist als die Kardinalität von k, die Abbildung $a \mapsto a \,\mathrm{id}_E$ einen Isomorphismus*

$$k \xrightarrow{\sim} \mathrm{End}_R E$$

2.2.8. Insbesondere besitzt eine irreduzible Darstellung einer Gruppe über einem algebraisch abgeschlossenen Körper, deren Dimension echt kleiner ist als die Kardinalität des Körpers, außer den Skalaren keine Endomorphismen.

Beweis. Das Anwenden auf ein beliebiges von Null verschiedenes Element definiert ein Injektion $(\mathrm{Mod}_R E) \hookrightarrow E$. Die Dimension des Endomorphismenrings von E über k ist folglich höchstens so groß wie die Dimension von E über k. Unser Endomorphismenring ist jedoch auch ein Schiefkörper. Wäre er echt größer als k, so müßte er den Funktionenkörper $k(X)$ umfassen, in dem die Familie der $((X-\lambda)^{-1})_{\lambda \in k}$ etwa nach III.3.4.17 linear unabhängig ist über k, im Widerspruch zu unserer Bedingung an die Kardinalitäten. □

Ergänzende Übung 2.2.9. Jede irreduzible Darstellung einer abelschen Gruppe über einem algebraisch abgeschlossenen Körper, deren Dimension echt kleiner ist als die Kardinalität des Körpers, ist eindimensional.

2.3 Der Dichtesatz von Jacobson

2.3.1. Jeder Modul ist nach 1.3.11 auch ein Modul über seinem eigenen Endomorphismenring.

Satz 2.3.2 (Jacobson's Dichtesatz). *Ist R ein Ring und M ein halbeinfacher R-Modul, so ist das Bild des offensichtlichen Ringhomomorphismus*

$$R \to \operatorname{End}_{(\operatorname{End}_R M)} M$$

dicht in folgendem Sinne: Gegeben $f \in \operatorname{End}_{(\operatorname{End}_R M)} M$ und endlich viele Elemente $m_1, \ldots, m_r \in M$ existiert stets ein $x \in R$ mit $f(m_i) = xm_i \ \ \forall i$.

2.3.3. Ist unser Modul der Ring R selber, so gilt nach 1.6.5 sogar ohne weitere Voraussetzungen stets $R \xrightarrow{\sim} \operatorname{End}_{(\operatorname{End}_R R)} R$.

2.3.4. Gegeben eine Menge mit Verknüpfung E und eine Teilmenge $T \subset E$ erklärt man den **Kommutator von T in E** durch die Formel $T' = \{x \in E \mid xt = tx \quad \forall t \in T\}$. Der Kommutator des Kommutators T'' heißt dann der **Bikommutator** und umfaßt natürlich T selbst. Unser Satz sagt in dieser Terminologie, daß gegeben ein halbeinfacher Modul M über einem Ring R das Bild von $R \to \operatorname{End}_{\mathbb{Z}} M$ in der oben ausgeführten Weise "dicht" liegt in seinem Bikommutator. Im übrigen fällt der "Trikommutator" stets mit dem Kommutator zusammen, in Formeln $T''' = T'$, denn $T'' \supset T$ impliziert $T''' \subset T'$ und $T''' \supset T'$ folgt durch Anwenden der Regel $S'' \supset S$ auf $S = T'$.

Beweis. Wir beginnen mit dem Fall $r = 1$ und betrachten zu $m = m_1$ ein Komplement N des Untermoduls $Rm \subset M$, also

$$M = Rm \oplus N$$

Da die Projektion $\pi : M \twoheadrightarrow Rm \hookrightarrow M$ längs unserer Zerlegung in $\operatorname{End}_R M$ liegt, und da gilt $f \circ \pi = \pi \circ f$ nach Annahme, folgt $f(m) \in Rm$. Es gibt also in anderen Worten $x \in R$ mit $f(m) = xm$. Den allgemeinen Fall führen wir auf den Fall $r = 1$ zurück, indem wir das Element $(m_1, \ldots, m_r) \in M \oplus \ldots \oplus M$ betrachten und die Abbildung $f \times \ldots \times f$, die in der Tat kommutiert mit allen Elementen von

$$\operatorname{End}_R(M \oplus \ldots \oplus M) = \mathrm{M}(r \times r; \operatorname{End}_R M) \qquad \square$$

Korollar 2.3.5 (Satz von Wedderburn). *Ist k ein algebraisch abgeschlossener Körper und $A \subset \mathrm{M}(n \times n; k)$ ein Teilring derart, daß k^n einfach ist als A-Modul, so gilt bereits $A = \mathrm{M}(n \times n; k)$.*

Beweis. Zunächst gilt $\operatorname{End}_A k^n = k$, da sonst Eigenräume von Elementen $\varphi \in \operatorname{End}_A k^n$ nichttriviale A-Untermoduln wären. Dann folgt $A = \operatorname{End}_k k^n$ aus dem Dichtesatz 2.3.2. □

2.3.6. Man mag den Satz von Wedderburn auch koordinatenfrei formulieren: Ist k ein algebraisch abgeschlossener Körper und V ein endlichdimensionaler k-Vektorraum und $A \subset \operatorname{End}_k V$ ein Teilring derart, daß V einfach ist als A-Modul, so gilt bereits $A = \operatorname{End}_k V$. In dieser Sprache läßt sich die Notwendigkeit der Bedingungen besonders gut einsehen: Sind $k \subset L$ Körper und betrachten wir den Teilring $L \subset \operatorname{End}_k L$, so ist ja L ein einfacher L-Modul, aber im Fall $k \neq L$ gilt $L \neq \operatorname{End}_k L$.

2.3.7. Aus dem Satz von Wedderburn folgt insbesondere, daß für jede irreduzible Darstellung V einer endlichen Gruppe G über einem algebraisch abgeschlossenen Körper gilt $(\dim V)^2 \leq |G|$. Stärkere Aussagen in dieser Richtung werden wir gleich kennenlernen. Über allgemeineren Körpern gilt diese Abschätzung jedoch im allgemeinen nicht mehr, wie 1.1.25 zeigt.

2.4 Darstellungen von Produkten

2.4.1. Gegeben eine Darstellung V einer Gruppe G und eine Darstellung W einer Gruppe H über demselben Grundkörper k können wir $V \otimes_k W$ zu einer Darstellung des Produkts $G \times H$ unserer Gruppen machen, indem wir setzen $(g,h)(v \otimes w) = gv \otimes hw$. Ich schlage für diese Darstellung die Notation $V \boxtimes W$ oder ausführlicher $V \boxtimes_k W$ vor und nenne sie das **äußere Produkt** der Darstellungen V und W.

2.4.2. Gegeben eine Gruppe G und ein Körper k bezeichne

$$\operatorname{irrf}_k G$$

die Menge aller Isomorphieklassen irreduzibler endlichdimensionaler Darstellungen von G über k. Der Buchstabe f steht hier für "finite" oder "fini", die Notation irre hätte zu merkwürdig ausgesehen.

Satz 2.4.3 (Einfache Darstellungen von Produkten). *Gegeben Gruppen G, H und ein algebraisch abgeschlossener Körper k induziert das Tensorprodukt oder genauer das äußere Produkt eine Bijektion*

$$(\operatorname{irrf}_k G) \times (\operatorname{irrf}_k H) \xrightarrow{\sim} \operatorname{irrf}_k(G \times H)$$

2.4.4. Ist k nicht algebraisch abgeschlossen, so ist das im allgemeinen falsch. Zum Beipiel ist $\mathbb{C}$ eine irreduzible Darstellung über $k = \mathbb{R}$ der Gruppe $G = \mu_4$ der komplexen vierten Einheitswurzeln, aber die Darstellung $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ von $G \times G$ hat den Kern der durch die Multiplikation gegebenen Surjektion $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \twoheadrightarrow \mathbb{C}$ als Unterdarstellung.

Beweis. Gegeben $V \in G\text{-Mod}_k$, $W \in H\text{-Mod}_k$ einfache endlichdimensionale Darstellungen ist $V \otimes_k W \in (G \times H)\text{-Mod}_k$ einfach, da nach dem Satz von Wedderburn 2.3.5 die Operationen Surjektionen $kG \twoheadrightarrow \operatorname{End}_k V$ und $kH \twoheadrightarrow \operatorname{End}_k W$ liefern und damit auch eine Surjektion des Gruppenrings von $G \times H$ auf $\operatorname{End}_k(V \otimes_k W)$. Die im Satz angegebene Abbildung ist also sinnvoll definiert. Ist T eine endlichdimensionale Darstellung von $G \times H$, so besitzt T als G-Darstellung eine einfache Unterdarstellung $V \subset T$. Die offensichtliche Abbildung $V \otimes_k \operatorname{Hom}_k(V,T)^G \to T$ ist dann nach 2.4.5 ein injektiver $(G \times H)$-Homomorphismus für die offensichtliche Operation von H auf dem Hom-Raum. Ist T einfach, so muß diese Abbildung auch surjektiv sein und der Hom-Raum muß eine einfache Darstellung W von H sein. Die im Satz angegebene Abbildung ist also surjektiv. Der Nachweis ihrer Injektivität kann der Leser ohne Mühe aus dem Nachweis der Surjektivität extrahieren. □

Lemma 2.4.5. *Ist T eine Darstellung einer Gruppe G über einem Körper k und ist weiter $V \in G\text{-Mod}_k$ eine einfache Darstellung mit Endomorphismenring $\operatorname{Mod}_k^G V = k$, so induziert das Auswerten eine Inklusion*

$$V \otimes_k \operatorname{Hom}_k(V,T)^G \hookrightarrow T$$

2.4.6. Das Bild dieser Injektion ist im Übrigen genau die isotypische Komponente des kG-Moduls T vom Typ V im Sinne von 2.1.11.

Beweis. Ohne Beschränkung der Allgemeinheit dürfen wir annehmen, daß T eine Summe und dann auch eine direkte Summe ist von zu V isomorphen Unterdarstellungen. In diesem Fall ist aber das Lemma explizit klar. □

2.5 Tensorprodukt von Darstellungen

Noch zu entwickeln...

2.5.1. Gegeben Darstellungen V, W einer Gruppe G über einem Körper k können wir ihr Tensorprodukt $V \otimes W$ zu einer Darstellung von G machen durch die Vorschrift $g(v \otimes w) = (gv) \otimes (gw)$. Es ist diese Konstruktion, die die Darstellungstheorie weit über das Studium von Moduln über Ringen hinauswachsen läßt.

2.6 Reduzibilität

Satz 2.6.1 (von Maschke). *Ist G eine endliche Gruppe und k ein Körper, dessen Charakteristik nicht die Gruppenordnung teilt, so ist jede Darstellung von G über k eine direkte Summe von einfachen Unterdarstellungen.*

Beispiel 2.6.2. Im Fall der einelementigen Gruppe stimmt das schon mal: Jeder Vektorraum ist eine direkte Summe von eindimensionalen Teilräumen.

2.6.3. Eine Darstellung, die eine direkte Summe von einfachen Unterdarstellungen ist, nennt man auch **vollständig reduzibel**.

2.6.4. Unser Satz gilt mit demselben Beweis auch für einen Schiefkörper k. Beispiel 1.1.12 zeigt, daß er im allgemeinen nicht mehr gilt, wenn die Charakteristik die Gruppenordnung teilt.

Beweis für endlichdimensionale Darstellungen über $\mathbb{R}$ oder $\mathbb{C}$. In diesen Fällen benutzen wir:

Lemma 2.6.5. *Ist V eine endlichdimensionale Darstellung über $\mathbb{R}$ oder $\mathbb{C}$ der endlichen Gruppe G, so gibt es auf V ein G-invariantes Skalarprodukt.*

Beweis. Ist $b : V \times V \to \mathbb{C}$ irgendein Skalarprodukt, so definiert die Formel

$$(v, w) = \sum_{g \in G} b(gv, gw)$$

ein G-invariantes Skalarprodukt, i.e. es gilt $(gv, gw) = (v, w) \quad \forall g \in G$. □

Ist nun $W \subset V$ eine Unterdarstellung, so ist auch ihr orthogonales Komplement $W^\perp \subset V$ unter einem invarianten Skalarprodukt eine Unterdarstellung, und wir haben $V = W \oplus W^\perp$. Induktiv zeigt man so, daß V zerfällt in eine direkte Summe von einfachen Unterdarstellungen. □

Beweis für endlichdimensionale Darstellungen im allgemeinen. Wir müssen nur zeigen, daß es für jede Unterdarstellung $W \subset V$ einer endlichdimensionalen Darstellung V von G ein Komplement gibt, als da heißt eine Unterdarstellung $D \subset V$ mit $V = W \oplus D$, denn dann sind wir fertig mit vollständiger Induktion über die Dimension. Ist nun $i : W \hookrightarrow V$ eine Unterdarstellung, so finden wir sicher eine k-lineare Abbildung $\pi : V \to W$ mit $\pi \circ i = \mathrm{id}_W$. Bilden wir dann in $\mathrm{Hom}(V, W)$ die lineare Abbildung

$$\psi = \frac{1}{|G|} \sum_{g \in G} g \circ \pi \circ g^{-1}$$

so erhalten wir einen Homomorphismus von Darstellungen $\psi : V \to W$ mit $\psi \circ i = \mathrm{id}_W$. Dann ist jedoch $\ker \psi$ eine Unterdarstellung von V mit $V = W \oplus \ker \psi$. □

Beweis im allgemeinen. Nach dem bereits behandelten endlichdimensionalen Fall wissen wir, daß der Gruppenring halbeinfach ist im Sinne von 2.1.1. Mit 2.1.10 folgt daraus, daß jede Darstellung eine direkte Summe von einfachen Unterdarstellungen ist. □

Übung 2.6.6. Ist G eine endliche Gruppe und k ein Körper, dessen Charakteristik die Gruppenordnung teilt, so besitzt die Unterdarstellung der konstanten Funktionen im Gruppenring kein G-invariantes Komplement. Hinweis: Der zu solch einer Zerlegung gehörige Projektor wäre nach 1.3.3 die Rechtsmultiplikation mit einem Element a des Gruppenrings, das einerseits einer von Null verschiedenen konstanten Funktion entsprechen müßte und andererseits der Formel $a^2 = a$ zu genügen hätte. Für die konstante Funktion $a \in kG$ mit dem einzigen Funktionswert $c \in k$ gilt jedoch $a^2 = |G|ca$.

2.6.7. Ich will den vorhergehenden Beweis nocheinmal von einem anderen Standpunkt aus diskutieren und dazu neue Konzepte einführen, die uns auch an anderer Stelle noch nützlich sein werden.

Definition 2.6.8. Sind V, W zwei Darstellungen einer Gruppe G über einem Körper k, so machen wir den Raum $\mathrm{Hom}_k(V, W)$ aller k-linearen Abbildungen von V nach W selbst zu einer Darstellung vermittels der Vorschrift $(gf)(v) = g(f(g^{-1}v))$ oder, anders geschrieben,

$$gf = g \circ f \circ g^{-1}$$

Wir nennen diese Operation der Gruppe auf dem Hom-Raum die **Operation durch Konjugation**.

2.6.9. Man sieht sofort, daß die Invarianten im Raum aller linearen Abbildungen von einer Darstellung V in eine Darstellung W unter der Operation durch Konjugation genau die Homomorphismen von Darstellungen sind, in Formeln

$$\mathrm{Hom}_k(V, W)^G = \mathrm{Hom}_{kG}(V, W)$$

Im vorhergehenden Beweis haben wir schlicht über die Bahn von π im Hom-Raum gemittelt und so einen G-invarianten Homomorphismus von Vektorräumen alias einen Homomorphismus von Darstellungen erhalten.

2.6.10. Ist noch allgemeiner V eine Darstellung einer Gruppe G und W eine Darstellung einer Gruppe H, so erhalten wir eine natürliche Operation von $G \times H$ auf $\mathrm{Hom}_k(V, W)$ durch die Vorschrift

$$(g, h)f = \rho_W(h) \circ f \circ \rho_V(g^{-1}) = h \circ f \circ g^{-1}$$

Unsere Definition ergibt sich im Fall $H = G$ durch Einschränken der $(G \times G)$-Operation auf dem Hom-Raum vermittels der diagonalen Einbettung $G \hookrightarrow G \times G$, $g \mapsto (g, g)$. Wir nennen sie präziser die Operation durch Konjugation auf dem Hom-Raum, um sie zu unterscheiden von der **Operation durch Nachschalten** $g : f \mapsto \rho_W(g) \circ f$ und der **Operation durch Vorschalten** $g : f \mapsto f \circ \rho_V(g^{-1})$.

Ergänzung 2.6.11. Gegeben ein komplexer Vektorraum V operiert die symmetrische Gruppe $\mathcal{S}_n$ auf $V^{\otimes n}$ durch die Permutation von Tensoren. Die Zerlegung in isotypische Komponenten

$$V^{\otimes n} = \bigoplus_{\lambda \in \operatorname{irr} \mathcal{S}_n} (V^{\otimes n})_\lambda$$

ist dann sogar eine Zerlegung in Unterdarstellungen von $\mathrm{GL}(V)$. Ist W ein weiterer komplexer Vektorraum, so liefert das Tensorieren beider Zerlegungen eine Zerlegung

$$(V \otimes W)^{\otimes n} = \bigoplus_{\lambda,\mu \in \operatorname{irr} \mathcal{S}_n} (V^{\otimes n})_\lambda \otimes (W^{\otimes n})_\mu$$

in eine Summe von unter $\mathrm{GL}(V) \times \mathrm{GL}(W)$ stabilen Teilräumen. Betrachten wir auf beiden Seiten nur die unter $\mathcal{S}_n$ alternierenden Tensoren, so erhalten wir mit dem ersten Isomorphismus nach II.9.5.17 eine Zerlegung der äußeren Potenzen

$$\bigwedge^n (V \otimes W) \xleftarrow{\sim} (V \otimes W)^{\otimes n}_{\mathrm{sgn}} = \bigoplus_{\lambda \in \operatorname{irr} \mathcal{S}_n} (V^{\otimes n})_\lambda \otimes (W^{\otimes n})_{\lambda \otimes \mathrm{sgn}}$$

Diese Zerlegung heißt auch die **Binet-Cauchy-Identität**. Sie kann mithilfe unserer Erkenntnisse 2.9.2 über irreduzible Darstellungen von symmetrischen Gruppen auch noch konkreter ausgeschrieben werden.

2.7 Zur Struktur von Gruppenringen

Satz 2.7.1 (Fouriertransformation für endliche Gruppen). *Seien G eine endliche Gruppe, k ein algebraisch abgeschlossener Körper, und $L_1, \ldots, L_r$ die irreduziblen Darstellungen von G über k bis auf Isomorphismus. Teilt die Charakteristik von k nicht die Gruppenordnung, so liefert die Operation einen Ringisomorphismus*

$$kG \quad \xrightarrow{\sim} \quad (\operatorname{End}_k L_1) \times \ldots \times (\operatorname{End}_k L_r)$$

Teilt die Charakteristik die Gruppenordnung, so ist der durch die Operation gegebene Ringhomomorphismus zumindest noch surjektiv.

Beweis. Die Surjektivität folgt ganz allgemein mit dem Schur'schen Lemma aus dem Dichtesatz 2.3.2. Die Injektivität im Fall teilerfremder Charakteristik folgt etwa daraus, daß der Gruppenring selbst direkte Summe einfacher Unterlinksmoduln ist und deshalb kein von Null verschiedenes Element des Gruppenrings alle einfachen Darstellungen annullieren kann. □

Alternative im Fall teilerfremder Charakteristik. Im Fall teilerfremder Charakteristik folgt das auch unmittelbar aus der Halbeinfachheit des Gruppenrings nach Maschke, der Strukturtheorie halbeinfacher Ringe 2.1.20, und dem Schur'schen Lemma. Diese Argumentation hat den Vorteil, ohne den Dichtesatz auszukommen. □

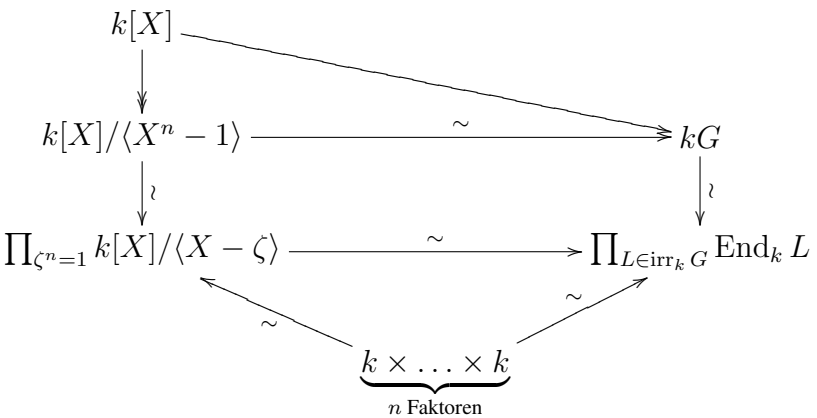
2.7.2. Der Gruppenring einer endlichen Gruppe über einem algebraisch abgeschlossenen Körper einer zur Gruppenordnung teilerfremden Charakteristik ist also in Worten isomorph vermittels der durch die Operation gegebenen Abbildung zum Produkt der Endomorphismenringe der irreduziblen Darstellungen.

Ergänzung 2.7.3. Ist G endlich und kommutativ, so ist jede irreduzible komplexe Darstellung von G eindimensional und die Isomorphieklassen komplexer irreduzibler Darstellungen von G entsprechen eineindeutig den Gruppenhomomorphismen $G \to \mathbb{C}^\times$. Unser Isomorphismus aus dem Satz entspricht dann der abstrakten Fouriertransformation

$$\mathrm{M}(G) \to \mathrm{Ens}(\hat{G}, \mathbb{C})$$

von komplexen Maßen auf G zu Funktionen auf $\hat{G}$, die wir in **??** im Fall einer Vektorgruppe eingeführt hatten und deren Verallgemeinerung auf beliebige lokal kompakte separable Hausdorff'sche topologische Gruppen in **??** diskutiert wird. Daß wir in unserem Satz einen Ringhomomorphismus definieren, entspricht Proposition **??** aus der Fouriertheorie, nach der unter der Fouriertransformation die Faltung zweier Maße in das punktweise Produkt ihrer Fouriertransformierten übergeht.

Beispiel 2.7.4. Ist $G = \mathbb{Z}/n\mathbb{Z}$ zyklisch, so finden wir unsere diskrete Fouriertransformation bereits im chinesischen Restsatz wieder, wie im folgenden Diagramm ausgeführt wird, das wir im Anschluß diskutieren, vergleiche auch 1.2.18.



Die universelle Eigenschaft des Polynomrings liefert sicher einen Homomorphismus von k-Kringen $k[X] \to kG$ mit $X \mapsto \mathrm{e}^{\bar{1}}$ in der Notation 1.2.12. Sicher liegt

$X^n - 1$ im Kern und die universelle Eigenschaft des Restklassenrings induziert so die obere Horizontale unseres Diagramms. Die Basis $X^0, X^1, \ldots, X^{n-1}$ des Restklassenrings geht dabei in die Standardbasis des Gruppenrings über, so daß unsere obere Horizontale ein Isomorphismus sein muß. Ist $k = \bar{k}$ algebraisch abgeschlossen und $\operatorname{char} k$ kein Teiler von n, so hat $X^n - 1$ nach III.3.6.6 genau n paarweise verschiedene Nullstellen $\zeta_1, \ldots \zeta_n$ in k und die Faktorisierung $X^n - 1 = (X - \zeta_1) \ldots (X - \zeta_n)$ zusammen mit dem chinesischen Restsatz III.2.2.4 liefert den Isomorphismus in der linken Vertikale. Die rechte Vertikale ist dahingegen unsere Fouriertransformation 2.7.1. Da nun nach 2.2.5 jede irreduzible Darstellung unserer abelschen Gruppe G über k eindimensional ist, entsprechen diese irreduziblen Darstellungen eineindeutig den Gruppenhomomorphismen $\mathbb{Z}/n\mathbb{Z} \to k^\times$ alias nach II.7.2.11 den n-ten Einheitswurzeln $\zeta_1, \ldots \zeta_n$. Die Kommutativität unseres Diagramms folgt aus den Definitionen. In diesem Sinne reduziert sich unser Satz 2.7.1 über die diskrete Fouriertransformation also im Fall zyklischer Gruppen auf einen Spezialfall des chinesischen Restsatzes.

2.7.5. Der obige Satz gilt analog für jeden halbeinfachen Ring R, der einen algebraisch abgeschlossenen Körper k enthält derart, daß gilt $ar = ra \; \forall a \in k, r \in R$ und daß R endlichdimensional ist über k. Die Fouriertransformation im Fall endlicher zyklischer Gruppen läuft meist unter der Bezeichnung **diskrete Fouriertransformation**.

Beweis. Die Surjektivität folgt mithilfe von 1.3.12 aus dem Dichtesatz 2.3.2, angewandt auf den kG-Modul $L_1 \oplus \ldots \oplus L_r$ mit seinem Endomorphismenring $k \times \ldots \times k$. Um die Injektivität zu zeigen bemerken wir, daß ja kG nach Maschke selbst eine Summe von einfachen Unterdarstellungen ist. Liegt also $a \in kG$ im Kern unserer Abbildung, so ist die Linksmultiplikation mit a die Nullabbildung auf kG und es folgt $a = 0$. □

Korollar 2.7.6. *Sei G eine endliche Gruppe und k ein algebraisch abgeschlossener Körper, dessen Charakteristik nicht die Gruppenordnung teilt. Seien $L_1, \ldots, L_r$ die irreduziblen Darstellungen von G über k, bis auf Isomorphismus. So gilt*

$$|G| = (\dim L_1)^2 + \ldots + (\dim L_r)^2$$

Beweis. Klar mit 2.7.1. □

Korollar 2.7.7. *Gegeben eine endliche Gruppe und ein algebraisch abgeschlossener Körper, dessen Charakteristik die Gruppenordnung nicht teilt, gibt es bis auf Isomorphismus genausoviele einfache Darstellungen unserer Gruppe über besagtem Körper wie Konjugationsklassen in unserer Gruppe.*

Beweis. Das Zentrum eines Gruppenrings kG besteht nun offensichtlich genau aus den Funktionen $G \to k$, die mit allen Gruppenelementen kommutieren, und

damit aus den Funktionen, die konstant sind auf Konjugationsklassen. Man nennt sie **Klassenfunktionen**. Das Zentrum der anderen Seite in Satz 2.7.1 ist aber nach den beiden anschließenden Übungen 2.7.8 und 2.7.9 offensichtlich isomorph als k-Vektorraum zu einem Produkt von r Kopien des Grundkörpers $k \times \ldots \times k$. □

Übung 2.7.8. Das Zentrum des Endomorphismenrings eines Vektorraums besteht genau aus allen Multiplikationen mit Skalaren aus dem Körper.

Übung 2.7.9. Das Zentrum eines Produkts von Ringen ist das Produkt ihrer Zentren.

Ergänzende Übung 2.7.10. Gegeben eine endliche Gruppe und ein algebraisch abgeschlossener Körper, dessen Charakteristik die Gruppenordnung nicht teilt, zeige man: Genau dann ist die Gruppe kommutativ, wenn alle ihre irreduziblen Darstellungen über besagtem Körper eindimensional sind.

Definition 2.7.11. Ist V eine Darstellung einer Gruppe G über einem Körper k, so definiert man ganz allgemein für $v \in V$, $\varphi \in V^*$ den **Matrixkoeffizienten** $c_{\varphi,v} : G \to k$ durch die Vorschrift $c_{\varphi,v}(g) = \varphi(gv)$.

2.7.12. Im Fall $V = k^n$ und $v = \mathrm{e}_i$ und $\varphi = \mathrm{e}_j^*$ ist $c_{\varphi,v}(g)$ in der Tat ein Koeffizient der Matrix $\rho(g) \in \mathrm{M}(n \times n; k)$. Die Matrixkoeffizienten definieren eine Abbildung, die **Matrixkoeffizientenabbildung**

$$\begin{array}{ccc} V^* \otimes_k V & \to & \mathrm{Ens}(G,k) \\ \varphi \otimes v & \mapsto & c_{\varphi,v} \end{array}$$

Satz 2.7.13 (Inverse Fouriertransformation). *Sei G eine endliche Gruppe und k ein algebraisch abgeschlossener Körper, dessen Charakteristik nicht die Gruppenordnung teilt. Sind L, M irreduzible Darstellungen von G über k, so ist $\dim L$ nicht Null in k und die Verknüpfung*

$$L^* \otimes_k L \to kG \to \mathrm{End}_k M$$

der Matrixkoeffizientenabbildung mit der Operation ist die Nullabbildung im Fall $M \ncong L^*$. Gibt es dahingegen einen Isomorphismus von Darstellungen $i : M \xrightarrow{\sim} L^*$, so fällt unsere Verknüpfung zusammen mit dem $|G|/(\dim L)$-fachen der Verknüpfung

$$L^* \otimes_k L \xrightarrow{\sim} \mathrm{End}_k L^* \xrightarrow{\sim} \mathrm{End}_k M$$

des kanonischen Isomorphismus mit der Abbildung $f \mapsto i \circ f \circ i^{-1}$.

2.7.14. Nach dem Lemma von Schur unterscheiden sich zwei Isomorphismen zwischen irreduziblen Darstellungen $i, j : M \xrightarrow{\sim} L^*$ unter den gegebenen Voraussetzungen höchstens um einen Skalar, $i = \lambda j$ mit $\lambda \in k$. Die zwischen ihren Endomorphismenringen induzierten Isomorphismen $f \mapsto i \circ f \circ i^{-1}$ und $f \mapsto j \circ f \circ j^{-1}$ sind also dieselben.

2.7.15. Wieder im Fall einer endlichen kommutativen Gruppe G haben wir kanonische Identifikationen $k \xrightarrow{\sim} \operatorname{End} L \xrightarrow{\sim} L^* \otimes_k L$ und die Matrixkoeffizientenabbildungen aller irreduziblen komplexen Darstellungen definieren eine Abbildung, die man als Spezialfall der Fouriertransformation

$$\mathrm{M}(\hat{G}) \to \mathrm{Ens}(G, \mathbb{C})$$

auffassen kann. Unser Satz besagt dann im Lichte von **??** und **??**, daß das Plancherelmaß zum auf Gesamtmasse Eins normalisierten Haarmaß auf G das Zählmaß auf $\hat{G}$ ist, wie das ja sogar ganz allgemein für kompakte Gruppen gilt. Der zugehörige Isomorphismus von Räumen quadratintegrierbarer Funktionen ist bereits ein Spezialfall von **??** und wird im folgenden insbesondere auch durch 2.7.17 verallgemeinert.

Beweis. Unsere Matrixkoeffizientenabbildung $V^* \otimes_k V \to kG$ ist ein Homomorphismus von Darstellungen für geeignete Operationen von $G \times G$ auf beiden Seiten, genauer gilt offensichtlich $c_{g\varphi,v} = g * c_{\varphi,v}$ und $c_{\varphi,gv} = c_{\varphi,v} * g^{-1}$ für alle $g \in G$. Die Abbildungen aus unserem Satz sind demnach Morphismen zwischen Darstellungen von $(G \times G)$. Nach 2.4.3 sind diese Darstellungen sogar irreduzibel, so daß als einzige offene Frage bleibt, das Wievielfache des üblichen Isomorphismus im Fall $M \cong L^*$ genommen werden muß. Es scheint mir besonders übersichtlich, das in physikalischer Notation ausrechnen. Gegeben ein Vektorraum L und ein Vektor $v \in L$ notieren wir $|v\rangle$ die lineare Abbildung $k \to L$, $\lambda \mapsto \lambda v$ und notieren Elemente $\varphi \in L^*$ des Dualraums als $\langle\varphi|$. Für $\varphi, \psi \in L^*$ und $v, w \in L$ ergibt sich damit, wenn wir die k-linearen Abbildungen von k in sich selber stillschweigend mit k identifizieren, für die Operation eines Matrixkoeffizienten auf $\psi \in L^*$ die Formel

$$(c_{\varphi,v} * \psi)(w) = \textstyle\sum_{g\in G} \langle\varphi|g|v\rangle\langle\psi|g^{-1}|w\rangle = \langle\varphi| \left(\sum_{g\in G} g|v\rangle\langle\psi|g^{-1}\right) |w\rangle$$

Nun ist die große Summe (Σ) in der Mitte der letzten Formel offensichtlich ein G-Endomorphismus von L, d.h. für alle $h \in G$ gilt $h \circ (\Sigma) \circ h^{-1} = (\Sigma)$. Da L irreduzibel ist, muß diese Summe folglich ein Vielfaches der Identität sein, es gilt also $(\Sigma) = d\,\mathrm{id}_L$ für ein $d \in k$. Berechnen wir auf beiden Seiten dieser Gleichung die Spur, so ergibt sich in k die Gleichung

$$d \cdot \dim L = |G| \operatorname{tr}(|v\rangle\langle\psi|) = |G|\langle\psi|v\rangle$$

Wegen $|G| \neq 0$ in k und da man stets ψ und v finden kann mit $\langle\psi|v\rangle = 1$ folgt $\dim L \neq 0$ in k. Durch Einsetzen von $(\Sigma) = d\,\mathrm{id}_L$ rechts in der vorigen Formelzeile erhalten wir schließlich die Behauptung in Gestalt der Formel

$$(c_{\varphi,v} * \psi)(w) = \frac{|G|}{\dim L}\langle\psi|v\rangle\langle\varphi|w\rangle \qquad \square$$

Korollar 2.7.16. *Ist G eine endliche Gruppe und k ein algebraisch abgeschlossener Körper, dessen Charakteristik nicht die Gruppenordnung teilt, so haben Matrixkoeffizienten zu nichtisomorphen irreduziblen Darstellungen im Gruppenring das Produkt Null.*

Beweis. Dem Leser überlassen. □

Korollar 2.7.17 (Orthogonalität von Matrixkoeffizienten). *Bilden gewisse $\rho_L : G \to \mathrm{U}(d_L)$ ein Repräsentantensystem für die einfachen unitären Darstellungen einer endlichen Gruppe G, so bilden die renormalisierten Matrixkoeffizienten $\sqrt{d_L}\,(\rho_L)_{ij}$ eine Orthonormalbasis des Gruppenrings $\mathbb{C}G$ für das Skalarprodukt $\langle f, h\rangle = |G|^{-1}\sum_{g\in G}\overline{f(g)}h(g)$.*

2.7.18. Im Fall einer endlichen kommutativen Gruppe ist das ein Spezialfall der Theorie der abstrakten Fourierreihen **??**, nach der die unitären Charaktere einer kompakten kommutativen Hausdorff'schen topologischen Gruppe eine Hilbertbasis des Raums der quadratintegrierbaren Funktionen auf meiner Gruppe bilden, in Bezug auf das auf Gesamtmasse Eins normalisierte Haarmaß.

Beweis. Haben wir auf einer endlichdimensionalen Darstellung V ein G-invariantes Skalarprodukt $\langle\ ,\ \rangle$ gewählt, das schieflinear ist in der ersten Variablen und linear in der zweiten, so erhalten wir einen Isomorphismus von Darstellungen $\overline{V} \xrightarrow{\sim} V^*$, $v \mapsto \langle v,\ \rangle$. Für beliebige $v, w \in V$ und $g \in G$ gilt dann natürlich $\langle v, g^{-1}w\rangle = \langle gv, w\rangle = \overline{\langle w, gv\rangle}$. Mit dieser Erkenntnis können wir die Formel vom Ende des Beweises von 2.7.13 umdeuten zu

$$\frac{1}{|G|}\sum_{g\in G}\langle\varphi, gv\rangle\overline{\langle w, g\psi\rangle} = \frac{\langle\psi, v\rangle\langle\varphi, w\rangle}{\dim L}$$

für alle $v, w, \varphi, \psi \in L$. Mit demselben Argument ergibt sich, daß für nicht isomorphe einfache unitäre Darstellungen L, M und $\varphi, v \in L$ und $w, \psi \in M$ gilt $\sum_{g\in G}\langle\varphi, gv\rangle\langle w, g\psi\rangle = 0$. □

2.8 Charaktere

2.8.1. Sei G eine endliche Gruppe und k ein algebraisch abgeschlossener Körper, dessen Charateristik nicht die Gruppenordnung teilt. Sei L eine einfache Darstellung von G. Nach unserer Fouriertransformation 2.7.1 gibt es genau ein Element $e_L \in kG$ derart, daß e_L durch die Identität auf L operiert und durch Null auf jeder einfachen Darstellung M von G, die nicht isomorph ist zu L, in Formeln

$$(e_L\cdot : M \to M) = \begin{cases} \mathrm{id} : M \to M & \text{falls } M \cong L; \\ 0 : M \to M & \text{falls } M \text{ einfach, } M \ncong L. \end{cases}$$

Dies Element e_L nennen wir den **Projektor** zu L. Die Summe aller dieser Projektoren ist natürlich die Eins des Gruppenrings.

Beispiel 2.8.2. Die Gruppe $\mathbb{Z}/2\mathbb{Z}$ hat über jedem Körper k der Charakteristik ungleich Zwei die beiden einfachen Darstellungen k_+ und k_-. Die zugehörigen Projektoren sind $e_{k_+} = (\mathrm{e}^{\bar{0}} + \mathrm{e}^{\bar{1}})/2$ und $e_{k_-} = (\mathrm{e}^{\bar{0}} - \mathrm{e}^{\bar{1}})/2$.

Beispiel 2.8.3. Der Projektor zur trivialen Darstellung k hat stets die Gestalt $e_k = |G|^{-1} \sum_{g\in G} g$. In der Tat operiert dieses Element des Gruppenrings auf der trivialen Darstellung als die Identität und auf allen anderen einfachen Darstellungen als Null, da diese ja außer der Null keinen unter G invarianten Vektor besitzen.

2.8.4. Um den Projektor im allgemeinen explizit anzugeben, erinnern wir uns an unsere inverse Fouriertransformation 2.7.13. Ist $v_1, \ldots, v_n$ eine Basis von L und $\varphi_1, \ldots, \varphi_n$ die duale Basis von L^*, so haben wir offensichtlich $\varphi_1 \otimes v_1 + \ldots + \varphi_n \otimes v_n \mapsto \mathrm{id}$ unter der kanonischen Identifikation $L^* \otimes_k L \xrightarrow{\sim} \mathrm{End}_k L^*$. Unter der Matrixkoeffizientenabbildung geht dieser Tensor auf die Funktion $\chi = \chi_L = c_{\varphi_1,v_1} + \ldots + c_{\varphi_n,v_n}$, die offensichtlich auch einfacher beschrieben werden kann durch die Formel $\chi_L(g) = \mathrm{tr}(g|L)$. Gegeben eine endlichdimensionale Darstellung V einer Gruppe G über einem Körper k definiert man ganz allgemein ihren **Charakter** $\chi_V : G \to k$ durch die Vorschrift

$$\chi_V(g) = \mathrm{tr}(g|V)$$

Da nach II.1.10.15 konjugierte Matrizen dieselbe Spur haben, sind Charaktere stets Klassenfunktionen. Die vorhergehenden Argumente zeigen für jede endliche Gruppe G und jeden algebraisch abgeschlossenen Körper k, dessen Charateristik nicht die Gruppenordnung teilt, die **Charakter-Projektor-Formel**

$$e_{L^*} = \frac{\dim L}{|G|}\chi_L$$

Die Dimension einer Darstellung ist offensichtlich gerade der Wert ihres Charakters beim neutralen Element, und wir erkennen so, daß die wesentlichen Informationen über die Struktur eines Gruppenrings bereits aus der Kenntnis der Charaktere der einfachen Darstellungen, d.h. der **einfachen Charaktere** hervorgehen. Im Fall komplexer Darstellungen einer abelschen Gruppe sind das natürlich genau die Gruppenhomomorphismen $G \to \mathbb{C}^\times$, weshalb unsere Terminologie hier mit der in **??** eingeführten Terminologie verträglich ist.

Übung 2.8.5. Gegeben eine Darstellung V einer Gruppe nennen wir $V^* = \mathrm{Hom}(V, k)$ auch die **kontragradiente Darstellung**. Man zeige, daß der Charakter der kontragradienten Darstellung gegeben wird durch die Formel $\chi_{V^*}(g) = \chi_V(g^{-1})$. Weiter zeige man $\chi_{V\oplus W} = \chi_V + \chi_W$.

Ergänzende Übung 2.8.6. Gegeben eine endlichdimensionale irreduzible Darstellung V einer Gruppe über einem Körper der Charakeristik Null oder einem algebraisch abgeschlossenen Körper ist ihr Charakter nicht die Nullfunktion. Hinweis: Satz von Wedderburn 2.3.5.

Ergänzung 2.8.7. Gegeben eine endliche inseparable Körpererweiterung L/K ist L eine irreduzible Darstellung über K der multiplikativen Gruppe $L^\times$, deren Charakter nach **??** die Nullfunktion ist.

Satz 2.8.8 (Dimensionen einfacher Darstellungen). *Gegeben ein algebraisch abgeschlossener Körper der Charakteristik Null und eine endliche Gruppe ist die Dimension jeder einfachen Darstellung unserer Gruppe über dem gegebenen Körper ein Teiler der Gruppenordnung.*

Beweis. Sei G unsere endliche Gruppe, L unsere einfache Darstellung und $M = L^*$ ihre kontragrediente Darstellung. Wir gehen aus von der Gleichung $e_M * e_M = e_M$. Mit der Charakter-Projektor-Formel 2.8.4 folgt

$$\chi_L * \chi_L = \frac{|G|}{\dim L}\chi_L$$

Per definitionem ist $\chi_L(g)$ die Summe der Eigenwerte von $g : L \to L$, und da gilt $g^n = 1$ für $n = |G|$ sind diese Eigenwerte n-te Einheitswurzeln. Ist also $\zeta \in k$ eine primitive n-te Einheitswurzel, so nehmen alle Charaktere Werte in $\mathbb{Z}[\zeta]$ an. Bezeichnet $I \subset \mathbb{Z}[\zeta]$ das von den Werten des Charakters χ_L erzeugte Ideal, so folgern wir im Körper k die Inklusionsrelation

$$I \supset \frac{|G|}{\dim L} I$$

Da die Potenzen $1, \zeta, \zeta^2, \ldots \zeta^{n-1}$ bereits $\mathbb{Z}[\zeta]$ als abelsche Gruppe erzeugen, ist mit II.7.3.12 auch I eine endlich erzeugte torsionsfreie abelsche Gruppe und mit II.7.4.9 ist dann I frei über $\mathbb{Z}$, in Formeln $I \cong \mathbb{Z}^r$ für geeignetes $r \in \mathbb{N}$. Zusammen mit der Erkenntnis $I \neq 0$ impliziert unsere Inklusion oben nun $(|G|/\dim L) \in \mathbb{Z}$ wie gewünscht. □

2.8.9. Wir definieren nun für jede endliche Gruppe G und jeden Körper k, dessen Charakteristik teilerfremd ist zur Gruppenordnung, auf dem Gruppenring kG eine symmetrische Bilinearform $(\ ,\ )$ durch die Vorschrift

$$(\varphi, \psi) = \frac{1}{|G|}\sum_{g\in G} \varphi(g)\psi(g^{-1})$$

Satz 2.8.10. *Seinen gegeben eine endliche Gruppe und ein Körper, dessen Charakteristik teilerfremd ist zur Gruppenordnung. So bilden die einfachen Charaktere für die vorstehende Bilinearform eine Orthonormalbasis des Raums der Klassenfunktionen.*

Beweis. Wir beachten $(\varphi, \psi) = |G|^{-1}(\varphi * \psi)(e)$. Jetzt schreiben wir die Gleichung $e_M * e_L = 0$ für die Projektoren zu nichtisomorphen einfachen Darstellungen um auf einfache Charaktere und erhalten schon mal $(\chi, \psi) = 0$ für verschiedene einfache Charaktere. Sonst kommen wir wieder zurück auf unsere Gleichung

$$\chi * \chi = \frac{|G|}{\dim L}\chi$$

für $\chi = \chi_L$, und werten wir diese Gleichung aus am neutralen Element und beachten $\chi(e) = \operatorname{tr}(e|L) = \dim L$, so ergibt sich auch $(\chi, \chi) = 1$ wie gewünscht. Die Charaktere bilden also ein Orthonormalsystem, und nach 2.7.7 bilden sie dann sogar eine Basis. □

Korollar 2.8.11. *Zwei endlichdimensionale Darstellungen einer endlichen Gruppe über einem Körper der Charakteristik Null sind isomorph genau dann, wenn sie denselben Charakter haben.*

Ergänzung 2.8.12. Eine Variante dieser Aussage findet man in **??**.

Beweis. Wir können sogar die Vielfachheit, mit der eine vorgegebene irreduzible Darstellung L in einer Zerlegung unserer Darstellung V als direkte Summe irreduzibler Darstellungen auftritt, berechnen als den Wert $\langle \chi_L, \chi_V \rangle$ unserer Bilinearform auf den Charakteren. □

Korollar 2.8.13 (Orthogonalitätsrelationen für Charaktere). *Sei G eine endliche Gruppe. Wir betrachten auf dem komplexen Gruppenring $\mathbb{C}G$ das Skalarprodukt $\langle\ ,\ \rangle$ gegeben durch*

$$\langle \varphi, \psi \rangle = \frac{1}{|G|} \sum \varphi(g)\overline{\psi(g)}$$

Für dieses Skalarprodukt bilden die einfachen Charaktere eine Orthonormalbasis des Raums der Klassenfunktionen.

Beweis. Mit 2.8.10 reicht es, für jeden Charakter $\chi = \chi_V$ über $\mathbb{C}$ die Formel $\chi(g^{-1}) = \overline{\chi(g)}$ zu zeigen. Nun sind aber alle Eigenwerte von $(g\cdot) : V \to V$ Einheitswurzeln und die Eigenwerte von $(g^{-1}\cdot) : V \to V$ sind ihre Inversen alias ihre komplex Konjugierten. Alternativ folgt die Aussage auch sofort aus den Orthonormalitätsrelationen für Matrixkoeffizienten 2.7.17. □

2.8.14. Die wesentlichen Informationen über die komplexen Darstellungen einer endlichen Gruppe wird meist in Form einer **Charaktertafel** dargeboten: Die Spalten solch einer Tafel sind indiziert durch Repräsentanten der Konjugationsklassen, die Zeilen durch irreduzible Darstellungen, und in der Tafel stehen die Werte des Charakters der entsprechenden irreduziblen Darstellung auf Elementen der entsprechenden Konjugationsklasse. Über den Konjugationsklassen wird meist in einer eigenen Zeile ihre Kardinalität angegeben, damit auch das Skalarprodukt auf dem Raum Klassenfunktionen aus der Tafel hervorgeht.

Beispiel 2.8.15. Die irreduziblen Darstellungen der symmetrischen Gruppe $\mathcal{S}_3$ sind die triviale Darstellung triv, die Signumsdarstellung sgn und die Darstellung spieg als zweidimensionale Spiegelungsgruppe, bei der die drei ungeraden Permutationen operieren als Spiegelungen an drei Geraden durch den Ursprung, die paarweise den Winkel $60°$ einschließen. Zeichenen wir zwei ungerade Permutationen $s, t \in \mathcal{S}_3$ aus, so können wir die Elemente von $\mathcal{S}_3$ aufzählen als $\mathcal{S}_3 = \{e, s, t, sts, ts, st\}$ und die Charaktertafel hat die Gestalt

	e	s,t,sts	ts,st
triv	1	1	1
sgn	1	-1	1
spieg	2	0	-1

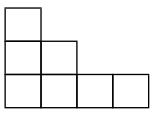
Um die unterste Zeile zu prüfen bemerkt man, daß jede ebene lineare Spiegelung Spur Null hat, jede ebene Drehung um $120°$ jedoch Spur $\zeta + \bar{\zeta} = -1$ für ζ eine primitive dritte Einheitswurzel.

2.9 Darstellungen der symmetrischen Gruppen

2.9.1. Wir stellen zunächst die beiden Hauptsätze vor, die wir beweisen wollen. Unter einem **Youngdiagramm** verstehen wir wie in III.1.3.3 eine endliche Teilmenge $T \subset \mathbb{N} \times \mathbb{N}$ mit der Eigenschaft

$$((i,j) \in T \text{ und } i' \leq i \text{ und } j' \leq j) \quad \Rightarrow \quad (i',j') \in T$$

Die Elemente von T nennen wir die "Kästchen" unseres Youngdiagramms und stellen uns ein Element (i,j) vor als das Kästchen auf einem Rechenpapier, bei dem die Koordinaten der linken unteren Ecke gerade (i,j) sind. Zum Beispiel stellt das Bild



die Menge $\{(0,0),(0,1),(0,2),(1,0),(1,1),(2,0),(3,0)\}$ dar. In der Praxis denke ich bei Youngdiagrammen stets an Bilder dieser Art.

Satz 2.9.2 (Einfache Darstellungen der symmetrischen Gruppen).

1. *Gegeben ein Youngdiagramm T besitzt die Gruppe $\mathcal{S}_T = \mathrm{Ens}^\times T$ aller Permutationen von T bis auf Isomorphismus genau eine einfache komplexe Darstellung $L(T)$ mit der Eigenschaft, daß darin sowohl die triviale Darstellung des Spaltenstabilisators von T als auch die Signumsdarstellung des Zeilenstabilisators von T vorkommen.*

2. *Gegeben $n \geq 0$ erhalten wir eine Bijektion*

$$\begin{array}{ccc} \mathcal{Y}_n & \xrightarrow{\sim} & \operatorname{irr} \mathbb{C}\mathcal{S}_n \\ T & \mapsto & L(T) \end{array}$$

zwischen der Menge $\mathcal{Y}_n$ aller Youngdiagramme mit n Kästchen und der Menge aller Isomorphieklassen von einfachen komplexen Darstellungen der symmetrischen Gruppe $\mathcal{S}_n$, indem wir für jedes Youngdiagramm T mit n Kästchen eine Bijektion $T \xrightarrow{\sim} \{1,\ldots,n\}$ wählen, dadurch $\mathcal{S}_T$ mit $\mathcal{S}_n$ identifizieren, und unsere einfache Darstellung $L(T)$ aus Teil 1 mit dieser Identifikation als Darstellung von $\mathcal{S}_n$ auffassen.

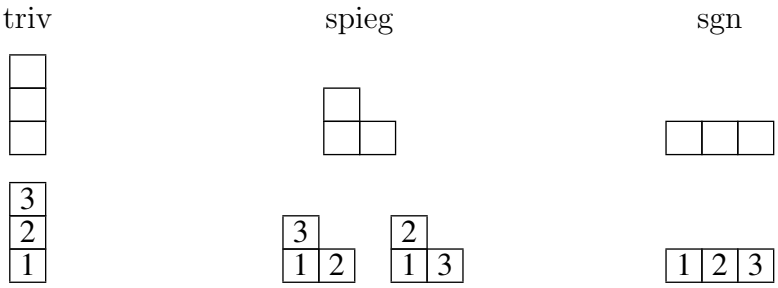
2.9.3. Nach 1.1.20 hängt die so erhaltene Darstellung $L(T)$ der Gruppe $\mathcal{S}_n$ bis auf Isomorphismus nicht von der Wahl der Bijektion $T \xrightarrow{\sim} \{1,\ldots,n\}$ ab.

Definition 2.9.4. Gegeben ein Youngdiagramm T mit n Kästchen ist ein **Tableau der Gestalt** T eine Bijektion $\varphi : T \xrightarrow{\sim} \{1,\ldots,n\}$. Wir veranschaulichen so ein Tableau, indem wir in jedes Kästchen unseres Youngdiagramms den Wert schreiben, den φ dort annimmt. Ein **Standardtableau** ist ein Tableau, dessen Einträge in allen Zeilen und Spalten monoton wachsen.

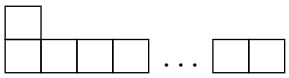
Satz 2.9.5 (Dimensionen der einfachen Darstellungen). *Für ein Youngdiagramm T stimmt die Dimension der zugehörigen einfachen komplexen Darstellung $L(T)$ von $\mathcal{S}_n$ überein mit der Zahl von Standardtableaus der Gestalt T.*

Beispiel 2.9.6. Im Fall der symmetrischen Gruppe $\mathcal{S}_3$ haben wir drei Young-Diagramme mit drei Kästchen. Sie entsprechen den drei irreduziblen Darstellungen nach 2.8.15. Die Spiegelungsdarstellung ist zweidimensional, was der Tatsache entspricht, daß es für das fragliche Youngdiagramm zwei Standardtableaus

gibt.



Beispiel 2.9.7. Die Permutationsdarstellung von $\mathcal{S}_n$ auf $\mathbb{C}^n$ zerfällt für $n \geq 2$ in zwei irreduzible Darstellungen, nämlich die Gerade $\langle(1,1,\ldots,1)\rangle$ und ihr orthogonales Komplement unter dem Standard-Skalarprodukt. Daß dieses Komplement irreduzibel ist, erkennt man zum Beispiel, indem man nachrechnet, daß der Endomorphismenring unserer Permutationsdarstellung zweidimensional ist: Genauer besteht er aus allen Matrizen, bei denen alle Einträge auf der Diagonalen übereinstimmen und alle Einträge außerhalb der Diagonale ebenfalls übereinstimmen. Das Youngtableau für den nichttrivialen Summanden hat die Gestalt



In der Tat kommt in unserem orthogonalen Komplement die triviale Darstellung von $\mathcal{S}_{n-1} \subset \mathcal{S}_n$ vor als die Gerade $\langle(1,1,\ldots,1-n)\rangle$ und die Signumsdarstellung von $\mathcal{S}_2 \subset \mathcal{S}_n$ als die Gerade $\langle(1,-1,0,\ldots 0)\rangle$.

2.9.8. Ist R ein Ring und $e \in R$ ein idempotentes Element und M ein R-Modul, so induziert das Auswerten bei e nach 1.3.4 eine Bijektion $\mathrm{Hom}_R(Re, M) \xrightarrow{\sim} eM$.

Beweis von 2.9.2. Wir betrachten im Gruppenring $\mathbb{C}\mathcal{S}_T$ die beiden Idempotenten

$$E_T = |S|^{-1} \sum_{g \in S} g \quad \text{und} \quad A_T = |Z|^{-1} \sum_{h \in Z} \mathrm{sgn}(h)\, h$$

Diese Idempotenten sind genau die Projektoren zur trivialen Darstellung von S und zur Signumsdarstellung von Z und die beiden von diesen Idempotenten erzeugten Linksideale $M(T) = (\mathbb{C}\mathcal{S}_T)E_T$ und $N(T) = (\mathbb{C}\mathcal{S}_T)A_T$ des Gruppenrings $\mathbb{C}\mathcal{S}_T$ wird der mit Induktion von Darstellungen **??** vertraute Leser im übrigen leicht identifizieren können mit den induzierten Darstellungen zur trivialen Darstellung des Spaltenstabilisators bzw. der Signumsdarstellung des Zeilenstabilisators. In einer Darstellung L von $\mathcal{S}_T$ kommt nach 2.9.8 die triviale Darstellung des Spaltenstabilisators vor genau dann, wenn gilt $E_T L \neq 0$ alias

$\mathrm{Hom}_{\mathbb{C}}^{\mathcal{S}_T}(M(T), L) \neq 0$, und ebenso kommt die Signumsdarstellung des Zeilenstabilisators vor genau dann, wenn gilt $A_T L \neq 0$ alias $\mathrm{Hom}_{\mathbb{C}}^{\mathcal{S}_T}(N(T), L) \neq 0$. Jede einfache Darstellung L von $\mathcal{S}_T$ mit beiden Eigenschaften ist also das Bild eines Homomorphismus von Darstellungen $M(T) \to N(T)$, und Teil 1 folgt leicht, wenn wir zeigen können, daß gilt

$$\dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}}^{\mathcal{S}_T}(M(T), N(T)) = 1 \qquad (*)$$

In der Tat ist dann unser L notwendig das Bild eines und jedes von Null verschiedenen derartigen Homomorphismus. Nehmen wir speziell den durch Rechtsmultiplikation mit A_T gegebenen Homomorphismus und beachten die im folgenden gezeigte Formel $E_T A_T \neq 0$, so ergibt sich für diese durch T bestimmte einfache Darstellung $L \cong L(T)$ sogar die explizite Formel

$$L(T) \cong (\mathbb{C}\mathcal{S}_T) E_T A_T$$

In anderen Worten kann $L(T)$ also beschrieben werden als das vom sogenannten **Young-Symmetrisator** $E_T A_T$ im Gruppenring erzeugte Linksideal. Um nun unsere Identität $(*)$ zu zeigen, schreiben wir sie zunächst mithilfe unserer Vorbemerkung 2.9.8 und den Definitionen um zur Behauptung

$$\dim_{\mathbb{C}} E_T(\mathbb{C}\mathcal{S}_T) A_T = 1$$

Nun gilt ja offensichtlich $S \cap Z = 1$, also $E_T A_T \neq 0$, und für alle $x \in SZ$ gilt $E_T x A_T = \pm E_T A_T$. Es reicht also, wenn wir zusätzlich für alle $x \notin SZ$ zeigen $E_T x A_T = 0$ oder gleichbedeutend $x^{-1} E_T x A_T = 0$. Nun haben wir natürlich

$$|S| x^{-1} E_T x = \sum_{g \in x^{-1} S x} g$$

und bezeichnet $T = T_1 \cup T_2 \cup \ldots$ die Partition von T in die Spalten des Youngdiagramms, so ist $x^{-1} S x$ gerade die Gruppe aller derjenigen Permutationen von T, die jedes Stück der Partition

$$T = x^{-1} T_1 \cup x^{-1} T_2 \cup \ldots$$

von T stabilisieren. Trifft nun jede transformierte Spalte $x^{-1} T_i$ jede Zeile unseres Youngdiagramms in höchstens einem Element, so scheint es mir offensichtlich, daß es ein y im Zeilenstabilisator Z geben muß mit $y x^{-1} T_i = T_i$ für alle i, woraus sofort folgt $x \in SZ$. Im Fall $x \notin SZ$ gibt es folglich eine transformierte Spalte $x^{-1} T_i$, die mit einer Zeile von T mindestens zwei Elemente gemeinsam hat. Die Vertauschung dieser beiden Elemente ist dann eine Transposition $t \in x^{-1} S x \cap Z$, und deren Existenz zeigt $E_T x A_T = 0$, da dann ja gilt

$$(x^{-1} E_T x) A_T = (x^{-1} E_T x t) A_T = (x^{-1} E_T x) t A_T = -(x^{-1} E_T x) A_T$$

Eine Permutation der Kästchen eines Youngdiagramms, bei der das Bild jeder Spalte höchstens ein Kästchen in jeder Zeile hat, kann durch Nachschalten eines Elements des Zeilenstabilisators in den Spaltenstabilisator geschoben werden. Das Bild deutet solch eine Permutation an, die Wirkung der Permutation auf die Kästchen der zweiten Spalte habe ich durch Pfeile angedeutet, bei den anderen Kästchen rechts ist nur an der Textur zu sehen, aus welcher Spalte sie kommen.

Damit wissen wir, daß die Darstellungen $L(T)$ einfach sind. Da es offensichtlich ebensoviele Young-Diagramme mit n Kästchen gibt wie Partitionen der Zahl n wie nach III.1.3.7 Konjugationsklassen in der symmetrischen Gruppe $\mathcal{S}_n$, ist der erste Satz bewiesen, sobald wir zeigen, daß die Darstellungen $L(T)$ paarweise nicht isomorph sind. Um das zu zeigen, führen wir auf der Menge $\mathcal{Y}_n$ aller Youngdiagramme mit n Kästchen eine partielle Ordnung ein.

Definition 2.9.9. Ein Youngdiagramm heißt kleinergleich einem anderen in der **Dominanz-Ordnung** genau dann, wenn es für jedes $s \in \mathbb{N}$ in den ersten s Spalten insgesamt höchstens ebensoviele Kästchen besitzt wie das andere. Wir notieren diese partielle Ordnung $T \leq T'$.

Fortführung des Beweises. Wählen wir irgendeine Bijektion $T \xrightarrow{\sim} \{1, \ldots, n\}$, identifizieren mit ihrer Hilfe $\mathcal{S}_T$ mit $\mathcal{S}_n$ und fassen mithilfe dieser Identifikation die Darstellungen $M(T)$ und $N(T)$ von $\mathcal{S}_T$ als Darstellungen von $\mathcal{S}_n$ auf, so erhalten wir nach 1.1.20 bis auf Isomorphismus wohldefinierte Darstellungen von $\mathcal{S}_n$. Für je zwei Diagramme $T, T' \in \mathcal{Y}_n$ behaupten wir nun

$$\mathrm{Hom}_{\mathbb{C}}^{\mathcal{S}_n}(M(T), N(T')) \neq 0 \quad \Rightarrow \quad T \leq T'$$

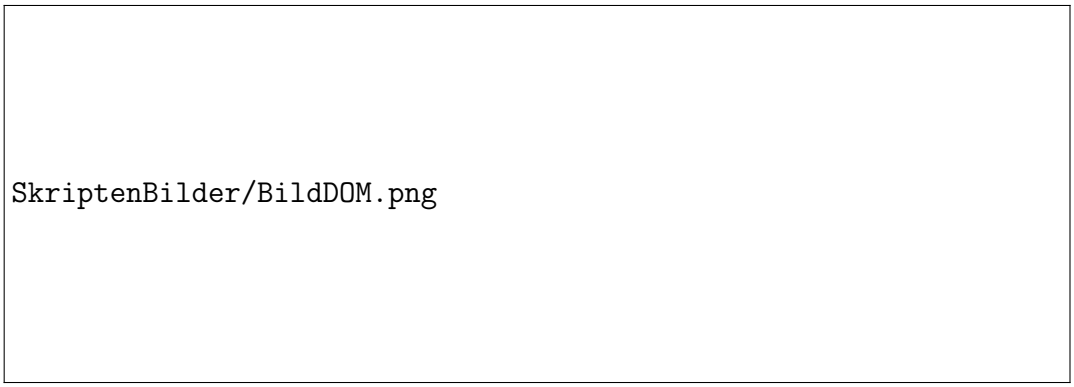
Sobald das gezeigt ist, sind wir fertig, denn dann folgt aus $L(T) \cong L(T')$ sofort $T \leq T' \leq T$ und damit $T = T'$. Seien also Bijektionen $\varphi : T \xrightarrow{\sim} \{1, \ldots, n\}$ und $\varphi' : T' \xrightarrow{\sim} \{1, \ldots, n\}$ beliebig gewählt. Die von φ induzierte Identifikation $\mathcal{S}_T \xrightarrow{\sim} \mathcal{S}_n$ hat die Gestalt $x \mapsto \varphi x \varphi^{-1}$, und den zugehörigen Isomorphismus von Gruppenringen notieren wir analog $C \mapsto \varphi C \varphi^{-1}$. Mit denselben Argumenten wie zuvor gilt es in diesen Notationen zu zeigen

$$T \not\leq T' \quad \Rightarrow \quad (\varphi E_T \varphi^{-1})(\mathbb{C}\mathcal{S}_n)(\varphi' A_{T'} \varphi'^{-1}) = 0$$

Es reicht dazu, für jede Bijektion $\psi : T' \xrightarrow{\sim} T$ zu zeigen

$$T \not\leq T' \quad \Rightarrow \quad E_T \psi A_{T'} = 0$$

Hier ist die Summe nun in hoffentlich offensichtlicher Weise als formale Linearkombination von Bijektionen $T' \xrightarrow{\sim} T$ zu verstehen. Wie zuvor reicht es dafür weiter zu zeigen, daß unter unserer Voraussetzung $T \not\leq T'$ unter jeder Bijektion $T \xrightarrow{\sim} T'$ aus mindestens einer Spalte von T mindestens zwei Kästchen in derselben Zeile von T' landen. In der Tat gibt es dann ja ein s derart, daß T mehr Kästchen in den ersten s Spalten stehen hat als T'. Dann können wir diese Kästchen jedoch nicht so mit Kästchen von T' identifizieren, daß wir in jeder Zeile von T' höchstens s Kästchen erwischen. Also erwischen wir in mindestens einer Zeile von T' mindestens $s+1$ Kästchen, und von denen müssen dann mindestens zwei aus derselben Spalte von T kommen. □



Beispiel zur Dominanzordnung. Stellen wir uns ein Youngdiagramm als eine Geröllhalde von Kästchen vor, so sind in unserer Dominanzordnung genau diejenigen Partitionen kleiner, die entstehen, wenn in unserer Geröllhalde ein oder mehrere Kästchen weiter nach unten purzeln.

Übung 2.9.10. Man zeige, daß das Tensorieren mit der Vorzeichendarstellung dem Übergang zur dualen Partition alias zum an der Hauptdiagonale gespiegelten Youngdiagramm entspricht, in Formeln $L(T) \otimes \operatorname{sgn} \cong L(\tau T)$ für τ die Vertauschung der beiden Koordinaten.

Übung 2.9.11. Man zeige in der Notation 1.4.17 die beiden Implikationen $[M(T) : L(T')] \neq 0 \Rightarrow T \leq T'$ und $[N(T) : L(T')] \neq 0 \Rightarrow T \geq T'$, die beschreiben, welche einfachen Darstellungen als Kompositionsfaktoren von $M(T)$ und $N(T)$ auftreten können. Darüberhinaus zeige man

$$[M(T) : L(T)] = [N(T) : L(T)] = 1$$

Beweis von 2.9.5. Gegeben ein Youngdiagramm T operiert die Gruppe $\mathcal{S}_T$ aller Permutationen der Kästchen frei und transitiv von rechts auf der Menge $\mathcal{B}_T$ aller Tableaus der Gestalt T vermittels der Vorschrift $\varphi^\sigma = \varphi \circ \sigma$ für

$$\varphi : T \xrightarrow{\sim} \{1, 2, \ldots, n\}$$

ein Tableau und $\sigma : T \xrightarrow{\sim} T$ eine Permutation. Als $\mathbb{C}\mathcal{S}_T$-Rechtsmodul ist also $\mathbb{C}\mathcal{S}_T$ isomorph zum freien $\mathbb{C}$-Vektorraum $\mathbb{C}\mathcal{B}_T = \operatorname{Ens}(\mathcal{B}_T, \mathbb{C})$ über der Menge aller Tableaus der Gestalt T mit seiner hoffentlich offensichtlichen Rechtsoperation von $\mathbb{C}\mathcal{S}_T$. Bezeichne nun $\mathcal{D}_T \subset \mathcal{B}_T$ die Menge aller Standardtableaus der Gestalt T. Ich behaupte, daß die Einschränkung res auf die Teilmenge aller Standardtableaus eine Surjektion

$$\operatorname{res} : \operatorname{Ens}(\mathcal{B}_T, \mathbb{C}) E_T A_T \twoheadrightarrow \operatorname{Ens}(\mathcal{D}_T, \mathbb{C})$$

induziert. In der Tat, wenden wir auf ein Standardtableau x der Gestalt T alle Elemente von SZ an, d.h. eine beliebige Vertauschung der Einträge jeder Spalte gefolgt von einer beliebigen Vertauschung der Einträge jeder Zeile, so erhalten wir zwar eventuell außer x selbst noch weitere Standardtableaus, aber für diese ist offensichtlich die Folge der Zeilensummen lexikographisch größer als bei unserem Ausgangstableau. Bezeichnet $[x] \in \operatorname{Ens}(\mathcal{B}_T, \mathbb{C})$ die charakteristische Funktion eines Standardtableaus x, so gilt für unsere Einschränkung res auf die Teilmenge aller Standardtableaus demnach

$$\operatorname{res}\left([x] E_T A_T\right) \in |S|^{-1} |Z|^{-1} [x] + \sum_{x<y} \mathbb{C}[y]$$

wobei die Notation $x < y$ rechts andeuten soll, daß nur über Standardtableaus y mit einer lexikographisch größeren Folge von Zeilensummen summiert wird. So ergibt sich die behauptete Surjektivität. Es folgt, daß die Zahl der Standardtableaus eine untere Schranke für die Dimension von $\operatorname{Ens}(\mathcal{B}_T, \mathbb{C}) E_T A_T$ und damit auch eine untere Schranke für die Dimension der einfachen Darstellung $L(T)$ ist. Daß die Zahl der Standardtableaus sogar mit dieser Dimension übereinstimmt, folgt

dann aus der durch 2.10.1 bewiesenen Formel mit der aus 2.7.6 spezialisierten allgemeinen Erkenntnis

$$\sum_{T\in\mathcal{Y}_n} (\dim_{\mathbb{C}} L(T))^2 = |\mathcal{S}_n| \qquad \square$$

Ergänzung 2.9.12. Eine besonders schöne Formel für die Dimension der irreduziblen Darstellung $L(T)$ einer symmetrischen Gruppe ist die **Hakenlängenformel**

$$\dim_{\mathbb{C}} L(T) = \frac{|T|!}{\prod_{(i,j)\in T}(\text{Hakenlänge von } (i,j))}$$

Die **Hakenlänge** eines Kästchens $(i,j) \in T$ ist dabei erklärt als die Zahl aller $(a,b) \in T$ mit $a = i, b \geq j$ oder $b = j, a \geq i$. Ich gebe hier keinen Beweis.

2.9.13. Über die Darstellungen der symmetrischen Gruppen ist noch sehr viel mehr bekannt, siehe zum Beispiel [Sag00, Jam78, JK81, FH91]. Was die Darstellungen über Körpern positiver Charakteristik angeht, ist aber auch noch vieles offen. Selbst die Dimensionen der meisten irreduziblen Darstellungen sind in diesem Fall noch nicht bekannt.

2.10 Der Robinson-Schensted-Algorithmus

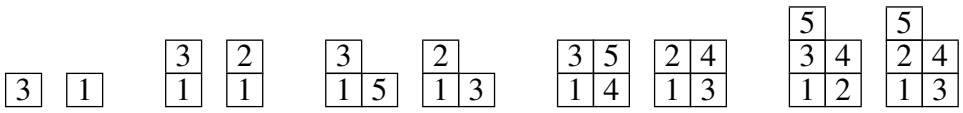
2.10.1. Wir erhalten eine Bijektion zwischen der Menge aller Permutationen σ von $\{1,\ldots,n\}$ und der Menge aller Paare von Standardtableaus mit jeweils n Kästchen und gleicher Gestalt, d.h. gleichem zugrundeliegendem Young-Diagramm vermittels des sogenannten **Robinson-Schensted-Algorithmus** wie folgt: Zunächst stellen wir unsere Zahlen in der durch σ gegebenen Reihenfolge auf als $\sigma(1), \sigma(2), \ldots, \sigma(n)$. Dann lassen wir sie "ein Young-Haus bauen und bewohnen" nach den folgenden Regeln: Im i-ten Schritt geht die Zahl $\sigma(i)$ von links nach rechts durch die erste Etage des Young-Hauses, wie es bis dahin bereits konstruiert ist. Ist sie größer als alle Bewohnerinnen der ersten Etage, baut sie an ihrem Ende ein Kästchen an und zieht dort ein. Sonst verdrängt sie die erste Bewohnerin der ersten Etage, die größer ist als sie selber, und diese versucht es in der zweiten Etage. Ist sie größer als alle Bewohnerinnen der zweiten Etage, so baut sie sich am Ende der zweiten Etage ein Kästchen an und zieht dort ein. Sonst verdrängt sie in der zweiten Etage die erste Bewohnerin, die größer ist als sie selber, und diese versucht es in der dritten Etage etc. Der i-te Schritt ist fertig, wenn die Zahlen $\sigma(1), \sigma(2), \ldots, \sigma(i)$ alle wieder in einem Kästchen wohnen. So entsteht, wie man sich unschwer überlegt, ein Standardtableau $L(\sigma)$. Die Reihenfolge, in der die Kästchen angebaut werden, erinnern wir in einem zweiten Standardtableau $R(\sigma)$ derselben Gestalt, bei dem in demjenigen Kästchen die Zahl i steht, das im i-ten Schritt angebaut

Illustration der Hakenlängenformel. Eingezeichnet sind alle Haken mit mehr als einem Kästchen. Die zu diesem Young-Diagramm gehörige irreduzible Darstellung hat danach die Dimension

$$\frac{8!}{6 \cdot 5 \cdot 3 \cdot 2 \cdot 2} = 8 \cdot 7 \cdot 2 = 112$$

wurde. Daß wir auf diese Weise in der Tat eine Bijektion zwischen der Menge aller Permutationen und der Menge aller Paare von Standardtableaus gleicher Gestalt erhalten, kann der Leser hoffentlich ohne allzu große Schwierigkeiten selbst einsehen. In jedem Fall denke ich, daß es noch schwieriger wäre, einen in Worten aufgeschriebenen Beweis nachzuvollziehen.

Beispiel 2.10.2. Es sei $\sigma(1), \sigma(2), \ldots, \sigma(5)$ die Folge $3, 1, 5, 4, 2$. Wir erhalten der Reihe nach



und das Paar von Standardtableaus ganz am Ende der Zeile ist dann dasjenige, das der Robinson-Schensted-Algorithmus unserer Permutation σ zuordnet.

2.11 Berechnung der Charaktere

2.11.1. Aus dem Beweis von Satz 2.9.2 wissen wir insbesondere, daß für je zwei Young-Diagramme $T, T' \in \mathcal{Y}_n$ gilt

$$\mathrm{Hom}_{\mathbb{C}}^{\mathcal{S}_n}(M(T), N(T')) \neq 0 \quad \Rightarrow \quad T \leq T'$$

Zusätzlich wissen wir aus demselben Beweis $\dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}}^{\mathcal{S}_T}(M(T), N(T)) = 1$. Es ist nun für das folgende bequemer, mit Partitionen natürlicher Zahlen im Sinne von III.1.3.1 zu arbeiten. Gegeben eine Partition $\lambda \in \mathcal{P}_n$ alias eine absteigende Folge $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_r > 0 = 0 = 0 \ldots$ natürlicher Zahlen mit Summe n bilden wir in hoffentlich offensichtlicher Weise die Untergruppe $\mathcal{S}_\lambda = \mathcal{S}_{\lambda_1} \times \ldots \times S_{\lambda_r} \subset \mathcal{S}_n$ der symmetrischen Gruppe und schreiben

$$M(\lambda) = (\mathbb{C}\mathcal{S}_n)E_\lambda$$

mit $E_\lambda = |\mathcal{S}_\lambda|^{-1} \sum_{g \in \mathcal{S}_\lambda} g$ für die Darstellung, die wir später auch als die induzierte der trivialen Darstellung $M(\lambda) = \mathrm{ind}_{\mathcal{S}_\lambda}^{\mathcal{S}_n} \mathbb{C}$ verstehen werden. Wie in III.1.3.4 erklärt liefert das Bilden der Spaltenlängen eine Bijektion $s : \mathcal{Y}_n \xrightarrow{\sim} \mathcal{P}_n$ und für $\lambda = s(T)$ haben wir per definitionem $M(\lambda) = M(T)$. Ebenso setzen wir dann $L(\lambda) = L(T)$ und übertragen die Dominanzordnung 2.9.9 vermittels s von Young-Tableaus auf Partitionen. Notieren wir nun die Charaktere der induzierten Darstellung $M(\lambda)$ und der einfachen Darstellung $L(\lambda)$ als

$$\chi_{M(\lambda)} = \psi_\lambda \quad \text{und} \quad \chi_{L(\lambda)} = \chi_\lambda$$

so liefern unsere obigen Formeln

$$\psi_\lambda = \chi_\lambda + \sum_{\mu > \lambda} a_{\lambda,\mu} \chi_\mu$$

mit natürlichen Zahlen $a_{\lambda,\mu}$.Wir können also die Charaktere χ_λ der einfachen Darstellungen erhalten, indem wir auf die Basis der ψ_λ mit einer Anordnung, in der die ψ_λ zu größeren Indizes zuerst kommen, das Gram-Schmidt'sche Orthogonalisierungsverfahren anwenden.

2.11.2. Nun liefert wie zu Beginn des Beweises von 2.9.2 das Auswerten auf dem Idempotenten Isomorphismen $\mathrm{Hom}_{\mathbb{C}}^{\mathcal{S}_n}((\mathbb{C}\mathcal{S}_n)E_\lambda, (\mathbb{C}\mathcal{S}_n)E_\mu) \xrightarrow{\sim} E_\lambda(\mathbb{C}\mathcal{S}_n)E_\mu$ und für das Skalarprodukt der zugehörigen Charaktere folgt sofort

$$(\psi_\lambda, \psi_\mu) = |\mathcal{S}_\lambda \backslash \mathcal{S} / \mathcal{S}_\mu|$$

Um die Kardinaltität des Raums der Doppelnebenklassen zu berechnen beachten wir die Bahnformel $|Gx| \cdot |G_x| = |G|$ und folgern für jede endliche G-Menge die Formel

$$|G\backslash X| = \sum_{x\in X} \frac{1}{|Gx|} = \sum_{x\in X} \frac{|G_x|}{|G|}$$

Ist speziell $X = \mathcal{S}_n$ und $G = \mathcal{S}_\lambda \times \mathcal{S}_\mu$, so spezialisiert sie zu

$$|\mathcal{S}_\lambda \backslash \mathcal{S}_n / \mathcal{S}_\mu| = \frac{1}{|\mathcal{S}_\lambda| \cdot |\mathcal{S}_\mu|} \sum_{x\in \mathcal{S}_n} |x\mathcal{S}_\lambda x^{-1} \cap \mathcal{S}_\mu|$$

Untersuchen wir das für jede Konjugationsklasse $\mathcal{C}_\nu \subset \mathcal{S}_n$ separat und beachten für den Zentralisator Z eines Elements der Konjugationsklasse $\mathcal{C}_\nu$ die Bahnformel $|\mathcal{C}_\nu| \cdot |Z| = |\mathcal{S}_n|$, so ergibt sich

$$|\mathcal{S}_\lambda \backslash \mathcal{S}_n / \mathcal{S}_\mu| = \frac{|\mathcal{S}|_n}{|\mathcal{S}_\lambda| \cdot |\mathcal{S}_\mu|} \sum_\nu \frac{|\mathcal{S}_\lambda \cap \mathcal{C}_\nu| \cdot |\mathcal{S}_\mu \cap \mathcal{C}_\nu|}{|\mathcal{C}_\nu|}$$

2.11.3. Für die Gruppe $\mathcal{S}_4$ haben wir zum Beispiel die Partitionen $\lambda = (4), (3,1), (2^2), (2,1^2), (1^4)$ in abkürzender Notation, wo die Hochzahlen Vielfachheiten meinen, so daß etwa $((2,1^2)$ ein Kürzel wäre für die Partition $4 = 2+1+1$. Wir erhalten $|\mathcal{S}_\lambda| = 24, 6, 4, 2, 1$ und $|\mathcal{C}_\lambda| = 6, 8, 3, 6, 1$ und die Kardinalitäten der Schnitte $|\mathcal{S}_\lambda \cap \mathcal{C}_\nu|$ werden gegeben durch

$\nu\backslash\lambda$	4	3,1	2^2	$2,1^2$	1^4
4	6	0	0	0	0
3,1	8	2	0	0	0
2^2	3	0	1	0	0
$2,1^2$	6	3	2	1	0
1^4	1	1	1	1	1

womit sich die Matrix der (ψ_λ, ψ_μ) ergibt zu

	4	3,1	2^2	$2,1^2$	1^4
4	1	1	1	1	1
3,1	1	2	2	3	4
2^2	1	2	3	4	6
$2,1^2$	1	3	4	7	12
1^4	1	4	6	12	24

Damit ergibt sich die Zerlegung unserer induzierten Darstellungen in einfache Darstellungen zu

$$\begin{aligned}
\psi_{(4)} &= \chi_{(4)} \\
\psi_{(3,1)} &= \chi_{(3,1)} + \chi_{(4)} \\
\psi_{(2^2)} &= \chi_{(2^2)} + \chi_{(3,1)} + \chi_{(4)} \\
\psi_{(2,1^2)} &= \chi_{(2,1^2)} + \chi_{(2^2)} + 2\chi_{(3,1)} + \chi_{(4)} \\
\psi_{(1^4)} &= \chi_{(1^4)} + 3\chi_{(2,1^2)} + 2\chi_{(2^2)} + 3\chi_{(3,1)} + \chi_{(4)}
\end{aligned}$$

2.12 Reeller, komplexer und quaternionaler Typ

2.12.1. Wir erinnern an die Körper bzw. Schiefkörper $\mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$ der reellen Zahlen, komplexen Zahlen und Quaternionen und bezeichnen Darstellungen einer Gruppe G über den jeweiligen Ringen als reelle, komplexe und quaternionale Darstellungen. Die Restriktion der Skalare macht in offensichtlicher Weise aus quaternionalen Darstellungen komplexe Darstellungen und aus komplexen Darstellungen reelle Darstellungen. Umgekehrt macht die Erweiterung der Skalare aus reellen Darstellungen komplexe Darstellungen und aus komplexen Darstellungen quaternionale Darstellungen. In Formeln meint man etwa für V eine komplexe Darstellung mit der durch Erweiterung der Skalare gegebene quaternionale Darstellung die quaternionale Darstellung $\mathbb{H} \otimes_{\mathbb{C}} V$ mit $\mathbb{H}$ aus II.2.9.4, wobei das Tensorprodukt in Bezug auf die Wirkung von $\mathbb{C}$ auf $\mathbb{H}$ durch Multiplikation von rechts zu verstehen ist.

Definition 2.12.2. 1. Eine reelle Darstellung heißt

(a) von **quaternionalem Typ** genau dann, wenn sie durch Restriktion der Skalare aus einer quaternionalen Darstellung entsteht;

(b) von **komplexem Typ**, wenn sie durch Restriktion der Skalare zwar nicht aus einer quaternionalen, aber doch immerhin aus einer komplexen Darstellung entsteht;

(c) und von **reellem Typ** sonst.

2. Eine komplexe Darstellung heißt
   (a) von **reellem Typ**, wenn sie isomorph ist zu einer Darstellung, die durch Erweiterung der Skalare aus einer reellen Darstellung entsteht;
   (b) von **quaternionalem Typ**, wenn sie durch Restriktion der Skalare aus einer quaternionalen Darstellung entsteht;
   (c) und von **komplexem Typ** sonst.
3. Eine quaternionale Darstellung heißt
   (a) von **reellem Typ**, wenn sie isomorph ist zu einer Darstellung, die durch Erweiterung der Skalare aus einer reellen Darstellung entsteht;
   (b) von **komplexem Typ**, wenn sie zwar nicht von reellem Typ ist, aber isomorph ist zu einer Darstellung, die durch Erweiterung der Skalare aus einer komplexen Darstellung entsteht;
   (c) und von **quaternionalem Typ** sonst.

2.12.3. Gegeben eine irreduzible reelle Darstellung höchstens abzählbarer Dimension ist ihr Endomorphismenring nach III.3.8.2 als $\mathbb{R}$-Ringalgebra isomorph zu genau einem der Ringe $\mathbb{R}, \mathbb{C}$ oder $\mathbb{H}$, und offensichtlich können wir den Typ unserer Darstellung in diesem Fall an ihrem Endomorphismenring ablesen.

2.12.4. Gegeben eine irreduzible quaternionale Darstellung höchstens abzählbarer Dimension ist ihr Endomorphismenring nach III.3.8.2 als $\mathbb{R}$-Ringalgebra isomorph zu genau einem der Ringe $\mathbb{R}, \mathbb{C}$ oder $\mathbb{H}$. Wieder können wir den Typ unserer Darstellung an ihrem Endomorphismenring ablesen, aber diesmal ist die Beziehung umgekehrt, der Endomorphismenring $\mathbb{R}$ zeigt quaternionalen Typ an und der Endomorphismenring $\mathbb{H}$ reellen Typ. In der Tat liefert die Rechtsmultiplikation auf dem ersten Tensorfaktor für jede reelle Darstellung V von G einen $\mathbb{R}$-linearen Ringhomomorphismus $\mathbb{H}^{\mathrm{opp}} \to \mathrm{End}^G_{\mathbb{H}}(\mathbb{H} \otimes_{\mathbb{R}} V)$, und ist umgekehrt eine quaternionale Darstellung W von G mit einem $\mathbb{R}$-linearen Ringhomomorphismus $\mathbb{H}^{\mathrm{opp}} \to \mathrm{End}^G_{\mathbb{H}}(W)$ gegeben, so können wir W als Modul über $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H}^{\mathrm{opp}}$ mit G-Operation auffassen, nach 2.12.5 also als Modul über $\mathrm{End}_{-\mathbb{R}} \mathbb{H}$ mit G-Operation und nach 1.6.11 entsteht W dann durch Erweiterung der Skalare $\mathbb{H}\otimes_{\mathbb{R}}$ aus einer reellen Darstellung von G. Ähnlich liefert die Rechtsmultiplikation auf dem ersten Tensorfaktor für jede komplexe Darstellung V von G einen $\mathbb{R}$-linearen Ringhomomorphismus $\mathbb{C}^{\mathrm{opp}} \to \mathrm{End}^G_{\mathbb{H}}(\mathbb{H} \otimes_{\mathbb{C}} V)$, und ist umgekehrt eine quaternionale Darstellung W von G mit einem $\mathbb{R}$-linearen Ringhomomorphismus $\mathbb{C}^{\mathrm{opp}} \to \mathrm{End}^G_{\mathbb{H}}(W)$ gegeben, so können wir W als Modul über $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C}^{\mathrm{opp}}$ mit G-Operation auffassen, nach 2.12.5 also als Modul über $\mathrm{End}_{-\mathbb{C}} \mathbb{H}$ mit G-Operation und nach 1.6.11 entsteht W dann durch Erweiterung der Skalare $\mathbb{H}\otimes_{\mathbb{C}}$ aus einer komplexen Darstellung von G.

Übung 2.12.5. Die Abbildung $q \otimes w \mapsto (u \mapsto quw)$ induziert einen Ringisomorphismus $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H}^{\mathrm{opp}} \xrightarrow{\sim} \mathrm{End}_{\mathbb{R}}(\mathbb{H})$. Dieselbe Abbildung induziert einen Ringisomorphismus $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C}^{\mathrm{opp}} \xrightarrow{\sim} \mathrm{End}_{-\mathbb{C}}(\mathbb{H})$.

2.12.6. Auch irreduzible komplexe Darstellungen höchstens abzählbarer Dimension haben einen wohlbestimmten Typ, d.h. können nicht gleichzeitig durch Skalarerweiterung aus einer reellen Darstellung und durch Restriktion aus einer quaternionalen Darstellung hervorgehen. Um das zu sehen, holen wir etwas weiter aus, um diese Behauptung dann schließlich in 2.12.10 sogar etwas allgemeiner zu zeigen für beliebige komplexe Darstellungen mit Endomorphismenring $\mathbb{C}$.

2.12.7. Zu jedem komplexen Vektorraum V bilden wir wie in II.4.6.14 den komplex konjugierten Vektorraum $\overline{V}$, indem wir dieselbe unterliegende additive Gruppe nehmen, die Operation von $a \in \mathbb{C}$ auf $v \in V$ jedoch ändern zu einer Operation $a \cdot v$, die mit der ursprünglichen Operation av verknüpft ist durch die Formel $a \cdot v = \bar{a}v$. Ist V eine komplexe Darstellung einer Gruppe G, so ist $\overline{V}$ mit derselben Operation von G auch eine komplexe Darstellung, die **komplex konjugierte Darstellung**.

Übung 2.12.8. Gegeben eine endlichdimensionale komplexe Darstellung V einer endlichen Gruppe G ist die komplex konjugierte Darstellung stets isomorph zur kontragredienten Darstellung, in Formeln $\overline{V} \cong V^*$. Hinweis: 2.6.5.

Proposition 2.12.9. *Sei V eine komplexe Darstellung einer Gruppe G.*

1. *Genau dann ist V die Komplexifizierung einer reellen Darstellung von G, wenn es einen Isomorphismus von Darstellungen $J : V \xrightarrow{\sim} \overline{V}$ gibt mit $J^2 = \mathrm{id}_V$;*

2. *Genau dann ist V die Restriktion einer quaternionalen Darstellung von G, wenn es einen Isomorphismus von Darstellungen $J : V \xrightarrow{\sim} \overline{V}$ gibt mit $J^2 = -\mathrm{id}_V$.*

Beweis. Im ersten Fall ist V isomorph zur Komplexifizierung der reellen Unterdarstellung V^J der J-Invarianten, vergleiche auch **??**. Im zweiten Fall können wir V zu einem $\mathbb{H}$-Rechtsmodul machen, indem wir als Rechtsmultiplikation mit $\mathrm{j} \in \mathbb{H}$ unser J nehmen. Der Rest des Beweises sei dem Leser überlassen. □

Korollar 2.12.10. *Sei V eine komplexe Darstellung einer Gruppe G, deren einzige Endomorphismen die Skalare sind, in Formeln $\mathrm{Mod}_{\mathbb{C}}^{G} V = \mathbb{C}$. So sind wir in genau einem der folgenden drei Fälle:*

1. *Die Darstellung V ist von reellem Typ, d.h. entsteht aus einer reellen Darstellung W durch Komplexifizierung.*

2. *Die Darstellung V ist von quaternionalem Typ, d.h. entsteht aus einer quaternionalen Darstellung V über $\mathbb{H}$ durch Restriktion der Skalare.*

3. *Die Darstellung V ist nicht isomorph zu ihrer komplex konjugierten Darstellung $\overline{V}$.*

2.12.11. Per definitionem heißt eine komplexe Darstellung von komplexem Typ genau dann, wenn sie weder von reellem noch von quaternionalem Typ ist. Das Korollar impliziert, daß diese Eigenschaft für komplexe Darstellungen mit Endomorphismenring $\mathbb{C}$ gleichbedeutend ist zur Eigenschaft, nicht isomorph zu sein zu ihrer konjugierten Darstellung.

Beweis. Aus unseren Voraussetzungen folgt $\dim \mathrm{Hom}^G(V, \overline{V}) \leq 1$. Ist diese Dimension Null, so sind wir im dritten Fall. Ist diese Dimension Eins, so gibt es einen von Null verschiedenen Homomorphismus $J : V \xrightarrow{\sim} \overline{V}$. Per definitionem gilt

$$Jav = a \cdot Jv = \bar{a}Jv \quad \forall a \in \mathbb{C}, v \in V$$

Nach Annahme gilt auch $J^2 = a\,\mathrm{id}_V$ für geeignetes $a \in \mathbb{C}^\times$, und da J^2 kommutiert mit J, haben wir nach der vorhergehenden Rechnung hier sogar $a \in \mathbb{R}^\times$. Ändern wir J ab um einen Skalar $z \in \mathbb{C}$, so ändert sich J^2 um den Skalar $|z|^2 \in \mathbb{R}_{>0}$. Unter der Voraussetzung $V \cong \overline{V}$ gilt also für alle von Null verschiedenen J entweder $J^2 = a\,\mathrm{id}_V$ mit $a > 0$ oder $J^2 = a\,\mathrm{id}_V$ mit $a < 0$. Im ersten Fall finden wir leicht ein J mit $J^2 = \mathrm{id}_V$ und nach 2.12.9 ist unsere Darstellung die Komplexifizierung einer reellen Darstellung. Im zweiten Fall finden wir leicht ein J mit $J^2 = -\mathrm{id}_V$ und nach 2.12.9 ist unsere Darstellung die Restriktion einer quaternionalen Darstellung. □

Übung 2.12.12. Gegeben eine Gruppe G bezeichne $\mathrm{irra}_{\mathbb{K}} G$ die Menge der Isomorphieklassen irreduzibler Darsellungen von G über $\mathbb{K} = \mathbb{R}, \mathbb{C}, \mathbb{H}$ von höchstens abzählbarer Dimension und

$$\mathrm{irra}_{\mathbb{K}} G = \mathrm{irra}^{\mathbb{R}}_{\mathbb{K}} G \;\sqcup\; \mathrm{irra}^{\mathbb{C}}_{\mathbb{K}} G \;\sqcup\; \mathrm{irra}^{\mathbb{H}}_{\mathbb{K}} G$$

die Zerlegung nach reellem, komplexem und quaterniomalem Typ. So liefern die offensichtlichen durch Restriktion bzw. Erweiterung der Skalare gegebenen Abbildungen Bijektionen

$$\begin{array}{ccccc}
\mathrm{irra}^{\mathbb{H}}_{\mathbb{H}} G & \xrightarrow{\sim} & \mathrm{irra}^{\mathbb{H}}_{\mathbb{C}} G & \xrightarrow{\sim} & \mathrm{irra}^{\mathbb{H}}_{\mathbb{R}} G \\
\mathrm{irra}^{\mathbb{R}}_{\mathbb{H}} G & \xleftarrow{\sim} & \mathrm{irra}^{\mathbb{R}}_{\mathbb{C}} G & \xleftarrow{\sim} & \mathrm{irra}^{\mathbb{R}}_{\mathbb{R}} G \\
\mathrm{irra}^{\mathbb{C}}_{\mathbb{H}} G & \xleftarrow{\sim} & \mathrm{irra}^{\mathbb{C}}_{\mathbb{C}} G/_{(V \sim \overline{V})} & \xrightarrow{\sim} & \mathrm{irra}^{\mathbb{C}}_{\mathbb{R}} G
\end{array}$$

wo in der Mitte der untersten Zeile der Quotient nach der Äquivalenzrelation gemeint ist, unter der eine Darstellung und ihre komplex konjugierte Darstellung

identifiziert werden. Hierbei bestehen im übrigen nach 2.12.10 alle Äquivalenzklassen aus genau zwei Elementen. Hinweis: Für die Wohldefiniertheit der Abbildung unten links muß der Leser zunächst $\mathbb{H} \otimes_{\mathbb{C}} V \cong \mathbb{H} \otimes_{\mathbb{C}} \overline{V}$ zeigen. Die Surjektivität aller Abbildungen folgt aus den Definitionen. Für die Injektivität etwa der ersten Abbildung oben links beachte man $\mathbb{H} \otimes_{\mathbb{C}} V \cong V \oplus V$ für jede quaternionale Darstellung V. Die Injektivität der anderen Pfeile zeigt man ähnlich.

Proposition 2.12.13. *Seien G eine Gruppe und V eine endlichdimensionale einfache Darstellung von G über einem algebraisch abgeschlossenen Körper k mit $\operatorname{char} k \neq 2$. So sind wir in genau einem der folgenden drei Fälle:*

1. *Es gibt auf V eine von Null verschiedene symmetrische G-invariante Bilinearform. Diese ist dann nichtausgeartet und bis auf einen Skalar eindeutig bestimmt.*
2. *Es gibt auf V eine von Null verschiedene symplektische G-invariante Bilinearform. Diese ist dann nichtausgeartet und bis auf einen Skalar eindeutig bestimmt.*
3. *Es gibt auf V keine von Null verschiedene G-invariante Bilinearform.*

Beweis. Nach dem Schur'schen Lemma haben wir $\dim \operatorname{Hom}_k^G(V, V^*) \leq 1$ und jeder von Null verschiedene Homomorphismus ist ein Isomorphismus. Da unsere Identifikation $\operatorname{Hom}(V, V^*) \xrightarrow{\sim} \operatorname{Bil}(V)$ aus 2.12.14 verträglich ist mit der Operation von G, folgt auch für den Raum der invarianten Bilinearformen

$$\dim_k \operatorname{Bil}(V)^G \leq 1$$

und jede von Null verschiedene invariante Bilinearform ist nichtausgeartet. Ist unser Raum von Bilinearformen eindimensional, so operiert schließlich unsere durch das Vertauschen der Argumente definierte Selbstinverse aus 2.12.15 darauf entweder als die Identität oder als die Multiplikation mit (-1). □

Übung 2.12.14. Gegeben ein Vektorraum V über einem Körper k erhalten wir eine Bijektion

$$\operatorname{Hom}(V, V^*) \xrightarrow{\sim} \operatorname{Bil}(V)$$

zwischen dem Raum der Homomorphismen von V in seinen Dualraum und dem Raum der Bilinearformen auf V, indem wir jedem Homomorphismus $\varphi : V \to V^*$ die Bilinearform $\hat{\varphi}$ zuordnen, die gegeben wird durch $\hat{\varphi}(v, w) = (\varphi(v))(w)$. Wir kennen diese Bijektion bereits aus **??**, wo wir ihre Inverse $g \mapsto \operatorname{can}_g$ notiert hatten.

Übung 2.12.15. Gegeben ein Vektorraum V über einem Körper k haben wir auf dem Raum $\operatorname{Bil}(V)$ der Bilinearformen eine natürliche selbstinverse Abbildung, das "Vertauschen der Argumente". Ihr Eigenraum zum Eigenwert 1 besteht genau

aus allen symmetrischen Bilinearformen, ihr Eigenraum zum Eigenwert (-1) aus allen symplektischen alias alternierenden Bilinearformen, und Fall $\operatorname{char} k \neq 2$ ist $\operatorname{Bil}(V)$ die direkte Summe dieser Eigenräume.

2.12.16. Im allgemeinen definiert man S^2V als den Quotienten von $V \otimes V$ nach allen $v \otimes w - w \otimes v$ und $\bigwedge^2 V$ als den Quotienten von $V \otimes V$ nach allen $v \otimes v$. Ist unsere Charakteristik nicht Zwei, so geht der Unterraum der Invarianten unter der Vertauschung der Faktoren unter der Projektion isomorph nach S^2V der Unterraum der Schiefinvarianten isomorph nach $\bigwedge^2 V$, aber in Charakteristik zwei ist beides nicht mehr richtig. Für endlichdimensionales V haben wir stets $\operatorname{Bil}(V) = V^* \otimes V^*$ in kanonischer Weise.

Lemma 2.12.17. *Ist V ein endlichdimensionaler Vektorraum und $g : V \to V$ eine lineare Abbildung, so haben wir*

$$\operatorname{tr}(g^2|V) = \operatorname{tr}(g|S^2V) - \operatorname{tr}(g|\bigwedge^2 V)$$

Beweis. Ist g diagonalisierbar und $v_1, \ldots, v_n$ eine Basis aus Eigenvektoren zu Eigenwerten $\lambda_1, \ldots, \lambda_n$, so ist $(v_i v_j)_{i \leq j}$ eine Basis aus Eigenvektoren in S^2V und $(v_i \wedge v_j)_{i<j}$ eine Basis von Eigenvektoren von $\bigwedge^2 V$ und unsere Behauptung reduziert sich auf die offensichtliche Identität

$$\sum_{i=1}^{n} \lambda_i^2 = \sum_{i \leq j} \lambda_i \lambda_j - \sum_{i<j} \lambda_i \lambda_j$$

Im allgemeinen ist g jedenfalls trigonalisierbar über einer geeigneten Erweiterung des Grundkörpers, und dann greift dasselbe Argument. □

Proposition 2.12.18. *Gegeben eine einfache Darstellung V einer endlichen Gruppe G über einem algebraisch abgeschlossenen Körper einer von Zwei verschiedenen Charakteristik gilt*

$$|G|^{-1} \sum \chi_V(g^2) = \begin{cases} 1 & \textit{falls } V \textit{ eine symmetrische Form besitzt;} \\ 0 & \textit{falls } V \textit{ keine Form besitzt;} \\ -1 & \textit{falls } V \textit{ eine symplektische Form besitzt.} \end{cases}$$

Mit der Abkürzung "Form" sind jeweils von Null verschiedene G-invariante Bilinearformen gemeint, die dann wie bereits gezeigt notwendig nichtausgeartet sind.

Beweis. Gegeben ein Vektorraum V über einem Körper einer von Zwei verschiedenen Charakteristik zerfällt der Raum der Bilinearformen $\operatorname{Bil}(V)$ in die Teilräume

$$\operatorname{Bil}(V) = \operatorname{Sym}(V) \oplus \operatorname{Alt}(V)$$

der symmetrischen bzw. alternierenden Bilinearformen. Ist V eine Darstellung einer Gruppe G, so notieren wir die entsprechende Darstellung

$$B = S \oplus A$$

Die entsprechenden kanonischen Identifikationen definieren Isomorphismen von Darstellungen $S^2V^* \xrightarrow{\sim} S$ und $\bigwedge^2 V^* \xrightarrow{\sim} A$ und mit Lemma 2.12.17 erhalten wir

$$\chi_V(g^2) = \chi_S(g^{-1}) - \chi_A(g^{-1})$$

Nun gilt ja $(\chi_S, \chi_{\text{triv}}) = 1$ bzw. $(\chi_A, \chi_{\text{triv}}) = 1$ in Bezug auf unsere symmetrische Bilinearform aus 2.8.9 genau dann, wenn es auf V bis auf Skalar genau eine nichtausgeartete symmetrische bzw. symplektische Form gibt. Die Proposition folgt. □

Proposition 2.12.19. *Sei G eine endliche Gruppe und V eine einfache komplexe Darstellung von G.*

1. *Genau dann ist V von reellem Typ, wenn es auf V eine nichtausgeartete symmetrische G-invariante Bilinearform gibt.*
2. *Genau dann ist V quaternionalem Typ, wenn es auf V eine nichtausgeartete symplektische G-invariante Bilinearform gibt.*
3. *Genau dann ist V von komplexem Typ, wenn V nicht isomorph ist zu seiner eigenen kontragredienten Darstellung, $V \ncong V^*$.*

2.12.20. Ich zeige zu Ende dieses Abschnitts als 2.12.26 auch noch eine Variante dieser Proposition im Fall nicht notwendig einfacher Darstellungen. Dann schließen sich die Fälle jedoch nicht mehr gegenseitig aus.

Beweis. 1. Ist unsere Darstellung die Komplexifizierung einer Darstellung über $\mathbb{R}$, so erhalten wir durch Komplexifizieren eines invarianten Skalarprodukts auf besagter Darstellung über $\mathbb{R}$ eine invariante nichtausgeartete symmetrische Bilinearform auf unserer komplexen Darstellung. Ist umgekehrt eine invariante symmetrische Bilinearform $(v, w) \mapsto s(v, w)$ gegeben, so wählen wir zusätzlich ein invariantes Skalarprodukt $(v, w) \mapsto \langle v, w\rangle$ und betrachten die Komposition J der von unserer Bilinearform und unserem Skalarprodukt induzierten Isomorphismen

$$V \xrightarrow{\sim} V^* \xrightarrow{\sim} \overline{V}$$

Per definitionem gilt $(v, w) = \langle v, Jw\rangle \ \forall v, w \in V$ und folglich

$$\langle v, J^2w\rangle = (v, Jw) = (Jw, v) = \langle Jw, Jv\rangle$$

und wir erkennen, daß J^2 selbstadjungiert ist und nur positive Eigenwerte hat. Aus dem Schur'schen Lemma folgt $J^2 = a\,\mathrm{id}_V$ mit $a > 0$. Mit 2.12.9 folgt dann leicht, daß unsere Darstellung die Komplexifizierung einer Darstellung über $\mathbb{R}$ ist.

2. Ist unsere Darstellung die Restriktion einer Darstellung über $\mathbb{H}$, so ist der j-Teil im Sinne von 2.12.23 eines invarianten quaternionalen Skalarprodukts im Sinne von 2.12.21, das es nach 2.12.24 stets gibt, eine invariante nichtausgeartete symplektische Bilinearform auf unserer komplexen Darstellung. Ist umgekehrt eine invariante symplektische Bilinearform gegeben, so liefert unsere Konstruktion wieder ein komplex-schieflineares J, für das J^2 selbstadjungiert ist und diesmal nur negative Eigenwerte hat. Aus dem Schur'schen Lemma folgt dann $J^2 = a\,\mathrm{id}_V$ mit $a < 0$, und mit 2.12.9 folgt dann leicht, daß unsere Darstellung die Restriktion einer quaternionalen Darstellung ist.

3. Das ist klar nach 2.12.8. □

Definition 2.12.21. Ein **Skalarprodukt** oder genauer ein **quaternionales Skalarprodukt** auf einem quaternionalen Vektorraum alias $\mathbb{H}$-Rechtsmodul V ist eine Abbildung $V \times V \to \mathbb{H}$, $(v,w) \mapsto \langle v,w\rangle$ derart, daß für alle $v,w,v',w' \in V$ und $\lambda,\mu \in \mathbb{H}$ gilt:

1. $\langle v+v',w\rangle = \langle v,w\rangle + \langle v',w\rangle$, $\langle v\lambda,w\rangle = \bar{\lambda}\langle v,w\rangle$.
2. $\langle v,w+w'\rangle = \langle v,w\rangle + \langle v,w'\rangle$, $\langle v,w\mu\rangle = \langle v,w\rangle\mu$.
3. $\langle v,w\rangle = \overline{\langle w,v\rangle}$, insbesondere $\langle v,v\rangle \in \mathbb{R}$.
4. $\langle v,v\rangle \leq 0 \Rightarrow v = 0$.

Beispiel 2.12.22. Auf dem $\mathbb{H}^n$ erhalten wir ein quaternionales Skalarprodukt durch die Vorschrift $\langle v,w\rangle = \bar{v}_1 w_1 + \ldots + \bar{v}_n w_n$.

Übung 2.12.23. Jedes $q \in \mathbb{H}$ läßt sich eindeutig schreiben als $q = z + \mathrm{j}\,w$ mit $z,w \in \mathbb{C}$. Ich nenne dann w den **j-Teil** von q und schreibe $w = \mathrm{jot}(q)$. Man prüft leicht $\mathrm{jot}(zq) = \bar{z}\,\mathrm{jot}(q)$ für $z \in \mathbb{C}$ und $\mathrm{jot}(\bar{q}) = -\mathrm{jot}(q)$. Man zeige: Gegeben ein Skalarprodukt auf einem quaternionalen Vektorraum ist die Zuordnung $(v,w) \mapsto \mathrm{jot}\langle v,w\rangle$ komplex-bilinear und symplektisch.

Übung 2.12.24. Auf jeder endlichdimensionalen quaternionalen Darstellung einer endlichen Gruppe existiert ein invariantes quaternionales Skalarprodukt.

Korollar 2.12.25. *Gegeben eine einfache komplexe Darstellung V einer endlichen Gruppe G gilt*

$$|G|^{-1}\sum \chi_V(g^2) = \begin{cases} 1 & \textit{falls } V \textit{ von reellem Typ ist;} \\ 0 & \textit{falls } V \textit{ von komplexem Typ ist;} \\ -1 & \textit{falls } V \textit{ von quaternionalem Typ ist.} \end{cases}$$

Beweis. Das folgt sofort, wenn man 2.12.18 mit 2.12.13 kombiniert. □

Proposition 2.12.26. *Seien G eine endliche Gruppe und V eine endlichdimensionale komplexe Darstellung von G. So gilt:*

1. *Genau dann ist V isomorph zur Komplexifizierung einer reellen Darstellung von G, wenn es auf V eine invariante nichtausgeartete symmetrische Bilinearform gibt.*

2. *Genau dann ist V isomorph zur Restriktion einer quaternionalen Darstellung von G, wenn es auf V eine invariante nichtausgeartete symplektische Bilinearform gibt.*

Beweis. Die Hinrichtung geht genauso wie im Beweis von 2.12.13. Für die Rückrichtung wählen wir wie im Beweis von 2.12.13 auf unserer Darstellung ein invariantes Skalarprodukt und finden wieder einen schieflinearen Automorphismus J unserer Darstellung derart, daß J^2 selbstadjungiert ist und nur positive bzw. negative Eigenwerte hat. Ändern wir dann J auf den Eigenräumen von J^2 durch einen geeigneten Skalar ab, so können wir $J^2 = \mathrm{id}$ bzw. $J^2 = -\mathrm{id}$ erreichen. □

2.13 Duale Paare

Definition 2.13.1. Seien G, H Gruppen, M ein $(G \times H)$-Modul über einem Körper k und $\phi : G \to \mathrm{GL}(M), \psi : H \to \mathrm{GL}(M)$ die zugehörigen Homomorphismen. Mann nennt (G, H) ein **duales Paar** vermittels M genau dann, wenn $\mathrm{End}_k^G M$ als k-Algebra erzeugt wird von $\psi(H)$ und ebenso $\mathrm{End}_k^H M$ als k-Algebra von $\phi(G)$.

Proposition 2.13.2 (Zerlegung unter dualen Paaren). *Sind zwei endliche Gruppen G, H ein duales Paar vermittels einer endlichdimensionalen komplexen Darstellung M, so gibt es einfache und paarweise nicht isomorphe Darstellungen $E_1, \ldots, E_r$ von G und $F_1, \ldots, F_r$ von H derart, daß M unter $G \times H$ zerfällt als*

$$M \cong \bigoplus_{\nu=1}^{r} E_\nu \otimes F_\nu$$

2.13.3. Insbesondere liefert ein duales Paar M eine natürliche Bijektion zwischen den einfachen Kompositionsfaktoren von M als G-Modul und den einfachen Kompositionsfaktoren von M als H-Modul. Dasselbe gilt mit demselben Beweis, wenn wir allgemeiner statt der Endlichkeit unserer Gruppen nur fordern, daß M vollständig reduzibel ist sowohl über G als auch über H. Unter dieser Voraussetzung gilt die Aussage sogar über einem beliebigen algebraisch abgeschlossenen Grundkörper.

Beweis. Mit 2.4.5 können wir so eine Zerlegung der gewünschten Art finden mit den E_r irreduzibel und paarweise nicht isomorph. Aber dann liefert die offensichtliche Abbildung einen Isomorphismus $\prod_{\nu=1}^{r} \operatorname{End}_{\mathbb{C}} F_\nu \xrightarrow{\sim} \operatorname{End}_{\mathbb{C}}^{G} M$. Folglich sind die F_ν einfache Moduln für $\operatorname{End}_{\mathbb{C}}^{G} M$ und damit nach Annahme für H. □

2.14 Darstellungen semidirekter Produkte

2.14.1. Wir gehen aus von einer Operation einer endlichen Gruppe G auf einer kommutativen Gruppe N und interessieren uns für die Menge der Isomorphieklassen $\operatorname{irrf}_{\mathbb{C}}(G \ltimes N)$ endlichdimensionaler irreduzibler komplexer Darstellungen des semidirekten Produkts $G \ltimes N$. Jede endlichdimensionale Darstellung V von $G \ltimes N$ zerfällt unter N in isotypische Komponenten

$$V = \bigoplus_{\chi \in \hat{N}} V_\chi$$

wo wir $\hat{N} := \operatorname{irrf}_{\mathbb{C}} N$ abgekürzt haben. Die Operation von G auf N induziert eine Operation von G auf $\hat{N}$, und für alle $g \in G$ gilt offensichtlich $g : V_\chi \to V_{g\chi}$. Folglich bilden für jede G-Bahn $\mathcal{O} \subset \hat{N}/G$ die zugehörigen isotypischen Komponenten eine Unterdarstellung

$$V_{\mathcal{O}} = \bigoplus_{\chi \in \mathcal{O}} V_\chi$$

Ist V irreduzibel, so muß es demnach genau eine Bahn $\mathcal{O} = \mathcal{O}(V)$ geben mit $V_{\mathcal{O}} \neq 0$, für die dann gilt $V = V_{\mathcal{O}}$. Nehmen wir nun $V = V_{\mathcal{O}}$ an und wählen $\chi \in \mathcal{O}$ beliebig und bezeichnen mit $G_\chi \subset G$ seine Isotropiegruppe, so ist V_χ eine Darstellung von $G_\chi \ltimes N$ und die von der Frobenius-Reziprozität **??** herkommende Abbildung ist ein Isomorphismus von G-Darstellungen

$$\operatorname{prod}_{G_\chi \ltimes N}^{G \ltimes N} V_\chi \xrightarrow{\sim} V$$

In der Tat induziert die kanonische Abbildung $V_\chi \to \operatorname{prod}_{G_\chi \ltimes N}^{G \ltimes N} V_\chi$ einen Isomorphismus auf die χ-isotypische Komponente der rechten Seite und ihr Bild erzeugt die produzierte Darstellung: Damit haben sowohl Kern als auch Kokern unseres Isomorphismus in spe höchstens von Null verschiedene isotypische Komponenten an Stellen $\psi \in \mathcal{O}$. Andererseits aber haben sowohl Kern als auch Kokern Komponente Null bei χ, und folglich auch Komponenten Null bei allen $\psi \in \mathcal{O}$. Ist also V_χ keine irreduzible Darstellung von $G_\chi \ltimes N$, so kann V auch selbst nicht irreduzibel gewesen sein. Betrachten wir nun als Menge von Parametern die Menge aller Paare

$$\operatorname{Par} = \{(\chi, W) \mid \chi \in \hat{N},\ W \in \operatorname{irrf}_{\mathbb{C}} G_\chi\}$$

und darauf die hoffentlich offensichtliche Operation von G.

Satz 2.14.2 (Darstellungen semidirekter Produkte). *Gegeben $G \ltimes N$ das semidirekte Produkt einer endlichen Gruppe G mit einer abelschen Gruppe N liefert die Abbildung $V \mapsto \{(\chi, V_\chi) \mid \chi \in \hat{N}$ mit $V_\chi \neq 0\}$ eine Bijektion*

$$\mathrm{irrf}_{\mathbb{C}}(G \ltimes N) \xrightarrow{\sim} \mathrm{Par}\,/G$$

2.14.3. Die Umkehrabbildung der Bijektion aus unserem Satz kann beschrieben werden als

$$[\chi, W] \mapsto \mathrm{prod}_{G_\chi \ltimes N}^{G \ltimes N} \mathbb{C}_\chi \otimes W$$

Hier meint $\mathbb{C}_\chi \otimes W$ die Darstellung von $G_\chi \ltimes N$, die aus W entsteht durch die Erweiterung der Wirkung von G_χ vermittels der Vorschrift, daß $n \in N$ durch Multiplikation mit $\chi(n) \in \mathbb{C}^\times$ operieren soll.

Beweis. Übung. □

Charakter einer induzierten Darstellung?

2.15 Erklärung zur diskreten Fouriertransformation

2.15.1. *Woanders!* Die Terminologie erklärt sich wie folgt: Die stetigen Gruppenhomomorphismen von der Kreislinie $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ in die multiplikative Gruppe $\mathbb{C}^\times$ der komplexen Zahlen sind genau die Abbildungen $z \mapsto z^n$ für $n \in \mathbb{Z}$. Die zugehörigen eindimensionalen Darstellungen $\{L_n\}_{n\in\mathbb{Z}}$ bilden ein Repräsentantensystem für die Isomorphieklassen von irreduziblen stetigen Darstellungen von S^1 in endlichdimensionalen $\mathbb{C}$-Vektorräumen. Die stetigen komplexwertigen Funktionen $\mathcal{C}(S^1)$ auf S^1 kann man verstehen als ein Analogon des Gruppenrings kG, und sie operieren auf jeder stetigen endlichdimensionalen Darstellung V durch die Regel

$$f * v = \int_{S^1} f(z)(\rho_V(z)(v)) \quad \forall f \in \mathcal{C}(S^1), v \in V$$

für das offensichtliche Maß auf S^1 mit Gesamtmasse 1. Auf L_n operiert also $f \in \mathcal{C}(S^1)$ durch Multiplikation mit dem Fourierkoeffizienten $\int_{S^1} f(z)z^n$, und die durch die Operation gegebene Abbildung

$$\mathcal{C}(S^1) \to \prod_{n\in\mathbb{Z}} \mathrm{End}_{\mathbb{C}}\, L_n = \prod_{n\in\mathbb{Z}} \mathbb{C}$$

ordnet demnach einer Funktion $f \in \mathcal{C}(S^1)$ die Familie ihrer Fourierkoeffizienten zu. Das ist die Analogie, die hinter unserer Terminologie steckt. Im Rahmen der nichtkommutativen Analysis kann man sogar in ganz präziser Weise unsere "nichtkommutative" Fouriertransformation, die Entwicklung einer Funktion auf

S^1 in ihre Fourierreihe und die übliche Fouriertransformation von Funktionen auf dem $\mathbb{R}^n$ als Spezialfälle einer sehr allgemeinen "abstrakten Fouriertransformation" begreifen. In der Technik spielt insbesondere die Fouriertransformation für endliche zyklische Gruppen eine Rolle und heißt die **diskrete Fouriertransformation** [MV00].

Kapitel V

Typische Prüfungsfragen

1 Lineare Algebra

1. Was ist ein Körper? Wie leitet man die Regel für das Addieren von Brüchen aus den Körperaxiomen ab?

2. Was ist eine Basis eines Vektorraums? Könnte es passieren, daß ich in demselben Vektorraum eine Basis mit 13 Elementen und eine mit 17 Elementen finde? Was ist die Dimension eines Vektorraums? Hat jeder Vektorraum eine Basis? Was ist überhaupt ein Vektorraum? Wie leitet man $0v = 0$ aus den Vektorraumaxiomen ab?

3. Warum ist jedes unverkürzbare Erzeugendensystem eine Basis? Warum ist jede unverlängerbare linear unabhängige Teilmenge eine Basis?

4. Wie versieht man die Menge der Homomorphismen von einem Vektorraum zu einem anderen mit der Struktur eines Vektorraums? Wie berechnet man die Dimension eines derartigen Raums von Homomorphismen?

5. Was ist die Matrix einer ebenen Drehung um $45°$? Was ist ihre Determinante? Ihre Eigenwerte?

6. Geben Sie eine (3×3)-Matrix vom Rang ... ohne Nullen an. Was ist deren Determinante? Was ist die Lösungsmenge des zugehörigen Gleichungssystems? Was sind die Eigenwerte?

7. Was ist die Determinante einer Matrix? Wie rechnet man sie aus? Warum hat die transponierte Matrix dieselbe Determinante? Warum ist jede Matrix mit von Null verschiedener Determinante invertierbar?

8. Besitzt jede Matrix einen Eigenwert? Ist jede Matrix diagonalisierbar? Beispiel? Gegenbeispiel? Ist jede relle symmetrische Matrix diagonalisierbar? Beweis?

9. Was ist ein Eigenwert einer linearen Abbildung? Welche Eigenwerte hat das Ableiten, aufgefaßt als lineare Abbildung vom Raum der beliebig oft differenzierbaren reellen Funktionen auf der reellen Zahlengeraden $\mathcal{C}^\infty_{\mathbb{R}}(\mathbb{R})$ in sich selbst? Welche Eigenwerte hat das Ableiten aufgefaßt als lineare Abildung vom Raum der Polynome in sich selbst? Was sind die Eigenräume? Und wenn man Koeffizienten in einem Körper der Charakteristik ... nimmt?

10. Wieviele Untervektorräume hat ein ...-dimensionaler Vektorraum über dem Körper mit ... Elementen?

11. Wieviele angeordnete Basen hat ein . . .-dimensionaler Vektorraum über dem Körper mit . . . Elementen?

12. Nimmt die quadratische Form . . . positive und negative Werte an? Wie findet man so etwas im allgemeinen heraus?

13. Berechnen Sie die inverse Matrix zu . . .

14. Was versteht man unter dem Rang einer Matrix? Warum stimmen Zeilenrang und Spaltenrang stets überein?

15. Wie hängen die Eigenwerte einer invertierbaren Matrix zusammen mit den Eigenwerten ihrer Inversen? Wie hängt die Jordan'sche Normalform einer invertierbaren Matrix zusammen mit der Jordan'schen Normalform ihrer Inversen?

2 Algebra

1. Gibt es eine Gruppe mit . . . Elementen? Gibt es eine abelsche Gruppe mit . . . Elementen? Wie konstruiert man überhaupt so eine Restklassengruppe? Was ist das Inverse zu . . . in $\mathbb{Z}/a\mathbb{Z}$? Wieviele paarweise nicht isomorphe abelsche Gruppen gibt es mit . . . Elementen? Welche?

2. Wieviele Gruppenhomomorphismen gibt es von $\mathbb{Z}/4\mathbb{Z}$ nach $\mathbb{Z}/6\mathbb{Z}$?

3. Wieviele Elemente hat $\mathrm{GL}(3;\mathbb{F}_7)$? Wie größ ist die 7-Sylow darin? Können Sie eine 7-Sylow angeben?

4. Hat jedes Polynom eine Nullstelle? Kann man den Grundkörper so vergrößern, daß es eine kriegt? Wie geht das?

5. Ist das Polynom . . . irreduzibel? Was ist ein irreduzibles Polynom? Inwieweit ist die Zerlegung eines Polynoms in irreduzible Faktoren eindeutig? Warum? Welche Grade können irreduzible Polynome in $\mathbb{R}[X]$ haben?

6. Wieviele Nullstellen kann das Polynom . . . höchstens haben? Warum? Gibt es zu vorgegebenen Nullstellen stets ein Polynom, das genau diese Nullstellen hat? Warum-warum nicht?

7. Gibt es einen Körper mit . . . Elementen? Wie zeigt man das? Wann ist $\mathbb{Z}/a\mathbb{Z}$ ein Körper? Warum ist $\mathbb{Z}/10\mathbb{Z}$ kein Körper? Wie rechnet man in diesem Ring? Besitzt . . . darin ein multiplikatives Inverses? Und zwar welches? Welche abelsche Gruppe erhält man als Einheitengruppe? Welche abelsche

Gruppe ist die multiplikative Gruppe des Körpers mit ... Elementen? Welche Kardinalität kann ein endlicher Körper haben? Warum? Sind je zwei Körper mit ... Elementen isomorph? Warum?

8. Was ist die Automorphismengruppe des Körpers mit ... Elementen? Wie zeigt man das?

9. Ist das regelmäßige ...-Eck konstruierbar mit Zirkel und Lineal? Warum oder warum nicht? Welche regelmäßigen n-Ecke sind eigentlich konstruierbar? Warum-warum nicht?

10. Warum hat in einem Körper jedes Element höchstens zwei Quadratwurzeln? Warum in Charakteristik Zwei höchstens eine Quadratwurzel?

11. Kann die reelle Zahl $\sqrt[3]{2}$ Nullstelle eines quadratischen Polynoms mit rationalen Koeffizienten sein?

3 Analysis

1. Wie bestimmt man die Ableitung des Arcustangens? Was ist überhaupt die Ableitung? Was bedeutet darin das Symbol $\varinjlim$? Wie entwickelt man arctg in eine Potenzreihe? Warum ist diese Rechnung erlaubt?...

2. Was ist $\lim_{x\to\infty} \frac{x+\mathrm{e}^x}{\log x+\mathrm{e}^x}$? Was bedeutet $\lim_{x\to\infty} g(x) = b$? Wie ist die Exponentialfunktion definiert? Kennen Sie andere Funktionen, die ihre eigene Ableitung sind? Sind das alle? Warum?

3. Warum ist jede stetige Funktion auf einem kompakten Intervall beschränkt?

4. Berechnen Sie den Schwerpunkt eines Kuchenstücks: Stellen Sie es auf die Spitze und integrieren die Höhe y über das entsprechende Gebiet. Wie lautet allgemein die Formel zur Transformation von Mehrfachintegralen auf krummlinige Koordinaten? Was ist die Beziehung zur Substitutionsregel?

5. Finden Sie eine Stammfunktion für den Arcustangens, $\int \arctan$; wie ist überhaupt das Integral definiert? Warum kann es mittels Stammfunktionen berechnet werden?

6. Was bedeutet $\lim_{n\to\infty} a_n = a$? Schreiben Sie es mit den zugehörigen „für alle“ und „es gibt“ einmal auf. Wie folgt $\lim_{n\to\infty} 1/n = 0$?

7. Wie ist die Exponentialfunktion definiert? Warum konvergiert diese Reihe? Wie zeigt man das Quotientenkriterium? Das Majorantenkriterium?

8. (Falls es dran war) Kennen Sie eine Funktion, die ihre eigene dritte Ableitung ist, $f''' = f$? Können Sie alle derartigen Funktionen $f\colon \mathbb{R} \to \mathbb{C}$ angeben? Können Sie alle derartigen Funktionen $f\colon \mathbb{R} \to \mathbb{R}$ angeben?

9. Wie ist das Integral $\int_a^b f(x)\,\mathrm{d}x$ für $f\colon [a,b] \to \mathbb{R}$ stetig definiert? Welche Probleme können für f unstetig auftreten? Was bedeutet gleichmäßig stetig?

10. Wie ist der Logarithmus definiert? Warum wird jede positive reelle Zahl als Wert der Exponentialfunktion angenommen? Was ist die Ableitung des Logarithmus? Seine Potenzreihenentwicklung? Das Integral? Die Potenzreihenentwicklung um den Punkt $p = 5$? Der Konvergenzradius daselbst?

11. Was ist das höherdimensionale Analogon der Ableitung? Wie hängt das totale Differential mit den partiellen Ableitungen zusammen? Wie lautet in dieser Allgemeinheit die Kettenregel? Wie zeigt man sie?

12. Was ist das Lebesgue-Maß? Wie ist das Lebesgue-Integral definiert? Was ist seine Beziehung zu absoluter Konvergenz von Reihen?

13. Was ist ein Hilbert-Raum?

14. Was ist die Fourier-Transformation?

4 Algebraische Geometrie (Staatsexamen)

1. Zwei Polynome in $\mathbb{C}[X,Y]$ haben dieselben Nullstellen. Sind sie dann gleich? Teilt eins das andere? Und wenn eines irreduzibel ist? Und wenn unsere beiden Polynome nur unendlich viele gemeinsame Nullstellen haben (für die letzte Teilfrage brauche Dimensionstheorie).

2. Kann es sein, daß zwei nichtkonstante Polynome $f, g \in \mathbb{C}[X,Y]$ überhaupt keine gemeinsame Nullstelle haben? Und wenn wir zum projektiven Raum übergehen?

3. Warum bilden die Nullstellenmengen endlicher Familien von Polynomen die abgeschlossenen Mengen einer Topologie auf $\mathbb{C}^n$?

4. Was ist eine reguläre Funktion auf einer affinen Varietät? Sind zwei affine Varietäten bereits isomorph, wenn die $\mathbb{C}$-Kringe ihrer regulären Funktionen isomorph sind? Kann $\mathbb{C}[X]/\langle X^2\rangle$ der Ring der regulären Funktionen auf einer affinen Varietät sein? Welche $\mathbb{C}$-Kringe sind Ringe von regulären Funktionen auf affinen Varietäten?

5. Was ist ein maximales Ideal? Warum ist der Quotient nach einem maximalen Ideal stets ein Körper? Was sind die maximalen Ideale von $\mathbb{C}[X, Y]$?

5 Algebraische Gruppen

1. Was ist eine (affine) algebraische Gruppe? Warum ist jede affine algebraische Gruppe linear?
2. Was sind die algebraischen Gruppenhomomorphismen $(\mathbb{C}, +) \to (\mathbb{C}^\times, \cdot)$?
3. Was sind die irreduziblen algebraischen Darstellungen von $(\mathbb{C}^n, +)$?
4. Welche eindimensionalen algebraischen Gruppen gibt es?
5. Was ist eine Borel'sche Untergruppe?
6. Wie konstruiert man Quotientenvarietäten?
7. Was ist eine diagonalisierbare algebraische Gruppe?
8. Ist eine Gruppe, deren Elemente sämtlich halbeinfach sind, diagonalisierbar? Und wenn sie zusammenhängend ist?
9. Was ist die Jordanzerlegung eines Elements von $\mathbb{Z}/10\mathbb{Z}$, aufgefaßt als algebraische Gruppe über einem Körper der Charakteristik 5?
10. Warum sind je zwei Borel'sche Untergruppen konjugiert?

Literaturverzeichnis

[Art] Emil Artin, *Galois theory*.

[Ben91] D. J. Benson, *Representations and cohomology I: Basic representation theory of finite groups and associative algebras*, Cambridge Studies in Advanced Mathematics, vol. 30, Cambridge University Press, 1991.

[Coh95] P. M. Cohn, *Skew fields*, Encyclopedia of Mathematics and its Applications, vol. 57, Cambridge University Press, Cambridge, 1995, Theory of general division rings.

[E+92] Ebbinghaus et al., *Zahlen*, Springer, 1992.

[FH91] William Fulton and Joe Harris, *Representation theory*, Springer, 1991.

[Gro72] Alexander Grothendieck, *Sga 4*, Lecture Notes in Mathematics, vol. 269, Springer, 1972.

[Jam78] G. D. James, *The representation theory of the symmetric groups*, Lecture Notes in Mathematics, vol. 682, Springer, 1978.

[JK81] Gordon James and Adalbert Kerber, *The representation theory of the symmetric group*, Encyclopedia, vol. 16, Addison-Wesley, 1981.

[JS06] Jens Carsten Jantzen and Joachim Schwermer, *Algebra*, Springer, 2006.

[Lor96] Falko Lorenz, *Einführung in die Algebra I*, Spektrum, 1996.

[LR03] William F. Lawvere and Robert Rosebrugh, *Sets for mathematics*, Cambridge University Press, 2003.

[Mac98] Saunders MacLane, *Categories for the working mathematician*, GTM, vol. 5, Springer, 1998.

[MV00] Meyberg and Vachenauer, *Höhere Mathematik 2*, Springer, 2000.

[Rus05] Lucio Russo, *Die vergessene revolution oder die wiedergeburt des antiken wissens*, Springer, 2005, Übersetzung aus dem Italienischen.

[Sag00] Bruce E. Sagan, *The symmetric group*, Springer, 2000.

[SDAT00] S. A. Katre S. D. Adhikari and Dinesh Thakur, *Cyclotomic fields and related topics*, Bhaskaracharya Pratishthana, Pune, 2000.

[Suz87] Jiro Suzuki, *On coefficients of cyclotomic polynomials*, Proc. Japan Acad. Ser. A Math. Sci. 63 **63** (1987), no. 7, 279–280.

[Wei74] André Weil, *Basic number theory*, Springer, 1974.

Index