Lineare Algebra — WS 2012/13

Sebastian Goette

Inhaltsverzeichnis

Einleitung

Die Lineare Algebra ist die Lehre von Vektorräumen und linearen Abbildungen. Was das ist und warum man sich das anschauen sollte, wird im Laufe der Vorlesung hoffentlich klarer. Jedenfalls werden Ihnen in vielen weiterführenden Vorlesungen immer wieder Vektorräume und lineare Abbildungen begegnen, so dass es sicher sinnvoll ist, sie bereits am Anfang des Studiums kennenzulernen.

Wir beginnen im ersten Kapitel mit einer allgemeinen Einfuehrung, bei der wir Grundlagen und erste Beispiele kennenlernen. Dazu wiederholen wir die Zahlbereiche $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$, die Sie aus der Schule kennen. Dann führen wir die komplexen Zahlen $\mathbb{C}$ und die Quaternionen $\mathbb{H}$ ein. Als ersten Vorgeschmack auf den Inhalt der Vorlesung beschäftigen wir uns mit der Euklidischen Geometrie der Ebene $\mathbb{R}^2$ und des Raumes $\mathbb{R}^3$ und stellen eine Beziehung zu $\mathbb{C}$ beziehungsweise $\mathbb{H}$ her.

Im zweiten Kapitel führen wir systematisch die Grundbegriffe ein. An die Stelle konkreter Zahlbereiche treten Ringe (wie $\mathbb{Z}$), Körper (wie $\mathbb{Q}$, $\mathbb{R}$ oder $\mathbb{C}$) und Schiefkörper (wie $\mathbb{H}$). Die Ebene $\mathbb{R}^2$ und der Raum $\mathbb{R}^3$ sind die einfachsten Beispiele von Vektorräumen. Abbildungen, die mit der Vektorraum-Struktur verträglich sind, heißen linear. Wir werden allgemeiner mit dem Begriff eines Moduls über einem Ring beginnen, und wir werden viele der folgenden Überlegungen für bestimmte Klassen von Moduln durchführen. Beispielsweise lernen wir, wie man Elemente in freien Moduln durch Koordinaten und lineare Abbildungen zwischen solchen Moduln durch Matrizen beschreibt. Wir werden aber immer nur dann allgemeinere Objekte als Vektorräume über Körpern betrachten, wenn das ohne zusätzlichen technischen Aufwand möglich ist.

Im dritten Kapitel konzentrieren wir uns auf Vektorräume über Körpern und Schiefkörpern. Wir zeigen, dass jeder Vektorraum eine Basis besitzt, und dass die Dimension eine Invariante des Vektorraums ist, die ihn bis auf Isomorphie bestimmt. Außerdem betrachten wir die Struktur einer allgemeinen linearen Abbildung und lernen ein universelles Verfahren zum Lösen linearer Gleichungssysteme.

Im vierten Kapitel beschäftigen wir uns mit Endomorphismen freier Moduln über kommutativen Ringen und lernen die Determinante als wichtige Invariante kennen. Anschließend betrachten wir Eigenwerte und das charakteristische Polynom, und lernen erste Strukturaussagen über lineare Abbildungen von einem festen Vektorraum in sich selbst kennen.

KAPITEL 1

Zahlen

In diesem ersten Kapitel legen wir dazu die Grundlagen. Zuerst führen wir Sprechweisen für Mengen, Abbildungen und natürliche Zahlen ein. Danach konstruieren wir ganze und rationale Zahlen, wohingegen wir die reellen Zahlen als gegeben annehmen werden — ihre Konstruktion fällt in den Bereich der Analysis. Aus den reellen Zahlen konstruieren wir die komplexen Zahlen und die Quaternionen. Zum einen sind beides wichtige Beispiele für Körper beziehungsweise Schiefkörper. Auf der anderen Seite besteht ein enger Zusammenhang zur Euklidischen Geometrie in den Dimensionen 2 und 3, und euklidische Geometrie ist sicher einer der wichtigsten Vorläufer für den Vektorraum-Kalkül, um den es in dieser Vorlesung schwerpunktmäßig gehen wird.

1.1. Mengen und Abbildungen

Wenn man möchte, kann man fast die gesamte Mathematik auf das Studium von Mengen und ihren Elementen zurückführen. Das ist aber leider recht mühsam, und man muss sehr sorgfältig sein, um nicht in Widersprüche zu geraten. Wenn Sie wissen möchten, wie das geht, sollten Sie später im Verlauf Ihres Studiums eine Vorlesung über Mengenlehre besuchen. Wir wollen die Mengenlehre als eine Sprache benutzen, in der man sehr elegant über mathematische Sachverhalte sprechen kann. Dazu lernen wir jetzt die ersten Vokabeln und grammatikalischen Regeln.

Georg Cantor hat den Mengenbegriff als erster eingeführt.

„Eine Menge ist eine Zusammenfassung von bestimmten, wohlunterschiedenen Objekten unseres Denkens oder unserer Anschauung zu einem Ganzen.“

1.1. Beispiel. Zahlen sind Objekte unserer Anschauung, also ist $\{1, 2, 3\}$ eine Menge. Die Menge $\mathbb{N} = \{0, 1, 2, \dots\}$ der natürlichen Zahlen lernen wir im Abschnitt 1.2 kennen.

Die „Objekte“ in einer Menge heißen *Elemente*. Wenn ein Objekt a in einer Menge M enthalten ist, schreiben wir

$$a \in M,$$

ansonsten $a \notin M$.

1.2. Definition. Zwei Mengen heißen gleich, wenn sie die gleichen Elemente enthalten.

1.3. Bemerkung. Wenn man Mengen als Aufzählung $M = \{a_1, \ldots, a_n\}$ angibt, kann es passieren, dass $a_i = a_j$ für zwei Indizes i und j. Trotzdem ist a_i dadurch nicht „zweimal“ in M enthalten. Also zum Beispiel

$$\{1, 1, 2\} = \{2, 1\} = \{1, 2\},$$

denn alle drei Mengen enthalten die gleichen Elemente, nämlich 1 und 2. Aber natürlich gilt

$$\{1, 2\} \neq \{1, 2, 3\}.$$

1.4. Beispiel. Besonders wichtig ist die *leere Menge*, die gar kein Element enthält. Wir schreiben

$$\emptyset = \{\,\}.$$

Inzwischen sind auch Mengen „Objekte unseres Denkens oder unserer Anschauung“ geworden. Also kann man auch Mengen betrachten, deren Elemente selbst wieder Mengen sind. In der Tat kann man ausgehend von der leeren Menge bereits sehr viele andere Mengen konstruieren, etwa

$$\emptyset = \{\,\}, \qquad \{\emptyset\}, \qquad \{\{\emptyset\}, \emptyset\} \qquad \text{usw.}\ldots,$$

genug, um alle Objekte dieser Vorlesung zu beschreiben.

Wir stoßen jetzt auf das erste Problem mit Cantors Mengenbegriff.

1.5. Satz (Russellsche Antinomie)**.** *Es gibt keine Menge M, deren Elemente genau diejenigen Mengen sind, die sich nicht selbst enthalten.*

Wir formulieren die Russellsche Antinomie hier wie selbstverständlich als einen *Satz*, also als eine bewiesene mathematische Aussage. Zu ihrer Zeit war die Russellsche Antinomie ein Widerspruch im mathematischen Denkgebäude — so etwas darf es nicht geben, denn aus einem Widerspruch lässt sich alles folgern, man könnte als Mathematiker nicht mehr zwischen „richtig“ und „falsch“ unterscheiden, und dadurch würde Mathematik als Ganzes bedeutungslos. Man hat einige Zeit gebraucht, um eine handhabbare Version der Mengenlehre zu formulieren, in der aus dem fatalen Widerspruch ein harmloser Satz wird.

Beweis. Würde es eine solche Menge M geben, dann müsste entweder $M \in M$ oder $M \notin M$ gelten. Aber nach Definition von M gilt $M \in M$ genau dann, wenn $M \notin M$, und das ist ein Widerspruch. Also gibt es keine Menge M. □

1.6. Bemerkung. Wir haben gerade unseren ersten *indirekten Beweis* kennengelernt. Bei einem indirekten Beweis nimmt man an, dass die Aussage, die man beweisen möchte, falsch ist, und leitet daraus einen Widerspruch her. Manchmal ist das die einfachste Weise, einen Satz zu beweisen. Der Nachteil ist aber, dass man — wie im obigen Beweis — nicht auf Anhieb versteht, warum der Satz gilt. Wenn möglich, wollen wir daher indirekte Beweise vermeiden.

Zurück zu Cantors Mengenbegriff und zur Russellschen Antinomie. Wir sehen, dass nicht jede „Zusammenfassung von Objekten unseres Denkens und unserer Anschauung“ eine Menge sein kann. Wir werden daher die Existenz einiger nützlicher Mengen annehmen, und wir werden einige Konstruktionen

angeben, die neue Mengen aus alten erzeugen. Die gesamte Mathematik basiert auf der Annahme, dass man das ohne Widersprüche machen kann — aber aus prinzipiellen Gründen lässt sich die Widerspruchsfreiheit der Axiome der Mengenlehre nicht beweisen.

1.7. Definition. Seien M und N Mengen, dann heißt M eine *Teilmenge* von N, wenn alle Elemente a von M auch in N enthalten sind. Dafür schreiben wir

$$M \subset N\ .$$

1.8. Bemerkung.
(1) Die leere Menge ist Teilmenge jeder Menge M.
(2) Es gilt $\{x\} \subset M$ genau dann, wenn $x \in M$.
(3) Es gilt immer $M \subset M$.
(4) Wenn $M \subset N$ und $M \neq N$ gilt, heißt M auch *echte Teilmenge* von N.

In den meisten Mathebüchern wird das Symbol „$\subset$“ so verwendet wie hier. Es gibt zwar eine internationale Norm, nach der nur echte Teilmengen mit „$\subset$“ bezeichnet werden sollen, aber in der Mathematik benötigt man das Symbol für beliebige Teilmengen weitaus häufiger, und schreibt daher „$\subset$“. Für echte Teilmengen verwenden wir das Symbol „$\subsetneq$“. Falls Sie ein Mathebuch zur Hand nehmen, in dem das Symbol „$\subset$“ vorkommt, sollten Sie zur Sicherheit trotzdem herausfinden, ob der Autor damit beliebige oder nur echte Teilmengen bezeichnet. Genauso vorsichtig sollten Sie eigentlich mit allen Definitionen und Bezeichnungen verfahren.

Kommen wir jetzt zur Konstruktion neuer Mengen aus alten.

1.9. Definition. Seien M und N Mengen.

(1) Der *Durchschnitt* $M \cap N$ enthält genau die Elemente, die sowohl in M als auch in N enthalten sind.
(2) Die *Vereinigung* $M \cup N$ enthält genau die Elemente, die in M oder in N enthalten sind.
(3) Wenn $M \cap N = \emptyset$ gilt, heissen M und N *disjunkt*, und $M \cup N$ ist eine *disjunkte Vereinigung*. Um zu zeigen, dass eine Vereinigung disjunkt ist, schreiben wir $M \dot\cup N$.
(4) Die (*Mengen-*) *Differenz* $N \setminus M$ enthält genau die Elemente, die in N, aber nicht in M enthalten sind. Ist M Teilmenge von N, so nennt man $N \setminus M$ auch das *Komplement* von M in N.
(5) Das *kartesische Produkt* $M \times N$ besteht aus allen Paaren (x, y) von Elementen $x \in M$ und $y \in N$. Für das Produkt einer Menge M mit sich selbst schreibt man auch $M^2 = M \times M$.

Insbesondere sind $M \cap N$, $M \cup N$, $N \setminus M$ und $M \times N$ auch wieder Mengen.Für den Anfang reichen uns diese Konstruktionen. Später werden wir Vereinigungen und Durchschnitte beliebig vieler Mengen benötigen.

1.10. Bemerkung. Die Notation (x, y) bezeichnet ein (geordnetes) *Paar*, allgemeiner bezeichnet $(x_1, \ldots, x_n)$ ein *n-Tupel*. Hierbei kommt es auf die Reihenfolge der Einträge (nicht „Elemente“!) an, und ein und derselbe Eintrag kann

mehrfach auftreten. Zum Beispiel:

$$(1,1) \in \{1,2\} \times \{1,2,3\}$$

und

$$(1,2) \neq (2,1) \neq (2,1,1).$$

1.11. Definition. Die Menge aller Teilmengen von M heißt *Potenzmenge* $\mathcal{P}(M)$. Auch die Potenzmenge einer Menge ist wieder eine Menge.

1.12. Beispiel. Sei $M = \{1,2\}$, dann gilt

$$\mathcal{P}(M) = \big\{\emptyset, \{1\}, \{2\}, \{1,2\}\big\}.$$

Es sei M eine Menge. Man betrachtet oft die Teilmenge aller Elemente z von M, die eine bestimmte Eigenschaft E haben, und schreibt dafür

$$\{z \in M \mid z \text{ hat die Eigenschaft } E\}.$$

Wenn E eine mathematisch wohldefinierte Eigenschaft ist, dann erhalten wir wieder eine Menge.

1.13. Folgerung (aus der Russellschen Antinomie 1.5)**.** *Die Gesamtheit aller Mengen ist keine Menge.*

Beweis. Wäre die Gesamtheit aller Mengen selbst eine Menge N, dann wäre auch

$$M = \{X \in N \mid X \notin X\}$$

wieder eine Menge, was nach Satz 1.5 aber nicht sein kann. □

1.14. Definition. Es seien M und N Mengen. Eine *Abbildung* $F\colon M \to N$ (lies „F von M nach N“) ordnet jedem Element $x \in M$ ein Element $F(x) \in N$ zu.

Formal fassen wir F als Tripel $(M, N, \Gamma(F))$ auf. Hierbei ist $\Gamma(F) \subset M \times N$ der *Graph* von F. Wir fordern, dass zu jedem $x \in M$ genau ein $y \in N$ mit $(x,y) \in \Gamma(F)$ existiert, und setzen $F(x) = y$.

1.15. Definition. Es sei $F\colon M \to N$ eine Abbildung. Dann heißt M der *Definitionsbereich* von M und N der *Wertebereich*. Die Menge aller Abbildungen von M nach N wird mit $\mathrm{Abb}(M,N)$ bezeichnet .

Zwei Abbildungen sind gleich, wenn sie den gleichen Definitions- und den gleichen Wertebereich haben, und jedem Element des Definitionsbereichs jeweils dasselbe Element des Bildbereichs zuordnen.

1.16. Definition. Es sei $F\colon M \to N$ eine Abbildung. Dann heißt die Teilmenge

$$\operatorname{im} F = \{\, y \in N \mid \text{ Es gibt } x \in M \text{ mit } F(x) = y \,\} = \{\, F(x) \mid x \in M \,\}$$

das *Bild* von F.

Sei $V \subset N$ eine Teilmenge, dann heißt

$$F^{-1}(V) = \{x \in M \mid F(x) \in V\}$$

das *Urbild* von V unter F.

Für das Urbild der einelementigen Menge $\{y\}$ schreibt man manchmal kurz $F^{-1}(y)$ statt $F^{-1}(\{y\})$. Da das zu Missverständnissen führen kann, bleiben wir erst einmal bei $F^{-1}(\{y\})$.

1.17. Definition. Eine Abbildung $F\colon M \to N$ heißt

(1) *injektiv*, wenn für alle $x_1, x_2 \in M$ aus $F(x_1) = F(x_2)$ schon $x_1 = x_2$ folgt,
(2) *surjektiv*, wenn für alle $y \in N$ ein $x \in M$ existiert mit $F(x) = y$, und
(3) *bijektiv*, wenn sie injektiv und surjektiv ist.

1.18. Beispiel.
(1) Für alle Mengen M ist die Abbildung $\mathrm{id}_M\colon M \to M$ mit $\mathrm{id}_M(x) = x$ definiert. Sie heißt die *Identität* und ist stets bijektiv.
(2) Die Abbildung $F\colon \mathbb{R} \to \mathbb{R}$ mit $F(x) = x^2$ ist weder injektiv noch surjektiv, denn
$$F(-2) = F(2) = 4 \qquad \text{und} \qquad -1 \notin \mathrm{im}\,(F).$$
(3) Die Abbildung $F\colon \mathbb{N} \to \mathbb{N}$ mit $F(x) = x^2$ ist injektiv. Die Abbildung $G\colon \mathbb{N} \to \{\, x^2 \mid x \in \mathbb{N} \,\}$ mit $G(x) = x^2$ ist bijektiv. Diese Abbildungen sind verschieden, da sie andere Wertebereiche haben.

Trotzdem werden wir später manchmal beide Abbildungen mit dem gleichen Symbol bezeichnen.

1.19. Definition. Seien L, M, N Mengen und $F\colon M \to N$, $G\colon L \to M$ Abbildungen. Die *Verkettung* $F \circ G\colon L \to N$ (lies „F nach G“) ist die durch
$$(F \circ G)(x) = F(G(x))$$
definierte Abbildung.

1.20. Bemerkung. Die Buchstaben in „$F \circ G$“ scheinen „falsch herum“ zu stehen, denn die Abbildungen verlaufen von links nach rechts geschrieben so:
$$\begin{array}{ccccc} L & \xrightarrow{G} & M & \xrightarrow{F} & N \\ x & \longmapsto & G(x) & \longrightarrow & F(G(x))\,. \end{array}$$
Aber in „$(F \circ G)(x) = F(G(x))$“ stimmt die Reihenfolge wieder. Beispielsweise seien $F, G\colon \mathbb{R} \to \mathbb{R}$ definiert durch
$$F(x) = x^2 \qquad \text{und} \qquad G(x) = x + 1\,,$$
dann ist
$$(F \circ G)(x) = (x+1)^2 \quad \text{und} \quad (G \circ F) = x^2 + 1\,.$$
Insbesondere gilt $G \circ F \neq F \circ G$.

1.21. Bemerkung. Sei $F\colon M \to N$ eine Abbildung, und sei $U \subset M$ eine Teilmenge. Die Abbildung $G\colon U \to M$ mit $G(x) = x$ für alle $x \in U$ heißt *Inklusion*. Sie ist stets injektiv. Die Verkettung
$$F|_U = F \circ G\colon U \to N$$
(lies „F eingeschränkt auf U“) heißt *Einschränkung* von F auf U.

1.22. Satz. *Seien L, M, N Mengen und $F, F' \colon M \to N$, $G, G' \colon L \to M$ Abbildungen. Dann gilt*

(1) *Sind F, G injektiv, so ist auch $F \circ G$ injektiv.*
(2) *Sind F, G surjektiv, so ist auch $F \circ G$ surjektiv.*
(3) *Sind F, G bijektiv, so ist auch $F \circ G$ bijektiv.*
(4) *Ist $F \circ G$ injektiv, so auch G.*
(5) *Ist $F \circ G$ surjektiv, so auch F.*
(6) *Ist F injektiv, so folgt aus $F \circ G = F \circ G'$ bereits $G = G'$.*
(7) *Ist G surjektiv, so folgt aus $F \circ G = F' \circ G$ bereits $F = F'$.*

Hierbei bezeichnen F' und G' beliebige Abbildungen und nicht die „Ableitungen“ von F und G.

Beweis. Zu (1) seien $x, y \in L$. Aus $(F \circ G)(x) = (F \circ G)(y)$ folgt $F(G(x)) = F(G(y))$, also $G(x) = G(y)$ wegen Injektivität von F, also $x = y$ wegen Injektivität von G, also ist $F \circ G$ ebenfalls injektiv. Der Beweis von (2) verläuft ähnlich wie (1), und (3) folgt sofort aus (1) und (2).

Die Punkte (4), (5) sind Übungsaufgaben zur Vorlesung “Analysis I” und werden hier daher nicht bewiesen.

Aussage (6) folgt ähnlich wie (7). Zu (7) sei $y \in M$. Wegen Surjektivität von G existiert $x \in L$ mit $G(x) = y$. Aus $F \circ G = F' \circ G$ folgt

$$F(y) = (F \circ G)(x) = (F' \circ G)(x) = F'(y).$$

Da das für alle $y \in M$ gilt, folgt $F = F'$. □

1.23. Satz. *Sei $F \colon M \to N$ bijektiv. Dann existiert genau eine Abbildung $G \colon N \to M$ mit $G \circ F = \mathrm{id}_M$ und $F \circ G = \mathrm{id}_N$.*

1.24. Definition. Die Abbildung G aus Satz 1.23 heißt die *Umkehrabbildung* von F.

Die Umkehrabbildung von F wird manchmal mit F^{-1} bezeichnet. Auch das kann zu Missverständnissen führen, so dass wir auf diese Bezeichnung verzichten wollen.

Beweis von Satz 1.23. Wir müssen zeigen, dass G *existiert*, und dass G *eindeutig* ist.

Zur Eindeutigkeit nehmen wir an, dass $G \colon N \to M$ eine Umkehrfunktion ist. Dann sei $y \in N$ beliebig, und sei $x \in M$ das eindeutige Element mit $F(x) = y$. Aus $G \circ F = \mathrm{id}_M$ folgt

$$G(y) = G(F(x)) = x \ .$$

Wenn eine Umkehrfunktion existiert, sind ihre Werte durch diese Gleichung eindeutig bestimmt. Also ist die Umkehrfunktion eindeutig.

Zur Existenz sei $\Gamma(F)$ der Graph von F. Gemäß der obigen Überlegung betrachten wir

$$X = \left\{ (y, x) \in N \times M \;\middle|\; (x, y) \in \Gamma(F) \right\},$$

das ist eine Menge, da M, N und $\Gamma(F)$ auch Mengen sind. Zu jedem $y \in N$ existiert genau ein $x \in M$ mit $F(x) = y$, also mit $(x, y) \in \Gamma(F)$, also auch mit $(y, x) \in X$. Also ist X der Graph einer Funktion $G\colon N \to M$.

Für alle $x \in M$ ist $(F(x), x) \in X = \Gamma(G)$, also $G(F(x)) = x$, und somit $G \circ F = \mathrm{id}_M$. Umgekehrt sei $y \in N$, und sei $x \in M$ das eindeutige Element mit $F(x) = y$, also $G(y) = x$ und $F(G(y)) = F(x) = y$. Somit gilt auch $F \circ G = \mathrm{id}_N$. Also existiert eine Umkehrfunktion, nämlich G. □

1.25. Definition. Zwei Mengen M und N heissen *gleichmächtig*, wenn es eine bijektive Abbildung $F\colon M \to N$ gibt.

1.26. Bemerkung. Gleichmächtige Mengen haben „gleich viele“ Elemente. Für alle Mengen L, M und N gilt (Übung):

(1) M ist gleichmächtig zu M;
(2) N ist genau dann gleichmächtig zu M, wenn M zu N gleichmächtig ist;
(3) sind L zu M und M zu N gleichmächtig, so ist auch L zu N gleichmächtig.

Das heißt, Gleichmächtigkeit verhält sich wie eine Äquivalenzrelation. Allerdings sollte eine Relation immer auf einer Menge definiert sein, und die Menge aller Mengen gibt es nach Folgerung 1.13 nicht.

1.27. Beispiel.
(1) Die Mengen $M = \{1, 2, 3\}$ und $N = \{4, 7, 15\}$ sind gleichmächtig. Definiere z.B. $F\colon M \to N$ durch
$$F(1) = 7, \quad F(2) = 4, \quad F(3) = 15.$$
(2) Sei $M = \{n^2 \mid n \in \mathbb{N}\} \subset \mathbb{N}$ die Menge der Quadratzahlen. Da $F\colon \mathbb{N} \to M$ mit $F(n) = n^2$ bijektiv ist, sind M und $\mathbb{N}$ gleichmächtig, obwohl M eine echte Teilmenge von $\mathbb{N}$ ist.

1.2. Natürliche Zahlen

Die natürlichen Zahlen sind uns bereits seit unserer Kindheit vertraut — wir benutzen sie zum Zählen. Für den Fall, dass es nichts zu zählen gibt, haben wir die Zahl 0. Es ist erstaunlich, dass die Zahl 0 selbst erst spät als eigenständige Zahl eingeführt wurde. Wenn wir schon ein Stück weit gezählt haben, etwa bis zu einer Zahl n, und weiterzählen wollen, brauchen wir die nächste Zahl. Wir nennen Sie den Nachfolger von n und schreiben $n + 1$. Schließlich wollen wir, dass die natürlichen Zahlen eine Menge bilden, die sonst keine weiteren Objekte enthält.

1.28. Annahme (Peano-Axiome)**.** *Wir nehmen an, dass es eine Menge* $\mathbb{N}$ *mit einem ausgezeichneten Element* $0 \in \mathbb{N}$ *und einer Abbildung* $+1\colon \mathbb{N} \to \mathbb{N}$ *gibt, die die folgenden* Peano-Axiome *erfüllt:*

(1) *Die Nachfolger-Abbildung ist bijektiv als Abbildung* $+1\colon \mathbb{N} \to \mathbb{N} \setminus \{0\}$.

(2) *Sei $M \subset N$ eine Teilmenge mit $0 \in M$, so dass für alle $m \in M$ auch $m + 1 \in M$ gilt, dann ist bereits $M = N$.*

Axiom (1) besagt, dass jede Zahl genau einen Nachfolger hat, und jede Zahl außer 0 selbst Nachfolger genau einer anderen Zahl ist. Axiom (2) besagt, dass die Menge N die "kleinste" Menge ist, die (1) erfüllt. Trotzdem bestimmen die Peano-Axiome die natürlichen Zahlen nicht eindeutig — warum das so ist, lernen Sie aber erst in einer Vorlesung über Logik. Wir wollen immerhin annehmen, dass $\mathbb{N}$ nur die Zahlen 0, 1, 2, ... enthält, aber keine weiteren Elemente. Übrigens gibt es Autoren, für die $0 \notin \mathbb{N}$. Zur Sicherheit können Sie beide Versionen mit $\mathbb{N}_0$ und $\mathbb{N}_>$ bezeichnen.

1.29. Bemerkung. Wir können natürliche Zahlen als Mengen $\underline{0}, \underline{1}, \underline{2}, \ldots$ konstruieren. Dazu setzen wir $\underline{0} = \emptyset$ und konstruieren Nachfolger als

$$\underline{n} + 1 = \underline{n+1} = \{\underline{0}, \ldots, \underline{n}\} = \underline{n} \cup \{\underline{n}\}.$$

Diese Definition ist *rekursiv*, das heißt, man muss alle Zahlen bis $\underline{n}$ kennen, um den Nachfolger $\underline{n+1}$ zu konstruieren. Wir schreiben $\underline{\mathbb{N}} = \{\underline{0}, \underline{1}, \underline{2}, \ldots\}$.

Die ersten „Zahlen" sehen so aus:

$$\begin{aligned} \underline{0} &= \emptyset \\ \underline{1} &= \{\underline{0}\} = \{\emptyset\} \\ \underline{2} &= \{\underline{0}, \underline{1}\} = \{\emptyset, \{\emptyset\}\} \\ \underline{3} &= \{\underline{0}, \underline{1}, \underline{2}\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \end{aligned}$$

Auf diese Weise erhalten wir alle Zahlen mit elementaren Konstruktionen aus der leeren Menge. Da das recht mühselig ist, werden wir natürliche Zahlen meistens als Zahlen und nicht als Mengen betrachten. Nur in diesem Abschnitt werden wir die obigen Mengen manchmal benutzen.

1.30. Definition. Eine Menge M heißt *endlich*, wenn sie zu einer Menge $\underline{n}$ gleichmächtig ist. In diesem Fall heißt die Zahl n die *Mächtigkeit* von M, geschrieben $n = \#M$. Ansonsten heißt M *unendlich*.

1.31. Bemerkung.

(1) Man kann sich überlegen, dass zwei Mengen $\underline{n}$ und $\underline{m}$ genau dann gleichmächtig sind, wenn $\underline{n} = \underline{m}$. Wegen Bemerkung 1.26 kann jede Menge M zu höchstens einer Menge $\underline{n}$ gleichmächtig sein. Die Schreibweise $\#M$ für endliche Mengen ist also sinnvoll.

(2) Endliche Mengen kann man immer als Aufzählung angeben. Sei etwa $F\colon \underline{n} \to M$ bijektiv, dann schreibe

$$M = \{F(0), \ldots, F(n-1)\}$$

Ist M umgekehrt als $\{x_1, \ldots, x_n\}$ gegeben, dann hat M höchstens n Elemente, ist also endlich.

(3) Für unendliche Mengen M führen wir die Schreibweise „$\#M = \infty$" nicht ein, da nicht alle unendlichen Mengen gleichmächtig sind.

1.32. Definition. Es seien $m, n \in \mathbb{N}$, dann gilt m *kleiner oder gleich* n, kurz $m \leq n$, genau dann, wenn $\underline{m} \subset \underline{n}$. Es ist m *kleiner* als n, kurz $m < n$, wenn $m \leq n$ und $m \neq n$ gilt.

1.33. Bemerkung. Aus Bemerkung 1.29 folgt auch, dass $m < n$ genau dann gilt, wenn $\underline{m} \in \underline{n}$. Man beachte den Unterschied in der Notation. Bei „$\subset$“ ist Gleichheit erlaubt, bei „$<$“ jedoch ausgeschlossen.

Der Vergleich von Zahlen führt uns auf den Begriff der Ordnung. Eine Ordnung einer Menge M ist eine *Relation*, das heißt, eine Teilmenge $R \subset M \times M$, die einige zusätzliche Eigenschaften besitzt. Wir sagen „es gilt xRy“ für $x, y \in M$, wenn $(x, y) \in R$.

1.34. Definition. Eine Relation R auf eine Menge M heißt *Halbordnung*, wenn für alle $x, y, z \in M$ gilt:

(O1) xRx (*Reflexivität*),

(O2) xRy und $yRx \implies x = y$ (*Antisymmetrie*),

(O3) xRy und $yRz \implies xRz$ (*Transitivität*).

Eine Halbordnung heißt *Ordnung*, wenn ausserdem für alle $x, y \in M$ gilt:

(O4) xRy oder yRx (*Totalität*).

Die Eigenschaften (1)–(4) heißen auch *Ordnungsaxiome.*

1.35. Beispiel.

(1) Sei M eine Menge, dann definiert „$\subset$“ eine Halbordnung auf der Potenzmenge $\mathcal{P}(M)$.

(2) Die Relation „$\in$“ ist nicht transitiv und daher keine Halbordnung, denn es gilt zum Beispiel $a \in \{a, b\}$ und $\{a, b\} \in \{\{a\}, \{a, b\}\}$, aber nicht $a \in \{\{a\}, \{a, b\}\}$.

(3) Die Relation „$\leq$“ auf $\mathbb{N}$ ist eine Ordnung, denn für alle $\ell, m, n \in \mathbb{N}$ gilt

$$n \leq n,$$
$$m \leq n \text{ und } n \leq m \implies m = n,$$
$$\ell \leq m \text{ und } m \leq n \implies \ell \leq n,$$
$$m \leq n \text{ oder } n \leq m.$$

Auch hier lassen wir den Beweis aus.

(4) Sei M eine Menge. Die Relation „hat höchstens so viele Elemente wie“ ist keine Ordnung auf der Potenzmenge $\mathcal{P}(M)$, denn sei $M = \{1, 2, 3\}$, dann hat $\{1, 2\}$ höchstens so viele Elemente wie $\{2, 3\}$ und umgekehrt, aber beide Mengen sind nicht gleich. Also ist die Antisymmetrie verletzt.

Das zweite Peano-Axiom 1.28 (2) führt uns zur Beweismethode durch vollständige Induktion.

1.36. Satz (Prinzip der *vollständigen Induktion*)**.** *Für jedes $n \in \mathbb{N}$ sei $A(n)$ eine Aussage. Wenn gilt*

(1) $A(0)$ *ist wahr, und*
(2) *aus* $A(n)$ *folgt* $A(n+1)$ *für alle* $n \in \mathbb{N}$,

dann ist $A(n)$ *für alle* $n \in \mathbb{N}$ *wahr.*

Beweis. Betrachte

$$M = \{\, n \in \mathbb{N} \mid \text{die Aussage } A(n) \text{ ist wahr} \,\}.$$

Nach unseren Annahmen in Abschnitt 1.1 ist das wieder eine Menge, also $M \subset \mathbb{N}$. Aus den Voraussetzungen folgt

(1) $0 \in M$, und
(2) für alle $n \in M$ gilt $n+1 \in M$.

Aus dem Axiom 1.28 (2) folgt dann $M = \mathbb{N}$. Nach Definition von M gilt $A(n)$ also für alle $n \in \mathbb{N}$. □

Eine andere Art der vollständigen Induktion funktioniert so: Wenn gilt

(1) $A(0)$ ist wahr, und
(2) aus $A(0) \wedge \cdots \wedge A(n)$ folgt $A(n+1)$ für alle $n \in \mathbb{N}$,

dann gilt $A(n)$ für alle $n \in \mathbb{N}$. Das zeigt man, indem man die Aussage

$$B(n) = A(0) \wedge \cdots \wedge A(n)$$

induktiv mit Satz 1.36 beweist.

Beispiele für diese Beweistechnik finden Sie im Analysis-Skript.

Wir haben in Bemerkung 1.29 Zahlen als Mengen rekursiv eingeführt. *Rekursive Definitionen* funktionieren ähnlich wie vollständige Induktion: um eine Abbildung F von $\mathbb{N}$ in eine Menge M anzugeben, reicht es $F(0) \in M$ festzulegen und eine Vorschrift anzugeben, die $F(n+1)$ aus $F(0), \ldots, F(n)$ bestimmt.

Wir führen jetzt die Grundrechenarten auf $\mathbb{N}$ rekursiv ein. Hierbei handelt es sich um *Verknüpfungen*, das heißt, um Abbildungen $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, etwa

$$+ \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N} \quad \text{mit} \quad +(m,n) = m+n.$$

1.37. Definition. Die *Addition, Multiplikation* und *Potenzierung* sind für m, $n \in \mathbb{N}$ definiert durch

(1) $m + 0 = m$ und $m + (n+1) = (m+n) + 1$,
(2) $m \cdot 0 = 0$ und $m \cdot (n+1) = m \cdot n + m$,
(3) $m^0 = 1$ und $m^{(n+1)} = m^n \cdot m$.

Beispiel. Zwei einfache Rechnungen:

$$3 + 2 = (3+1) + 1 = ((3+0)+1) + 1 = (3+1) + 1 = 4 + 1 = 5 \,,$$
$$3 \cdot 2 = (3 \cdot 1) + 3 = ((3 \cdot 0) + 3) + 3 = \cdots = 6 \,.$$

1.38. Proposition. *Seien* M, N *endliche Mengen.*

(1) *Falls* $M \cap N = \emptyset$ *ist, gilt* $\#(M \dot\cup N) = \#M + \#N$.
(2) *Es gilt* $\#(M \times N) = \#M \cdot \#N$.
(3) *Es gilt* $\#\mathrm{Abb}(N, M) = \#M^{\#N}$.

BEWEIS. Wir beweisen (1) zur Illustration durch vollständige Induktion über die Mächtigkeit $n = \#N$. Es sei $m = \#M$.

Induktionsanfang: Es sei $n = 0$. Nach den Definitionen 1.25 und 1.30 existiert eine bijektive Abbildung von $\emptyset = \underline{0}$ nach N, also gilt $N = \emptyset$. Somit

$$\#(M \dot\cup N) = \#(M \dot\cup \emptyset) = \#M = m = m + 0 = \#M + \#N \ .$$

Induktionsschritt: Es sei $\#N = n + 1$. Dann existiert eine bijektive Abbildung $F\colon \underline{n+1} = \underline{n} \dot\cup \{\underline{n}\} \to N$. Setze

$$N' = \mathrm{im}(F|_{\underline{n}}) = \{F(\underline{0}), \dots, F(\underline{n-1})\} \qquad \text{und} \qquad x = F(\underline{n}) \ ,$$

so dass $\#N' = n$. Nach Induktionsvoraussetzung gilt $\#(M \dot\cup N') = m + n$, also existiert eine bijektive Abbildung $G'\colon \underline{m+n} \to M \dot\cup N'$. Wir definieren $G\colon \underline{(m+n)+1} \to M \dot\cup N$ durch

$$G(\underline{k}) = \begin{cases} G'(\underline{k}) & \text{falls } \underline{k} \in \underline{m+n}, \text{ also } k < m+n, \text{ und} \\ x & \text{falls } \underline{k} = \underline{m+n}, \text{ also } k = m+n. \end{cases}$$

Man überzeugt sich leicht, dass G bijektiv ist. Mit Definition 1.37 (1) folgt

$$\#(M \dot\cup N) = (m+n)+1 = m + (n+1) = \#M + \#N \ . \qquad \square$$

1.39. Bemerkung. Die Grundrechenarten hätten wir auch über die Eigenschaften (1)–(3) definieren können. Außerdem folgt aus (1), dass $m \le \ell$ genau dann gilt, wenn ein $n \in \mathbb{N}$ mit $m + n = \ell$ existiert.

Bevor wir das Assoziativgesetz kennenlernen, überlegen wir uns, was „Klammern“ eigentlich bewirken. Fassen wir $+\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ als Abbildung auf, dann bedeutet $(\ell + m) + n$ gerade $+(+(\ell, m), n)$, $\ell + (m + n)$ bedeutet $+(\ell, +(m, n))$.

1.40. Satz. *Für* $\ell, m, n \in \mathbb{N}$ *gelten die Rechenregeln*

(1) Assoziativgesetze
$$(\ell + m) + n = \ell + (m + n)$$
$$(\ell \cdot m) \cdot n = \ell \cdot (m \cdot n)$$
(2) Neutrale Elemente
$$n + 0 = n$$
$$n \cdot 1 = n$$
(3) Kommutativgesetze
$$n + m = m + n$$
$$n \cdot m = m \cdot n$$

(4) Distributivgesetz

$$\ell \cdot (m+n) = \ell \cdot m + \ell \cdot n$$

(5) Kürzungsregeln

$$\begin{aligned} \ell + n = m + n \quad &\Longrightarrow \quad \ell = m \\ \ell \cdot n = m \cdot n \quad &\Longrightarrow \quad \ell = m \text{ oder } n = 0\,. \end{aligned}$$

Beweis. Die Aussagen (2) folgen leicht aus Definition 1.37. Alle anderen lassen sich durch vollständige Induktion beweisen. Der Beweis von (5) ist Übung. □

1.3. Ganze und Rationale Zahlen

In diesem Abschnitt „lösen“ wir zwei Probleme: man kann in $\mathbb{N}$ nicht subtrahieren, und man kann in $\mathbb{N}$ auch nicht durch Zahlen $n \neq 0$ dividieren. Um diese „Grundrechenarten“ einführen zu können, werden wir $\mathbb{N}$ erst zu den ganzen Zahlen $\mathbb{Z}$, und dann zu den rationalen Zahlen $\mathbb{Q}$ erweitern. Dazu ist zunächst etwas Vorarbeit nötig. Wir erinnern uns an die Definition 1.34 einer Halbordung.

1.41. Definition. Eine Relation R auf einer Menge M heißt *Äquivalenzrelation*, wenn für alle x, y, z gilt:

(Ä1)	xRx			(*Reflexivität*),
(Ä2)	xRy	$\Longrightarrow$	yRx	(*Symmetrie*),
(Ä3)	xRy und yRz	$\Longrightarrow$	xRz	(*Transitivität*).

Im Unterschied zu Halbordnungen sind Äquivalenzrelationen symmetrisch und nicht antisymmetrisch. Das erlaubt uns, Äquivalenzklassen und Quotientenmengen zu definieren. Wir erinnern uns an die Potenzmenge $\mathcal{P}(M)$ von M aus Definition 1.11.

1.42. Definition. Es sei R eine Äquivalenzrelation auf M. Für alle $x \in M$ definieren wir die *Äquivalenzklasse* $[x]$ von x als

$$[x] = \left\{\, y \in M \;\middle|\; xRy \,\right\}.$$

Die Gesamtheit aller Äquivalenzklassen bildet die *Quotientenmenge* (kurz: den *Quotienten*) M/R, also

$$M/R = \left\{\, [x] \;\middle|\; x \in M \,\right\} = \left\{\, N \in \mathcal{P}(M) \;\middle|\; \text{es gibt ein } x \in M \text{ mit } N = [x] \,\right\},$$

und alle Elemente $y \in [x]$ heißen *Repräsentanten* von $[x] \in M/R$. Die Abbildung $p\colon M \to M/R$ mit $p(x) = [x]$ heißt *Quotientenabbildung*.

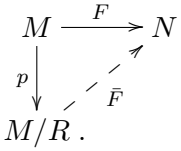
Das einfachste Beispiel für eine Äquivalenzrelation ist die Gleichheit „=“ auf einer beliebigen Menge M. Die Axiome (Ä1)–(Ä3) gelten offensichtlich. In diesem Fall ist die Äquivalenzklasse von $x \in M$ gerade $[x] = \{x\}$, und die Quotientenabbildung $p\colon M \to M/=$ ist bijektiv mit $x \mapsto \{x\}$. Allerdings gilt strenggenommen nicht $M = M/=$, zum Beispiel ist

$$\{1,2,3\}/= \;= \{\{1\},\{2\},\{3\}\}\,.$$

1.43. Proposition. *Es sei R eine Äquivalenzrelation auf M.*

(1) *Für alle $x \in M$ und alle $y \in [x]$ gilt $[x] = [y]$, insbesondere liegt jedes $x \in M$ in genau einer Äquivalenzklasse von R.*
(2) *Die Abbildung $p\colon M \to M/R$ ist surjektiv, und es gilt $p(x) = p(y)$ genau dann, wenn xRy gilt.*
(3) *Es sei $F\colon M \to N$ eine Abbildung. Dann existiert genau dann eine Abbildung $\bar{F}\colon M/R \to N$ mit $F = \bar{F} \circ p$, wenn für alle x, $y \in M$ aus xRy folgt, dass $F(x) = F(y)$. In diesem Fall ist $\bar{F}$ eindeutig.*

Die Aussage (3) heißt auch die *universelle Eigenschaft des Quotienten.* Wir nennen $\bar{F}$ die *von F induzierte Abbildung.* Wir stellen (3) als Diagramm dar:



Beweis. Zu (1) seien $y \in [x]$ und $z \in [y]$ beliebig, dann gilt xRy und yRz. Aus Transitivität folgt xRz, also gilt $z \in [x]$ für alle $z \in [y]$, es folgt $[y] \subset [x]$.

Aus xRy folgt yRx wegen der Symmetrie von R, also folgt $x \in [y]$ aus $[y] \in x$. Nach obigem Argument gilt also auch $[x] \subset [y]$, und somit $[x] = [y]$.

Die Surjektivität von p ist klar nach Definition von M/R, und aus (1) folgt, dass $p(x) = [x] = [y] = p(y)$ genau dann, wenn xRy gilt. Also stimmt (2).

In (3) beginnen wir mit „$\Longrightarrow$“. Sei also $\bar{F}\colon M/R \to N$ gegeben mit $F = \bar{F} \circ p$, und seien x, $y \in M$ gegeben mit xRy. Aus (2) folgt $p(x) = p(y)$, also erst recht

$$F(x) = \bar{F}(p(x)) = \bar{F}(p(y)) = F(y)\ .$$

Zu „$\Longleftarrow$“ gelte $F(x) = F(y)$ für alle x, $y \in M$ mit xRy, also für alle $x \in M$ und alle $y \in [x]$. Seien also $[x] \in M/R$ und $y \in [x]$ beliebig, dann dürfen wir $\bar{F}([x]) = F(y)$ setzen. Diese Konstruktion hängt nach Voraussetzung nicht von der Wahl von $y \in [x]$ ab. Dazu sagen wir, $\bar{F}$ ist *wohldefiniert.*

Die Eindeutigkeit von $\bar{F}$ folgt mit Satz 1.22 (7) aus der Surjektivität von p. □

In der Schule definiert man $\mathbb{Z}$, indem man zu $\mathbb{N}$ noch negative Zahlen hinzunimmt:

$$\mathbb{Z} = \mathbb{N} \,\dot\cup\, \{\, -n \mid n \in \mathbb{N} \setminus \{0\} \,\}.$$

Anschließend definiert man Addition, Subtraktion und Multiplikation. Dabei muss man immer einige Fälle unterscheiden. Wir beschreiben ganze Zahlen stattdessen als Differenzen natürlicher Zahlen, also als $m - n$ für $m, n \in \mathbb{N}$.

1.44. Bemerkung. Um die folgenden Konstruktionen zu verstehen, hier ein paar Vorüberlegungen. Für alle m, n, p, $q \in \mathbb{N}$ gilt in $\mathbb{Z}$:

$$(m-n) = (p-q) \in \mathbb{Z} \quad \Longleftrightarrow \quad m+q = n+p \in \mathbb{N}\,, \tag{1}$$

$$(m-n) + (p-q) = (m+p) - (n+q)\,, \tag{2}$$

$$-(m-n) = n-m\,, \tag{3}$$

$$(m-n)\cdot(p-q) = (m\cdot p + n\cdot q) - (m\cdot q + n\cdot p)\,, \tag{4}$$

$$(m-n) \leq (p-q) \quad \Longleftrightarrow \quad m+q \leq n+p\,. \tag{5}$$

Anstelle von $m - n \in \mathbb{Z}$ betrachten wir das Paar $(m, n) \in \mathbb{N} \times \mathbb{N}$. Gemäß Bemerkung 1.44 (1) definieren wir eine Relation $\sim$ auf der Menge $\mathbb{N} \times \mathbb{N}$ durch

$$(m,n) \sim (p,q) \quad \Longleftrightarrow \quad m+q = n+p \in \mathbb{N}.$$

Außerdem definieren wir Addition, Negatives, Multiplikation und eine Relation $\leq$ gemäß Bemerkung 1.44 (2)–(5) durch

$$\begin{aligned}
(m,n) + (p,q) &= (m+p, n+q),\\
-(m,n) &= (n,m),\\
(m,n)\cdot(p,q) &= (m\cdot p + n\cdot q, m\cdot q + n\cdot p),\\
(m,n) \leq (p,q) \quad &\Longleftrightarrow \quad m+q \leq n+p.
\end{aligned}$$

1.45. Proposition. *Es seien m, n, p, q, r, s, t, $u \in \mathbb{N}$. Dann gilt*

(1) *„$\sim$“ ist eine Äquivalenzrelation.*

(2) *Aus $(m,n) \sim (p,q)$ und $(r,s) \sim (t,u)$ folgt*

$$\begin{aligned}
(m,n) + (r,s) &\sim (p,q) + (t,u),\\
(m,n)\cdot(r,s) &\sim (p,q)\cdot(t,u)\\
\text{und } -(m,n) &\sim -(p,q).
\end{aligned}$$

(3) *Aus $(m,n) \sim (p,q)$ und $(r,s) \sim (t,u)$ folgt*

$$(m,n) \leq (r,s) \quad \Longrightarrow \quad (p,q) \leq (t,u).$$

Beweis. Zu (1): „$\sim$“ ist reflexiv und symmetrisch nach Konstruktion und dem Kommutativgesetz 1.40 (3). Zur Transitivität benutzen wir zusätzlich die Kürzungsregel 1.40 (5):

$$\begin{aligned}
& (m,n) \sim (p,q) \text{ und } (p,q) \sim (r,s)\\
\Longrightarrow \quad & m+q = n+p \text{ und } p+s = q+r\\
\Longrightarrow \quad & m+q+p+s = n+p+q+r\\
\Longrightarrow \quad & m+s = n+r\\
\Longrightarrow \quad & (m,n) \sim (r,s).
\end{aligned}$$

Zu (2): Seien $(m,n) \sim (p,q)$ und $(r,s) \sim (t,u)$, also $m+q = n+p$ und $r+u = s+t$. Wegen $m+q+r+u = n+p+s+t$ folgt

$$(m,n) + (r,s) = (m+r, n+s) \sim (p+t, q+u) = (p,q) + (t,u).$$

Außerdem gilt

$$\begin{aligned} mr + ns + ps + qr &= (m+q)\cdot r + (n+p)\cdot s \\ =&(n+p)\cdot r + (m+q)\cdot s = pr + qs + ms + nr, \end{aligned}$$

also

$$(m,n)(r,s) = (mr+ns, ms+nr) \sim (pr+qs, ps+qr) = (p,q)(r,s).$$

Genauso zeigt man $(p,q)(r,s) \sim (p,q)(t,u)$, und wegen Transitivität gilt $(m,n)(r,s) \sim (p,q)(t,u)$. Die Behauptung $-(m,n) = (n,m) \sim (q,p) = -(p,q)$ ist leicht einzusehen.

Zu (3): Mit $(m,n) \sim (p,q)$ und $(r,s) \sim (t,u)$ wie oben: Aus $(m,n) \leq (r,s)$ folgt $m+s \leq n+r$, also existiert nach Bemerkung 1.39 ein $k \in \mathbb{N}$ mit

$$\begin{aligned} & m+s+k = n+r \\ \quad\Longrightarrow\quad & m+p+s+u+k = n+p+r+u = m+q+s+t \\ \quad\Longrightarrow\quad & p+u+k = q+t \quad\Longrightarrow\quad p+u \leq q+t \\ \quad\Longrightarrow\quad & (p,q) \leq (t,u). \end{aligned}$$

□

Wir definieren also $\mathbb{Z}$ als Quotienten

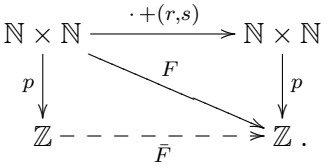
$$\mathbb{Z} = \mathbb{N}\times\mathbb{N} \,/\sim\; = \{\, [(m,n)] \mid (m,n) \in \mathbb{N}\times\mathbb{N} \,\}\,.$$

Proposition 1.45 garantiert wegen der universellen Eigenschaft aus 1.43 (3), dass wir mit Äquivalenzklassen rechnen dürfen:

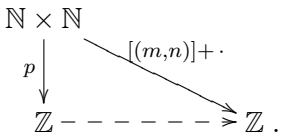
$$\begin{aligned} [(m,n)] + [(p,q)] &= [(m+p, n+q)], \\ [(m,n)] \cdot [(p,q)] &= [(mp+nq, mq+np)], \\ -[(m,n)] &= [(n,m)], \end{aligned}$$

unabhängig von den Repräsentanten $(m,n) \in [(m,n)]$, $(p,q) \in [(p,q)]$. Auch $[(m,n)] \leq [(p,q)]$ ist wohldefiniert.

Konkreter sei $p\colon \mathbb{N}\times\mathbb{N} \to \mathbb{Z}$ die Quotientenabbildung. Wir halten zunächst das Paar $(r,s) \in \mathbb{N}\times\mathbb{N}$ fest und betrachten die Abbildung $F = p \circ (\,\cdot + (r,s))$ wie im folgenden Diagramm:



Also können wir zu einer ganzen Zahl ein festes Paar (r,s) addieren. Jetzt halten wir die ganze Zahl $[(m,n)]$ fest und betrachten die Abbildung $G = [(m,n)] + \cdot : \mathbb{N}\times\mathbb{N} \to \mathbb{Z}$ wie im folgenden Diagramm:



Also dürfen wir zwei ganze Zahlen addieren. Mit den analogen zwei Diagrammen erhalten wir auch die Multiplikation.

1.46. Definition. Die Menge $\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\sim$ heißt Menge der *ganzen Zahlen.*

Wir identifizieren $n \in \mathbb{N}$ mit $[(n,0)] \in \mathbb{Z}$ und schreiben $-n$ für $[(0,n)] \in \mathbb{Z}$. Insbsondere schreiben wir $0 = [(0,0)]$ und $1 = [(1,0)]$.

1.47. Satz. *In $\mathbb{Z}$ gelten Assoziativ- und Kommutativgesetz sowohl für die Addition als auch für die Multiplikation. Neutrale Elemente sind 0 für die Addition und 1 für die Multiplikation. Es gilt das Distributivgesetz. Jedes Element $[(m,n)]$ besitzt ein* additives Inverses $-[(m,n)] = [(n,m)]$*, das heißt, es gilt*

$$[(m,n)] + \big(-[(m,n)]\big) = [(m,n)] + [(n,m)] = [(0,0)].$$

Es gilt die Kürzungsregel für die Multiplikation.

Die Relation „$\leq$“ auf $\mathbb{Z}$ ist eine Ordnung, und für alle a, b, $c \in \mathbb{Z}$ gilt:

$$\begin{aligned} a \leq b \qquad &\Longrightarrow \qquad a + c \leq b + c\,, \\ 0 \leq a \text{ und } 0 \leq b \qquad &\Longrightarrow \qquad 0 \leq ab\,. \end{aligned}$$

Beweis. Das meiste folgt direkt aus Satz 1.40 und den obigen Definitionen. Die neue Gleichung

$$[(m,n)] + \big(-[(m,n)]\big) = [(m,n)] + [(n,m)] = [(0,0)]$$

ergibt sich aus

$$(m,n) + (n,m) = (m+n, n+m) \sim (0,0).$$

Ähnlich zeigt man die Eigenschaften von „$\leq$“. □

Wir haben die natürlichen Zahlen $\mathbb{N}$ zu den ganzen Zahlen $\mathbb{Z}$ erweitert, um additive Inverse zu finden, also Zahlen $-n$ mit $n + (-n) = 0$. Dazu haben wir natürliche Zahlen durch Paare $(m,n) \in \mathbb{N} \times \mathbb{N}$ ersetzt, die für die Zahl $m - n \in \mathbb{Z}$ stehen. Die Zahlen $-n = [(0,n)]$ sind gerade die negativen Zahlen aus der Schule. Der Einfachheit halber schreiben wir ab sofort $a, b, c, \dots \in \mathbb{Z}$, nicht mehr $[(m,n)]$.

Um nun auch multiplikative Inverse $\frac{1}{n}$ mit $n \cdot \frac{1}{n} = 1$ für alle $n \in \mathbb{Z} \setminus \{0\}$ zu erhalten, ersetzen wir ganze Zahlen durch Paare $(p,q) \in \mathbb{Z} \times (\mathbb{N} \setminus \{0\})$, die für Brüche $\frac{p}{q}$ stehen. Das ist die Bruchrechnung, wie wir sie aus der Schule kennen.

Dazu definieren wir für (p,q), $(r,s) \in \mathbb{Z} \times (\mathbb{N} \setminus \{0\})$:

$$(p,q) \sim (r,s) \quad \Longleftrightarrow \quad p \cdot s = q \cdot r \qquad \left(\Longleftrightarrow \quad \frac{p}{q} = \frac{r}{s} \right) ,$$

$$(p,q) + (r,s) = (ps + qr, qs) \qquad \left(\text{da } \frac{p}{q} + \frac{r}{s} = \frac{ps+qr}{qs} \right) ,$$

$$(p,q) \cdot (r,s) = (pr, qs) \qquad \left(\text{da } \frac{p}{q} \cdot \frac{r}{s} = \frac{pr}{qs} \right) ,$$

$$-(p,q) = (-p, q) \qquad \left(\text{da } -\frac{p}{q} = \frac{-p}{q} \right) ,$$

$$(p,q) \leq (r,s) \quad \Longleftrightarrow \quad p \cdot s \leq q \cdot r \qquad \left(\Longleftrightarrow \quad \frac{p}{q} \leq \frac{r}{s}, \text{ da } q, s > 0 \right) .$$

Beachte, dass $qs \in \mathbb{N} \setminus \{0\}$, denn aus $qs = 0 = 0 \cdot s$ würde mit der Kürzungsregel entweder $q = 0$ oder $s = 0$ folgen. Für $p \neq 0$ definieren wir:

$$(p,q)^{-1} = \begin{cases} (q,p) & \text{falls } p > 0, \\ (-q,-p) & \text{falls } p < 0. \end{cases}$$

Beachte: die rechte Seite $(\pm q, \pm p)$ liegt immer in $\mathbb{Z} \times (\mathbb{N} \setminus \{0\})$.

1.48. Proposition. (1) *Die Relation „$\sim$“ ist eine Äquivalenzrelation.*

(2) *Es seiem $(m,n), (p,q), (r,s), (t,u) \in \mathbb{Z} \times (\mathbb{N} \setminus \{0\})$ mit $(m,n) \sim (p,q)$ und $(r,s) \sim (t,u)$ gegeben, dann gilt*

$$(m,n) + (r,s) \sim (p,q) + (t,u),$$
$$(m,n) \cdot (r,s) \sim (p,q) \cdot (t,u),$$

und es gilt $m \neq 0 \Rightarrow p \neq 0$, und in diesem Fall

$$(m,n)^{-1} \sim (p,q)^{-1}.$$

(3) *Unter den gleichen Voraussetzungen wie in* (2) *gilt*

$$(m,n) \leq (r,s) \Rightarrow (p,q) \leq (t,u).$$

Beweis. Die Beweismethode ist die gleiche wie bei Proposition 1.45, wir lassen den Beweis daher aus, ein Teil ist Übung. □

1.49. Definition. Der Quotient $\mathbb{Z} \times (\mathbb{N} \setminus \{0\})/\sim$ heißt Menge der *rationalen Zahlen* und wird mit $\mathbb{Q}$ bezeichnet. Für die Äquivalenzklasse $[(p,q)]$ schreiben wir $\frac{p}{q}$.

Wie zuvor schließen wir aus Proposition 1.48 (2), dass wir mit Brüchen so rechnen dürfen, wie wir es aus der Schule kennen. Proposition 1.48 (3) besagt, dass wir zwei Brüche vergleichen können.

Wir identifizieren eine ganze Zahl $n \in \mathbb{Z}$ mit dem Bruch $\frac{n}{1} \in \mathbb{Q}$ und fassen $\mathbb{Z}$ als Teilmenge von $\mathbb{Q}$ auf. Insbesondere liegen $0 = \frac{0}{1}$ und $1 = \frac{1}{1}$ in $\mathbb{Q}$.

1.50. Satz. *In $\mathbb{Q}$ gelten die folgenden Rechenregeln:*

(1) *Assoziativgesetz für Addition und Multiplikation*

(2) *neutrale Elemente:* $\frac{p}{q} + 0 = \frac{p}{q}$, $\frac{p}{q} \cdot 1 = \frac{p}{q}$ *für alle* $\frac{p}{q} \in \mathbb{Q}$;
(3) *inverse Elemente:* $\frac{p}{q} + \frac{-p}{q} = 0$ *für alle* $\frac{p}{q} \in \mathbb{Q}$, $\frac{p}{q} \cdot \left(\frac{p}{q}\right)^{-1} = 1$ *für alle* $\frac{p}{q} \in \mathbb{Q} \setminus \{0\}$;
(4) *Kommutativgesetz für Addition und Multiplikation;*
(5) *Distributivgesetz;*
(6) *Die Relation „$\leq$“ ist eine Ordnung;*
(7) *Aus* $\frac{p}{q} \leq \frac{r}{s}$ *folgt* $\frac{p}{q} + \frac{t}{u} \leq \frac{r}{s} + \frac{t}{u}$;
(8) *Aus* $0 \leq \frac{p}{q}$ *und* $0 \leq \frac{r}{s}$ *folgt* $0 \leq \frac{p}{q} \cdot \frac{r}{s}$.

Beweis. Diese Aussagen folgen aus den Sätzen 1.40 und 1.47, und aus der Konstruktion von $\mathbb{Q}$. Seien etwa $p, r, t \in \mathbb{Z}$, $q, s, u \in \mathbb{N} \setminus \{0\}$, dann ergibt sich das Assoziativgesetz für die Addition aus

$$\left(\frac{p}{q} + \frac{r}{s}\right) + \frac{t}{u} = \frac{ps + qr}{qs} + \frac{t}{u} = \frac{(ps + qr) \cdot u + qst}{qsu} = \frac{psu + qru + qst}{qsu}$$
$$= \frac{psu + q(ru + st)}{qsu} = \frac{p}{q} + \frac{ru + st}{su} = \frac{p}{q} + \left(\frac{r}{s} + \frac{t}{u}\right) .$$

Betrachten wir das *multiplikative Inverse* $\left(\frac{p}{q}\right)^{-1}$ von $\frac{p}{q} \in \mathbb{Q} \setminus \{0\}$. Wir unterscheiden zwei Fälle:

Falls $0 < p$, gilt $\left(\frac{p}{q}\right)^{-1} = \frac{q}{p}$ und $\frac{p}{q} \cdot \left(\frac{p}{q}\right)^{-1} = \frac{pq}{qp} = 1$.

Falls $p < 0$, gilt $\left(\frac{p}{q}\right)^{-1} = \frac{-q}{-p}$ und $\frac{p}{q} \cdot \left(\frac{p}{q}\right)^{-1} = \frac{p(-q)}{q(-p)} = \frac{-pq}{-qp} = 1$.

Alle anderen Aussagen lassen sich ähnlich beweisen. □

1.4. Etwas Euklidische Geometrie

Der nächste Schritt wäre jetzt die Einführung der reellen Zahlen $\mathbb{R}$. In der Schule definiert man reelle Zahlen als Dezimalbrüche. Diese Konstruktion hat einige Probleme, eines davon ist $0,99\ldots = 1$. In der Analysis lernen Sie eine andere Konstruktion kennen. Die reellen Zahlen haben folgende Eigenschaften.

(1) Die reellen Zahlen bilden einen *angeordneten Körper,* das heißt, es gelten alle Rechenregeln aus Satz 1.50.
(2) Die reellen Zahlen sind *archimedisch angeordnet,* das heißt, die natürlichen Zahlen $\mathbb{N}$ sind in $\mathbb{R}$ enthalten, und zu jeder reellen Zahl $r \in \mathbb{R}$ gibt es eine natürliche Zahl $n \in \mathbb{N}$ mit $r \leq n$.
(3) Die reellen Zahlen sind *vollständig,* das heißt, er ist der größte Körper, für den (1) und (2) gelten. Genauer: wenn es einen anderen Körper $\Bbbk$ gibt, der (1) und (2) erfüllt und $\mathbb{R}$ enthält, dann gilt bereits $\mathbb{R} = \Bbbk$.
(4) Die rationalen Zahlen $\mathbb{Q}$ liegen *dicht* in $\mathbb{R}$, das heißt, zu r, $s \in \mathbb{R}$ mit $r < s$ existiert $\frac{p}{q} \in \mathbb{Q}$ mit $r \leq \frac{p}{q} \leq s$.
(5) Addition, Subtraktion, Multiplikation und Division sind *stetig.*

Die Eigenschaften (1)–(3) definieren $\mathbb{R}$ eindeutig (modulo der Probleme, die wir mit der Eindeutigkeit von $\mathbb{N}$ hatten). Es ist nicht offensichtlich, dass Eigenschaft (3) zu der Definition von Vollständigkeit aus der Analysis äquivalent ist. Aber es ist die einfachste Art, Vollständigkeit zu definieren, ohne analytische Begriffe zu verwenden.

In der Schule haben Sie Vektorrechnung wie folgt kennengelernt. Es sei

$$\mathbb{R}^n = \underbrace{\mathbb{R} \times \cdots \times \mathbb{R}}_{n \text{ Faktoren}} = \left\{ x = (x_1, \ldots, x_n) \;\middle|\; x_1, \ldots, x_n \in \mathbb{R} \right\} ,$$

dann definiert man eine Vektoraddition $\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$, eine skalare Multiplikation $\mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n$ für $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in \mathbb{R}^n$ und $a \in \mathbb{R}$ und einen Nullvektor 0 durch

$$\begin{aligned} x + y &= (x_1 + y_1, \ldots, x_n + y_n) , \\ ax &= (ax_1, \ldots, ax_n) , \\ 0 &= (0, \ldots, 0) . \end{aligned}$$

Um Euklidische Geometrie zu betreiben, definiert man ein Skalarprodukt. Daraus kann man Längen von Vektoren und Winkel zwischen Vektoren ableiten. Für die folgende Definition erinnern wir uns daran, dass die Cosinus-Funktion invertierbar ist als Funktion $\cos\colon [0, \pi] \to [-1, 1]$ mit Umkehrfunktion $\arccos\colon [-1, 1] \to [0, \pi]$. Hierbei messen wir Winkel grundsätzlich in Bogenmaß. Insbesondere gilt

$$1^\circ = \frac{\pi}{180} .$$

1.51. Definition. Wir definieren das *Standard-Skalarprodukt* auf $\mathbb{R}^n$ als Abbildung $\langle \cdot\,, \cdot \rangle\colon \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ für Vektoren x und $y \in \mathbb{R}^n$ durch

$$\langle x, y \rangle = x_1 y_1 + \cdots + x_n y_n . \tag{1}$$

Die *Euklidische Norm* $\| \cdot \| : \mathbb{R}^n \to \mathbb{R}$ auf dem $\mathbb{R}^n$ ist definiert durch

$$\|x\| = \sqrt{\langle x, x \rangle} = \sqrt{x_1^2 + \cdots + x_n^2} . \tag{2}$$

Für zwei Vektoren x, $y \in \mathbb{R}^n \setminus \{0\}$ definieren wir den *Winkel* durch

$$\measuredangle(x, y) = \arccos \frac{\langle x, y \rangle}{\|x\| \, \|y\|} \in [0, \pi] . \tag{3}$$

Wir sammeln einige wichtige Eigenschaften und Rechenregeln.

1.52. Bemerkung. Seien x, y, $z \in \mathbb{R}^n$ sowie a, $b \in \mathbb{R}$, dann gilt

$$\langle ax + by, z \rangle = a\langle x, z \rangle + b\langle y, z \rangle ; \tag{1}$$

$$\langle x, y \rangle = \langle y, x \rangle ; \tag{2}$$

$$\langle x, x \rangle \geq 0 \qquad \text{und} \qquad \langle x, x \rangle = 0 \iff x = 0 . \tag{3}$$

All das rechnet man leicht nach; für (3) nutzen wir aus, dass $x_1^2, \ldots, x_n^2 \geq 0$. Man sagt, das Skalarprodukt ist *linear* in der ersten Variablen (1), *symmetrisch* (2)

und *positiv definit*(3). Aus (1) und (2) folgt, dass das Skalarprodukt auch in der zweiten Variable linear ist, denn

(1') $\quad \langle x, ay + bz\rangle = \langle ay + bz, x\rangle = a\langle y, x\rangle + b\langle z, x\rangle = a\langle x, y\rangle + b\langle x, z\rangle$.

Für den folgenden Satz benötigen wir den reellen *Absolutbetrag* $|\cdot| : \mathbb{R} \to \mathbb{R}$, definiert durch

$$|r| = \begin{cases} r & \text{falls } r \geq 0, \text{ und} \\ -r & \text{falls } r < 0. \end{cases}$$

Insbesondere gilt immer $|r| \geq 0$, und $|r| = \sqrt{r^2}$.

1.53. Satz (Cauchy-Schwarz-Ungleichung)**.** *Für alle Vektoren x, $y \in \mathbb{R}^n$ gilt*

$$|\langle x, y\rangle| \leq \|x\| \cdot \|y\| \ .$$

Gleichheit gilt genau dann, wenn Zahlen a, $b \in \mathbb{R}$ existieren, die nicht beide Null sind, so dass

$$ax + by = 0 \ .$$

Beweis. Wir machen eine Fallunterscheidung.

Fall 1: Es sei $x = 0$. Dann folgt sofort

$$\langle x, y\rangle = 0 = 0 \cdot \|y\| = \|x\| \cdot \|y\| \ .$$

Also gilt sogar Gleichheit, und mit $a = 1$ und $b = 0$ gilt ebenfalls

$$ax + by = 1 \cdot 0 + 0 \cdot y = 0 \ .$$

Fall 2: Es sei $x \neq 0$, dann ist auch $\|x\|^2 \neq 0$, und wir berechnen

$$\begin{aligned} 0 \leq \left\| y - \frac{\langle x, y\rangle}{\|x\|^2}\, x \right\|^2 &= \left\langle y - \frac{\langle x, y\rangle}{\|x\|^2}\, x, y - \frac{\langle x, y\rangle}{\|x\|^2}\, x \right\rangle \\ &= \|y\|^2 - 2\frac{\langle x, y\rangle}{\|x\|^2}\,\langle x, y\rangle + \frac{\langle x, y\rangle^2}{\|x\|^4}\ \|x\|^2 = \|y\|^2 - \frac{\langle x, y\rangle^2}{\|x\|^2} \ . \end{aligned}$$

Da $\|x\|^2 > 0$, folgt mit elementaren Umformungen

$$\langle x, y\rangle^2 \leq \|x\|^2 \cdot \|y\|^2 \ .$$

Wurzelziehen liefert die Behauptung.

Wegen $x \neq 0$, ist Gleichheit in der Cauchy-Schwarz-Ungleichung äquivalent zu

$$y - \frac{\langle x, y\rangle}{\|x\|^2}\, x = 0 \ .$$

Daraus folgt $ax + by = 0$ mit $a = \|x\|^2 \neq 0$ und $b = -\langle x, y\rangle$.

Umgekehrt sei $ax + by = 0$. Wäre $b = 0$, so würde aus $ax = 0$ und $x \neq 0$ bereits $a = 0$ folgen, aber a und b dürfen nicht beide verschwinden. Also folgt $b \neq 0$ und

$$y = -\frac{a}{b}\, x = -\frac{\langle x, \frac{a}{b}\, x\rangle}{\|x\|^2}\, x = \frac{\langle x, y\rangle}{\|x\|^2}\, x \ ,$$

und es gilt Gleichheit in der Cauchy-Schwarz-Ungleichung. □

Der Vektor $y - \frac{\langle x,y\rangle}{\|x\|^2}\, x$ im obigen Beweis entspricht dem Lot vom Punkt y auf die Gerade durch 0 mit Richtung x. Insbesondere gilt Gleichheit, wenn der Punkt y auf dieser Geraden liegt.

1.54. Bemerkung. Aus der Cauchy-Schwarz-Ungleichung 1.53 folgt

$$\frac{\langle x, y\rangle}{\|x\|\,\|y\|} \in [-1, 1] \subset \mathbb{R}\ ,$$

also ist der Arcuscosinus in Definition 1.51 (3) erklärt und der Winkel wohldefiniert. Umgekehrt gilt also

$$\langle x, y\rangle = \|x\|\,\|y\| \cos \measuredangle(x, y)\ . \tag{1}$$

Zur geometrischen Interpretation betrachten wir das Dreieck mit den Endpunkten 0, x und y. Die dritte Seite ist $x - y$, und wir erhalten den Cosinussatz der Euklidischen Geometrie:

$$\|x - y\|^2 = \|x\|^2 - 2\langle x, y\rangle + \|y\|^2 = \|x\|^2 + \|y\|^2 - 2\,\|x\|\,\|y\| \cos \measuredangle(x, y)\ . \tag{2}$$

1.5. Komplexe Zahlen und die Geometrie der Ebene

In den reellen Zahlen können wir Wurzeln aus positiven Zahlen ziehen, beispielsweise aus 2, was in $\mathbb{Q}$ nicht möglich ist. Man kann aber keine Wurzeln aus negativen Zahlen ziehen. Diesen Missstand wollen wir jetzt beheben, indem wir die reellen Zahlen zu den komplexen Zahlen erweitern.

Die Idee ist, eine neue Zahl i einzuführen, deren Quadrat -1 ist. Wir möchten mit Zahlen $a + bi$ mit a, $b \in \mathbb{R}$ rechnen, und alle von $\mathbb{R}$ vertrauten Rechenregeln sollen gelten. Zum Beispiel sollten die folgenden Rechnungen richtig sein:

$$(a + bi) + (c + di) = a + c + bi + di = (a + c) + (b + d)i\ ,$$

$$\text{und} \qquad (a + bi) \cdot (c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i\ .$$

Um das rigoros zu machen, betrachten wir eine komplexe Zahl als Paar aus zwei reellen Zahlen, und definieren Addition und Multiplikation wie oben. Für eine Menge M und $n \in \mathbb{N}$ bezeichne M^n das n-fache kartesische Produkt von M mit sich selbst, etwa $M^2 = M \times M$.

1.55. Definition. Die *komplexen Zahlen* sind definiert als $\mathbb{C} = \mathbb{R}^2$, mit

$$(a, b) + (c, d) = (a + c, b + d)$$

$$\text{und} \qquad (a, b) \cdot (c, d) = (ac - bd, ad + bc)$$

für alle a, b, c, $d \in \mathbb{R}$.

1.56. Satz. *In $\mathbb{C}$ gelten Assoziativ- und Kommutativgesetz sowohl für die Addition als auch für die Multiplikation. Neutrale Elemente sind $0_{\mathbb{C}} = (0, 0)$ für die Addition und $1_{\mathbb{C}} = (1, 0)$ für die Multiplikation. Es gilt das Distributivgesetz. Jedes Element (a, b) besitzt ein additives Inverses*

$$-(a, b) = (-a, -b)$$

und, falls $(a,b) \neq 0_{\mathbb{C}}$*, ein multiplikatives Inverses*

$$(a,b)^{-1} = \left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2} \right) .$$

Beweis. Alle Behauptungen lassen sich direkt mit den Formeln aus Definition 1.55 nachrechnen. Beispielsweise gilt

$$(a,b) \cdot \left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2} \right) = \left(\frac{a^2+b^2}{a^2+b^2}, \frac{-ab+ba}{a^2+b^2} \right) = (1,0) = 1_{\mathbb{C}} . \qquad \square$$

Wir sehen, dass die Abbildung $\mathbb{R} \to \mathbb{C}$ mit $a \mapsto (a,0)$ verträglich mit $+$ und $\cdot$ ist, und 0 und $1 \in \mathbb{R}$ auf $0_{\mathbb{R}}$ und $1_{\mathbb{R}}$ abbildet. Wir dürfen also $\mathbb{R}$ mit den komplexen Zahlen der Form $(\,\cdot\,, 0)$ identifizieren. Wenn wir außerdem noch $i = (0,1)$ definieren, können wir uns überzeugen, dass

$$(a,b) = a \cdot (1,0) + b \cdot (0,1) = a + bi$$

für alle a, $b \in \mathbb{R}$ gilt. Damit haben wir unsere Idee vom Anfang des Abschnitts verwirklicht. Außerdem dürfen wir jetzt auch 0 und 1 für $0_{\mathbb{C}}$ und $1_{\mathbb{C}}$ schreiben.

1.57. Bemerkung. Auf $\mathbb{C}$ gibt es keine Ordnung „$\leq$“, die zu Satz 1.50 (7) und (8) analoge Eigenschaften hat. Denn gäbe es solch eine Ordnung, dann gälte entweder $0 < x$ oder $0 > x$ für alle $x \neq 0$ wegen Totalität, aber wegen (7) gälte $0 > x$ genau dann, wenn $-x > 0$. Also gälte $x^2 = (-x)^2 > 0$ für alle $x \neq 0$ wegen (8), aber dann erhielten wir wegen (7) und Transitivität einen Widerspruch:

$$0 = 1^2 + i^2 \geq 1^2 > 0 .$$

1.58. Definition. Sei $z = a + bi \in \mathbb{C}$ mit a, $b \in \mathbb{R}$, dann heißt a der *Realteil* $\mathrm{Re}(z)$ von z und b der *Imaginärteil* $\mathrm{Im}(z)$ von z.

Der Imaginärteil ist also immer eine reelle Zahl, und es gilt

$$z = \mathrm{Re}(z) + \mathrm{Im}(z) \cdot i .$$

1.59. Definition. Die Abbildung $\mathbb{C} \to \mathbb{C}$ mit $z \mapsto \bar{z} = \mathrm{Re}(z) - \mathrm{Im}(z) \cdot i$ heißt *komplexe Konjugation,* $\bar{z}$ heißt das (*komplex*) *Konjugierte* von z.

1.60. Bemerkung. Die komplexe Konjugation ist verträglich mit allen Rechenoperationen, das heißt, es gilt

$$\bar{z} + \bar{w} = \overline{z+w} , \qquad \bar{z} \cdot \bar{w} = \overline{z \cdot w} ,$$
$$\overline{-z} = -\bar{z} , \qquad \overline{z^{-1}} = \bar{z}^{-1} ,$$
$$\overline{0} = 0 , \qquad \overline{1} = 1 ,$$

auch das rechnet man leicht nach.

Es gilt $\bar{\bar{z}} = z$ für alle z, also ist die komplexe Konjugation ihre eigene Umkehrabbildung. Für eine komplexe Zahl z gilt $z = \bar{z}$ genau dann, wenn $z \in \mathbb{R} \subset \mathbb{C}$.

Man kann die komplexen Zahlen dadurch charakterisieren, dass sie die kleinste Erweiterung der reellen Zahlen $\mathbb{R}$ ist, so dass alle Rechenregeln aus Satz 1.56

gelten und eine Zahl i mit $i^2 = -1$ existiert. Aber i ist dadurch nicht eindeutig bestimmt, denn offensicht sind i und $\bar{i} = -i$ gleichberechtigt.

Die Zahl $z = i$ löst die Gleichung $z^2 + 1 = 0$. In den Übungen werden Sie sehen, dass man $z^2 = w$ für alle komplexen Zahlen w lösen kann. All das sind Spezialfälle des folgenden Satzes.

1.61. Satz (Fundamentalsatz der Algebra)**.** *Es seien $n \geq 1$ und $a_1, \ldots, a_n \in \mathbb{C}$, dann existiert $z \in \mathbb{C}$, so dass*

$$z^n + a_1 z^{n-1} + \cdots + a_{n-1} z + a_n = 0 \, .$$

Mit rein algebraischen Methoden lässt sich dieser Satz nicht beweisen. Das liegt daran, dass die reellen Zahlen, die den komplexen ja zugrundeliegen, mit analytischen Mitteln konstruiert wurden. Einen Beweis für diesen Satz lernen Sie daher erst später, zum Beispiel in einer Vorlesung über Funktionentheorie oder Topologie.

Für $z = a + bi$ mit $a, b \in \mathbb{R}$ ist

$$z \cdot \bar{z} = (a + bi)(a - bi) = a^2 - (bi)^2 = a^2 + b^2 \geq 0$$

reell. Das ermöglicht folgende Definition.

1.62. Definition. Wir definieren den *Absolutbetrag* (die *Norm* oder die *Länge*) einer komplexen Zahl $z \in \mathbb{C}$ als die reelle Zahl

$$|z| = \sqrt{z \cdot \bar{z}} \geq 0 \, .$$

1.63. Bemerkung. Wir sammeln ein paar Eigenschaften des Absolutbetrages.

(1) Da $|a + bi|^2 = a^2 + b^2$, entspricht $|z| = \|z\|$ der euklidischen Norm auf $\mathbb{C} = \mathbb{R}^2$ aus Definition 1.51 (1).

(2) Unsere Konstruktion von $z^{-1} = \frac{\bar{z}}{|z|^2}$ wird jetzt etwas klarer, denn

$$z \cdot \frac{\bar{z}}{|z|^2} = \frac{|z|^2}{|z|^2} = 1 \, .$$

(3) Der Absolutbetrag ist *multiplikativ,* das heißt, für alle z und w gilt

$$|zw| = \sqrt{zw\,\overline{zw}} = \sqrt{(z\bar{z})(w\bar{w})} = \sqrt{z\bar{z}} \cdot \sqrt{w\bar{w}} = |z|\,|w| \ .$$

(4) Der Absolutbetrag ist *subadditiv* wegen (1) und der Cauchy-Schwarz-Ungleichung 1.53, das heißt, für alle z, $w \in \mathbb{C}$ gilt

$$|z + w| \leq |z| + |w| \ ,$$

denn

$$\begin{aligned} |z + w|^2 &= \|z + w\|^2 = \|z\|^2 + \|w\|^2 + 2\langle z, w\rangle \\ &\leq \|z\|^2 + \|w\|^2 + 2\,\|z\|\,\|w\| = (\|z\| + \|w\|)^2 = (|z| + |w|)^2 \, . \end{aligned}$$

(5) Komplexe Konjugation ist mit dem Absolutbetrag verträglich, denn

$$|\bar{z}| = \sqrt{\bar{z}z} = \sqrt{z\bar{z}} = |z| \ .$$

Wir wollen uns Addition und Multiplikation in $\mathbb{C}$ jetzt mit Hilfer der zweidimensionalen Euklidischen Geometrie veranschaulichen. Dazu machen wir einige Anleihen aus der Schulmathematik und identifizieren $\mathbb{C}$ mit dem Vektorraum $\mathbb{R}^2$.

Die Addition in $\mathbb{C}$ entspricht der Vektoraddition in $\mathbb{R}^2$. Die komplexe Konjugation ist eine Spiegelung an der reellen Achse (also an der x-Achse).

Wir schreiben einen Vektor $z \in \mathbb{C} \setminus \{0\}$ als

$$z = |z| \cdot \frac{z}{|z|} \, .$$

Dann misst $|z| = \|z\|$ die Länge von z. Multiplikation mit $|z| \in \mathbb{R} \subset \mathbb{C}$ entspricht offenbar der Streckung im $\mathbb{R}^2$ mit dem Faktor $|z|$, denn

$$|z| \cdot (a + bi) = (|z| + 0i)(a + bi) = |z|\, a + |z|\, bi \, .$$

Der Vektor $\frac{z}{|z|}$ hat Länge 1 und beschreibt die Richtung von z. Wir nehmen jetzt an, dass bereits $|z| = 1$ gilt. Es sei φ der Winkel zwischen der positiven reellen Achse $\mathbb{R}_> \subset \mathbb{C}$ ("x-Achse") und z (entgegen dem Uhrzeigersinn gemessen), so dass

$$z = \cos\varphi + i \, \sin\varphi \, .$$

Für einen beliebigen Vektor $w = c + di$ folgt

$$z \cdot w = (c\cos\varphi - d\sin\varphi) + (c\sin\varphi + d\cos\varphi)\, i \, .$$

Sei auf der anderen Seite R_φ die Drehung um den Winkel φ gegen den Uhrzeigersinn mit Zentrum 0. Aus der Schulzeit wissen wir, dass diese Drehung $\mathbb{R}$-linear ist. Für c, $d \in \mathbb{R}$ gilt also

$$\begin{aligned} R_\varphi(c + di) &= c\, R_\varphi(1) + d\, R_\varphi(i) \\ &= c(\cos\varphi + i \, \sin\varphi) + d\,(-\sin\varphi + i \, \cos\varphi) = z \cdot w \, , \end{aligned}$$

Also beschreibt die komplexe Multiplikation mit einer komplexen Zahl $z = \cos\varphi + i \, \sin\varphi$ vom Betrag 1 genau eine Drehung um φ.

Sei jetzt $z \in \mathbb{C}$, $z \neq 0$, und sei $0 \leq \varphi < 2\pi$ der Winkel zwischen z und der positiven reellen Achse, so dass

$$z = |z| \cdot (\cos\varphi + i \, \sin\varphi) \, .$$

Der Winkel φ heißt auch das *Argument* von z, geschrieben $\varphi = \arg(z)$, und die obige Schreibweise heißt auch die *Polardarstellung* von z. Dann entspricht Multiplikation mit z einer Drehung um den Winkel φ mit Zentrum 0 und einer anschließenden Streckung um den Faktor $|z|$.

1.64. Bemerkung (Geometrische Interpretation der komplexen Multiplikation)**.** Es seien z, $w \in \mathbb{C} \setminus \{0\}$ Zahlen mit Beträgen $r = |z|$, $s = |w|$ und Argumenten $\varphi = \arg z$ und $\psi = \arg w$. Nach unser Vorüberlegung wird der

Vektor w durch Multiplikation mit z um r gestreckt und um φ gedreht, so dass schließlich

$$|zw| = rs = |z|\,|w|\ , \qquad \arg(zw) = \varphi + \psi = \arg(z) + \arg(w)$$
$$\text{und} \qquad zw = rs\big(\cos(\varphi+\psi) + i\sin(\varphi+\psi)\big)\ .$$

Für $r = s = 1$ folgen aus der Rechnung

$$\begin{aligned}\cos(\varphi+\psi) + i\sin(\varphi+\psi) &= (\cos\varphi + i\sin\varphi)\cdot(\cos\psi + i\sin\psi)\\ &= (\cos\varphi\cos\psi - \sin\varphi\sin\psi) + i(\cos\varphi\sin\psi + \sin\varphi\cos\psi)\end{aligned}$$

die *Additionstheoreme* für Sinus und Cosinus:

$$\cos(\varphi+\psi) = \cos\varphi\cos\psi - \sin\varphi\sin\psi$$
$$\text{und} \qquad \sin(\varphi+\psi) = \cos\varphi\sin\psi + \sin\varphi\cos\psi\ .$$

Man beachte aber, dass wir uns in dieser ganzen Bemerkung voll und ganz auf unsere Anschauung und unsere Schulkenntnisse in ebener Geometrie verlassen haben. Das reicht nicht als Grundlage für einen strikten Beweis, daher werden wir nach diesem Abschnitt nicht mehr auf diese Überlegungen zurückgreifen. Nichtsdestotrotz wollen wir aber aus den obigen Formeln in den Übungen noch einige interessante Folgerungen ziehen.

1.65. Bemerkung. Die Isometrien der Ebene werden erzeugt von

(1) Verschiebungen $w \mapsto a + w$ mit $a \in \mathbb{C}$,
(2) Drehungen um den Ursprung, $w \mapsto zw$, wobei $z \in \mathbb{C}$ mit $|z| = 1$, und
(3) der Spiegelung an der x-Achse, $w \mapsto \bar{w}$.

Insgesamt können wir also jede Isometrie $F\colon \mathbb{R}^2 \to \mathbb{R}^2$ mit Hilfe komplexer Zahlen schreiben als

$$F(w) = a + zw \qquad \text{oder} \qquad F(w) = a + z\bar{w}\ ,$$

wobei a und $z \in \mathbb{C}$ mit $|z| = 1$ durch F eindeutig festgelegt sind.

Es fällt auf, dass der oben benutzte Winkelbegriff nicht ganz mit dem aus dem letzten Abschnitt übereinstimmt. Hier betrachten wir Drehungen gegen den Uhrzeigersinn um beliebige Winkel, wobei der Winkel φ und der Winkel $\varphi+2\pi n$ für alle $n \in \mathbb{Z}$ die gleiche Drehung beschreiben. Alle Winkel im Intervall

$$(-\pi, \pi] = \big\{\, x \in \mathbb{R} \;\big|\; -\pi < x \le \pi \,\big\}$$

stehen für verschiedene Drehungen, insbesondere entsprechen Winkel $\varphi \in (-\pi, 0)$ Drehungen im Uhrzeigersinn um $|\varphi|$.

In Definition 1.51 (3) hingegen haben wir nur „ungerichtete“ Winkel im Intervall $[0, \pi]$ betrachtet. Besser ging es nicht, da die Winkel φ und $-\varphi$ den gleichen Cosinus haben, und die Funktion Arcus Cosinus sich nach unser Definition für Winkel in $[0, \pi]$ entscheidet.

1.6. Geometrie des Raumes und Quaternionen

Wir geben einen kurzen Abriss der Euklidischen Geometrie des Raumes, inbesondere führen wir das Kreuzprodukt ein. In Analogie zu den komplexen Zahlen definieren wir die Quaternionen, bei denen sowohl Kreuz- als auch Skalarprodukt auf dem $\mathbb{R}^3$ eine wichtige Rolle spielen. Die wichtigsten Eigenschaften der Quaternionen lernen wir später kennen.

1.66. Definition. Das *Kreuzprodukt* (*Vektorprodukt*) auf dem $\mathbb{R}^3$ ist eine Abbildung $\times\colon \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$ mit

$$(u_1, u_2, u_3) \times (v_1, v_2, v_3) = (u_2v_3 - u_3v_2, u_3v_1 - u_1v_3, u_1v_2 - u_2v_1) \; .$$

Beachten Sie, dass das Symbol "$\times$" sowohl das kartesiche Produkt von Mengen ($\mathbb{R}^3 \times \mathbb{R}^3$) als auch das Kreuzprodukt von Vektoren bezeichnet. Missverständnisse wird es deswegen voraussichtlich nicht geben.

1.67. Bemerkung. Für alle u, v, $w \in \mathbb{R}^3$ und alle a, $b \in \mathbb{R}$ gilt

$$(au + bv) \times w = a(u \times w) + b(v \times w) \; , \tag{1}$$

$$u \times v = -v \times u \; . \tag{2}$$

All dies folgt unmittelbar aus Definition 1.66. Man sagt, das Kreuzprodukt ist linear im ersten Argument (1) und *antisymmetrisch* (2) .

Wegen (1) und (2) ist das Kreuzprodukt auch im zweiten Argument linear, denn

$$\begin{aligned} u \times (av + bw) &= -(av + bw) \times u \\ &= -a(v \times u) - b(w \times u) = a(u \times v) + b(u \times w) \; . \end{aligned} \tag{1'}$$

1.68. Satz. *Für alle u, v, w, $t \in \mathbb{R}^3$ gilt*

$$\langle u \times v, w\rangle = \langle v \times w, u\rangle = \langle w \times u, v\rangle \; , \tag{1}$$

$$(u \times v) \times w = \langle u, w\rangle \cdot v - \langle v, w\rangle \cdot u = w \times (v \times u) \; , \tag{2}$$

$$0 = (u \times v) \times w + (v \times w) \times u + (w \times u) \times v \; , \tag{3}$$

$$\langle u \times v, w \times t\rangle = \langle u, w\rangle\langle v, t\rangle - \langle u, t\rangle\langle v, w\rangle \tag{4}$$

Die Gleichung (2) heißt auch *Graßmann-Identität,* und (3) heißt *Jacobi-Identität.* Den Ausdruck $\langle u \times v, w\rangle$ in (1) nennt man auch das *Spatprodukt* der Vektoren u, v, w.

Beweis. Zu (1) berechnen wir

$$\langle u \times v, w\rangle = u_2v_3w_1 - u_3v_2w_1 + u_3v_1w_2 - u_1v_3w_2 + u_1v_2w_3 - u_2v_1w_3 \; ,$$

und dieser Ausdruck ist invariant unter zyklischer Vertauschung von u, v und w.

Die Graßmann-Identität (2) überprüfen wir nur in der ersten Komponente der ersten Gleichung:

$$\begin{aligned}\big((u\times v)\times w\big)_1 &= (u\times v)_2\cdot w_3 - (u\times v)_3\cdot w_2\\ &= u_3\cdot v_1\cdot w_3 - u_1\cdot v_3\cdot w_3 - u_1\cdot v_2\cdot w_2 + u_2\cdot v_1\cdot w_2\\ &= (u_1\cdot w_1 + u_2\cdot w_2 + u_3\cdot w_3)\cdot v_1\\ &\qquad - (v_1\cdot w_1 + v_2\cdot w_2 + v_3\cdot w_3)\cdot u_1\\ &= \langle u,w\rangle\cdot v_1 - \langle v,w\rangle\cdot u_1\ ;\end{aligned}$$

die zweite und dritte Komponente ergeben sich, indem man oben die Indizes 1, 2 und 3 zyklisch vertauscht. Die zweite Gleichung folgt aus der ersten mit Antisymmetrie.

Die Jacobi-Identität (3) folgt, indem man u, v und w in (2) zyklisch permutiert und dann alle drei Gleichungen addiert.

Behauptung (4) folgt aus (1) und (2) durch folgende Rechnung:

$$\begin{aligned}\langle u\times v, w\times t\rangle &= \langle (w\times t)\times u, v\rangle\\ &= \big\langle \langle w,u\rangle\cdot t - \langle t,u\rangle\cdot w, v\big\rangle = \langle u,w\rangle\langle v,t\rangle - \langle u,t\rangle\langle v,w\rangle\ .\end{aligned}$$ □

1.69. Bemerkung. Wir geben eine geometrische Interpretation.

(1) Satz 1.68 (4) und Bemerkung 1.54 (1) implizieren, dass

$$\begin{aligned}\|u\times v\| &= \sqrt{\|u\|^2\,\|v\|^2 - \langle u,v\rangle^2}\\ &= \sqrt{\|u\|^2\,\|v\|^2\,(1-\cos^2\measuredangle(u,v))} = \|u\|\,\|v\|\sin\measuredangle(u,v)\ ,\end{aligned}$$

da $\sin^2+\cos^2 = 1$ und $\sin\varphi \geq 0$ für alle $\varphi\in[0,\pi]$. Also ist $\|u\times v\|$ gerade der Flächeninhalt des von u und v aufgespannten Parallelogramms. Aus Bemerkung 1.67 (2) und Satz 1.68 (1) folgt

$$\langle u\times v, u\rangle = \langle u\times u, v\rangle = 0 \qquad \text{und} \qquad \langle u\times v, v\rangle = \langle v\times v, u\rangle = 0\ .$$

Also steht $u\times v$ senkrecht auf der Fläche dieses Parallelogramms. Damit haben wir eine geometrische Beschreibung des Kreuzproduktes *bis auf das Vorzeichen.* Das Vorzeichen ergibt sich durch die Wahl einer Orientierung, wie wir später in Beispiel 4.29 lernen werden.

(2) Das Spatprodukt können wir nun als Volumen des Parallelotops mit den Kanten u, v und w interpretieren. Da $u\times v$ senkrecht auf der Grundfläche steht, wird die Höhe dieses Parallelotops gerade gegeben durch

$$\|w\|\,|\cos\measuredangle(u\times v, w)| = \|w\|\ \frac{|\langle u\times v, w\rangle|}{\|u\times v\|\,\|w\|} = \frac{|\langle u\times v, w\rangle|}{\|u\times v\|}\ .$$

Als Produkt aus Grundfläche $\|u\times v\|$ und Höhe erhalten wir das Volumen also als Absolutbetrag $|\langle u\times v, w\rangle|$ des Spatproduktes. Das Vorzeichen des Spatproduktes ist wiederum eine Frage der Orientierung.

Wir erinnern uns an unsere Definition 1.55 der komplexen Zahlen. Dort wurde eine Multiplikation auf $\mathbb{R} \times \mathbb{R}$ erklärt durch

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc) \; .$$

Wir führen jetzt die etwas kompliziertere Quaternionen-Multiplikation ein. Die Quaternionen wurden von Hamilton entdeckt, daher der Buchstabe $\mathbb{H}$.

1.70. Definition. Die *Quaternionen* sind definiert als $\mathbb{H} = \mathbb{R} \times \mathbb{R}^3$, mit

$$\begin{aligned} (a, u) + (b, v) &= (a + b, u + v) \; , \\ (a, u) \cdot (b, v) &= \big(a \cdot b - \langle u, v \rangle, a \cdot v + b \cdot u + u \times v\big) \\ \text{und} \qquad \overline{(a, u)} &= (a, -u) \end{aligned}$$

für alle a, $b \in \mathbb{R}$ und alle u, $v \in \mathbb{R}^3$. Wir identifizieren $a \in \mathbb{R}$ mit $(a, 0) \in \mathbb{H}$ und $u \in \mathbb{R}^3$ mit $(0, u) \in \mathbb{H}$, und definieren Real- und Imaginärteil von (a, u) durch

$$\begin{aligned} \mathrm{Re}(a, u) &= \frac{1}{2} \left((a, u) + \overline{(a, u)} \right) = a \in \mathbb{R} \\ \text{und} \qquad \mathrm{Im}(a, u) &= \frac{1}{2} \left((a, u) - \overline{(a, u)} \right) = u \in \mathbb{R}^3 \; . \end{aligned}$$

1.71. Satz. *In $\mathbb{H}$ gelten Assoziativ- und Kommutativgesetz für die Addition. Die Multiplikation ist assoziativ aber nicht kommutativ. Es gelten Distributivgesetze*

$$p \cdot (q + r) = p \cdot q + p \cdot r \qquad \text{und} \qquad (p + q) \cdot r = p \cdot r + q \cdot r \tag{1}$$

für alle p, q, $r \in \mathbb{H}$. Neutrale Elemente sind $0_{\mathbb{H}} = (0, 0)$ für die Addition und $1_{\mathbb{H}} = (1, 0)$ für die Multiplikation. Jedes Element (a, u) besitzt ein additives Inverses

$$-(a, u) = (-a, -u) \tag{2}$$

und, falls $(a, u) \neq 0_{\mathbb{H}}$, ein multipliktives Inverses

$$(a, u)^{-1} = \left(\frac{a}{a^2 + \|u\|^2}, -\frac{u}{a^2 + \|u\|^2} \right) \; . \tag{3}$$

Für ein Quaternion (a, u) gilt

$$(a, u) \cdot (b, v) = (b, v) \cdot (a, u) \tag{4}$$

für alle $(b, v) \in \mathbb{H}$ genau dann, wenn $(a, u) \in \mathbb{R}$, das heißt, wenn $u = 0$.

Für die Quaternionen-Konjugation gilt

$$\overline{(a, u) + (b, v)} = \overline{(a, u)} + \overline{(b, v)} \; , \qquad \overline{-(a, u)} = -\overline{(a, u)} \; , \tag{5}$$

$$\overline{(a, u) \cdot (b, v)} = \overline{(b, v)} \cdot \overline{(a, u)} \; , \qquad \overline{(a, u)^{-1}} = \overline{(a, u)}^{-1} \tag{6}$$

und es gilt

$$\overline{(a, u)} \cdot (a, u) = a^2 + \|u\|^2 = (a, u) \cdot \overline{(a, u)} \; . \tag{7}$$

Man beachte, dass wir in (1) zwei Distributivgesetze brauchen, da die Multiplikation in $\mathbb{H}$ nicht kommutativ ist.

BEWEIS. Die Rechenregeln für die Addition sind leicht zu überprüfen. Die Distributivgesetze (1) folgen aus den Bemerkungen 1.52 (1) und 1.67 (1), zum Beispiel gilt

$$\begin{aligned}(a,u)\cdot\big((b,v)+(c,w)\big)&\\ &= (a,u)\cdot(b+c,v+w)\\ &= \big(a(b+c)-\langle u,v+w\rangle, a(v+w)+(b+c)u+u\times(v+w)\big)\\ &= (ab-\langle u,v\rangle, av+bu+u\times v)+(ac-\langle u,w\rangle, aw+cu+u\times w)\\ &= (a,u)\times(b,v)+(a,u)\times(c,w)\ .\end{aligned}$$

Das Assoziativgesetz für die Multiplikation folgt aus Satz 1.68 (1) und (2) und bleibt Übung. Außerdem überprüft man leicht, dass

$$(a,u)+(0,0)=(a,u)=(a,u)\cdot(1,0)=(1,0)\cdot(a,u)\ .$$

Auch die Formel (2) für das additive Inverse ist klar.

Es gelte (4). Aus der Symmetrie des Skalarproduktes und der Antisymmetrie des Kreuzproduktes folgt

$$\begin{aligned}0&=(a,u)\cdot(b,v)-(b,v)\cdot(a,u)\\ &=(0,u\times v-v\times u)=(0,2u\times v)\ .\end{aligned}$$

Nach Bemerkung 1.69 (1) folgt: wenn (4) für alle (b,v) gilt, dann hat für jeden Vektor $v\in\mathbb{R}^3$ das von u, v aufgespannte Parallelogramm den Flächeninhalt 0. Aber dann muss bereits $u=0$, also $(a,u)\in\mathbb{R}$ gelten.

Es gilt

$$\begin{aligned}\overline{(a,u)}\cdot(a,u)&=(a,-u)\cdot(a,u)\\ &=\big(a^2+\langle u,u\rangle, au-au-u\times u\big)=a^2+\|u\|^2\in\mathbb{R}\ ,\end{aligned}$$

und es folgt die erste Gleichung in (7). Die zweite erhalten wir, indem wir u durch $-u$ ersetzen. Aus (7) folgt (3), denn

$$\left(\frac{a}{a^2+\|u\|^2},-\frac{u}{a^2+\|u\|^2}\right)\cdot(a,u)=\frac{1}{\overline{(a,u)}\cdot(a,u)}\,\overline{(a,u)}\cdot(a,u)=1\ .$$

Gleichung (5) ist wiederum klar, und (6) folgt aus der Antisymmetrie des Kreuzproduktes, denn

$$\begin{aligned}\overline{(a,u)\cdot(b,v)}&=(ab-\langle u,v\rangle,-av-bu-u\times v)\\ &=\big(ab-\langle -v,-u\rangle, b(-u)+a(-v)+(-v)\times(-u)\big)\\ &=\overline{(b,v)}\cdot\overline{(a,u)}\ .\end{aligned}$$

□

1.72. Definition. Wir definieren den *Absolutbetrag* eines Quaternions $q\in\mathbb{H}$ als die reelle Zahl

$$|q|=\sqrt{\overline{q}q}\ .$$

Wegen Satz 1.71 (7) ist das möglich, und für $q = (a, u_1, u_2, u_3) \in \mathbb{H}$ gilt

$$|q|^2 = a^2 + u_1^2 + u_2^2 + u_3^2 \,,$$

also stimmt $|q|$ wiederum mit der Euklidischen Norm $\|q\|$ auf $\mathbb{R}^4$ überein.

1.73. Bemerkung. So, wie wir den komplexen Zahlen $(1,0)$ und $(0,1)$ die Namen 1 und i gegeben haben, wollen wir hier die folgenden Bezeichnungen einführen:

$$1 = (1,0) \,, \qquad i = (0, e_1) \,, \qquad j = (0, e_2) \qquad \text{und} \qquad k = (0, e_3) \,.$$

Wir erhalten die Multiplikationstabelle

$\cdot$	i	j	k
i	-1	k	$-j$
j	$-k$	-1	i
k	j	$-i$	-1 .

Zusammen mit den Distributivgesetzen und Satz 1.71 (4) können wir jetzt alle Quaternionen miteinander multiplizieren.

So wie die komplexen Zahlen die Geometrie der Ebene beschreiben, beschreiben die imaginären Quaternionen die Geometrie des dreidimensionalen Raumes. Wir sehen, dass sowohl das Standard-Skalarprodukt als auch das Kreuzprodukt in der Definition auftauchen, und in der Tat erhalten wir diese zurück als

$$\langle u, v \rangle = \operatorname{Re}(\overline{(0,u)} \cdot (0,v)) \qquad \text{und} \qquad u \times v = \operatorname{Im}((0,u) \cdot (0,v)) \,.$$

Jetzt wollen wir Isometrien des $\mathbb{R}^3$ mit Hilfe von Quaternionen beschreiben.

1.74. Satz. *Es sei $q = (\cos\varphi, v \sin\varphi) \in \mathbb{H}$, wobei $v \in \mathbb{R}^3$ mit $\|v\| = 1$ und $\varphi \in \mathbb{R}$. Für ein imaginäres $w \in \mathbb{R}^3$ ist $qw\bar{q}$ wieder imaginär. Die Abbildung $F_q \colon \mathbb{R}^3 \to \mathbb{R}^3$ mit $w \mapsto qw\bar{q}$ beschreibt eine Drehung um die Achse durch 0 in Richtung v um den Winkel 2φ.*

Beweis. Ein Quaternion w ist imaginär genau dann, wenn $\bar{w} = -w$ gilt. Wenn w imaginär ist, ist auch $qw\bar{q}$ imaginär, denn

$$\overline{qw\bar{q}} = \bar{\bar{q}}\bar{w}\bar{q} = -qw\bar{q} \,.$$

Die Abbildung F_q ist $\mathbb{R}$-linear wegen Satz 1.71 (1) und (4). Das gleiche gilt für die Drehung $R_{v,2\varphi}$ um die Achse durch 0 in Richtung v um den Winkel 2φ. Wir zerlegen $w \in \mathbb{R}^3$ wie im Beweis der Cauchy-Schwarz-Ungleichung 1.53 als

$$w = \langle v, w \rangle v + (w - \langle v, w \rangle v) \,,$$

so dass der zweite Vektor wegen $\|v\| = 1$ senkrecht auf v steht. Wegen Linearität reicht es, $F_q v = R_{v,2\varphi} v$ und $F_q w = R_{v,2\varphi} w$ für alle Vektoren w mit $|w| = 1$ und $\langle v, w \rangle = 0$ zu zeigen.

Betrachte zunächst v. Wegen $\langle v, v\rangle = 1$ und $v \times v = 0$ gilt in diesem Fall

$$\begin{aligned} qw\bar{q} &= (\cos\varphi, v\sin\varphi)\cdot(0,v)\cdot(\cos\varphi, -v\sin\varphi) \\ &= \big(-\sin\varphi, v\cos\varphi\big)\cdot(\cos\varphi, -v\sin\varphi) \\ &= \big(-\cos\varphi\sin\varphi + \cos\varphi\sin\varphi, v\sin^2\varphi + v\cos^2\varphi\big) = (0,v)\ , \end{aligned}$$

da $\cos^2\varphi + \sin^2\varphi = 1$. Auch die Drehung $R_{v,2\varphi}$ hält v fest, es gilt also $F_q v = v = R_{v,2\varphi} v$.

Es gelte jetzt $\langle v, w\rangle = 0$ und $\|w\| = 1$. Wegen $\langle v \times w, v\rangle = 0$ und der Graßmann-Identität gilt in diesem Fall

$$\begin{aligned} qw\bar{q} &= (\cos\varphi, v\sin\varphi)\cdot(0,w)\cdot(\cos\varphi, -v\sin\varphi) \\ &= \big(0, w\cos\varphi + v\times w\sin\varphi\big)\cdot(\cos\varphi, -v\sin\varphi) \\ &= \big(0, w\cos^2\varphi + v\times w\cos\varphi\sin\varphi - w\times v\cos\varphi\sin\varphi - (v\times w)\times v\sin^2\varphi\big) \\ &= \big(0, w(\cos^2\varphi - \sin^2\varphi) + v\times w\cdot 2\cos\varphi\sin\varphi\big)\ . \end{aligned}$$

Cosinus und Sinus des doppelten Winkels berechnen sich als

$$\cos(2\varphi) = \cos^2\varphi - \sin^2\varphi \qquad \text{und} \qquad \sin(2\varphi) = 2\cos\varphi\sin\varphi\ .$$

Wenn wir $\|w\|$ annehmen, dann folgt aus Bemerkung 1.69, dass die Vektoren v, w und $v \times w$ aufeinander sekrecht stehen, und dass auch

$$\|v\times w\| = \|v\| \times \|w\| \times \sin\measuredangle(v,w) = 1\ .$$

Insbesondere bilden w und $v \times w$ eine Orthonormalbasis der zu v senkrechten Ebene. Die Drehung $R_{v,2\varphi}$ bildet den Vektor w also ab auf

$$R_{v,2\varphi} w = \cos(2\varphi)\, w + \sin(2\varphi)\, v\times w = F_q w\ . \qquad \square$$

1.75. Bemerkung. Die Isometrien des Raumes werden erzeugt von

(1) Verschiebungen $w \mapsto u + w$ mit $u \in \mathbb{R}^3$,
(2) Drehungen um die Achse durch den Ursprung in Richung v mit Winkel φ, also $w \mapsto F_q w$, wobei jetzt

$$q = \cos\frac{\varphi}{2} + v\,\sin\frac{\varphi}{2}\ ,$$

(3) Die Punktspiegelung $w \mapsto -w$.

In Analogie zu Bemerkung 1.65 können wir also jede Isometrie schreiben als

$$F(w) = u + qw\bar{q} \qquad \text{oder} \qquad F(w) = u + q\bar{w}\bar{q}\ .$$

Dabei sind $u \in \operatorname{Im}\mathbb{H}$ und $q \in \mathbb{H}$ mit $|q| = 1$ durch F fast eindeutig festgelegt — man kann nur noch q durch $-q$ ersetzen. Dieses Phänomen nennt man „Spin“. Es hat sowohl in der Mathematik als auch in der Physik eine Bedeutung.

Die obige Darstellung hat zwei interessante Eigenschaften.

- Sei $G(w) = v + rw\bar{r}$ eine weitere Isometrie, dann hat auch die Verkettung $F \circ G$ die gleiche Form:
$$(F \circ G)(w) = u + q(v + rw\bar{r})\bar{q} = (u + qv\bar{q}) + qr\, w\, \overline{qr} \; .$$
- Anhand der obigen Formel kann man q leicht bestimmen, wenn man Drehachse und -winkel kennt. Umgekehrt man Drehachse und -winkel ablesen, wenn q bekannt ist.

Aufgrund dieser beiden Vorteile werden Quaternionen in der Praxis eingesetzt, zum Beispiel in der Robotersteuerung und in der dreidimensionalen Bildverarbeitung.

1.76. Bemerkung. Analog zu den Bemerkungen 1.65 und 1.75 können wir auch alle Isometrien des $\mathbb{R}^4$ beschreiben durch
$$F(w) = v + pw\bar{q} \qquad \text{oder} \qquad F(w) = v + p\bar{w}\bar{q} \; .$$
Hierbei ist $w \in \mathbb{R}^4 = \mathbb{H}$, und die Quaternionen v, p, $q \in \mathbb{H}$ mit $|p| = |q| = 1$ sind durch F fast eindeutig festgelegt — man darf nur das Paar (p, q) durch das Paar $(-p, -q)$ ersetzen. Es gibt also auch hier einen „Spin“. Der Zusammenhang zwischen dem Paar (z, w) und der Gestalt der Isometrie ist nicht so einfach zu erklären wie in Bemerkung 1.75.

Für $\mathbb{R}^n$ mit $n \geq 5$ gibt es leider keine so schönen Beschreibungen der Isometrien mehr. Wir werden im zweiten Semester sehen, wie man Isometrien generell durch Matrizen darstellen kann.

KAPITEL 2

Vektorräume und Moduln

In diesem Kapitel lernen wir mit Vektoren zu rechnen, indem wir Koordinaten angeben und lineare Abbildungen als Matrizen schreiben. Einem Vektor in Koordinaten entspricht ein Element in einem freien Modul, und einer Matrix entspricht eine lineare Abbildung zwischen freien Moduln. Anschließend überlegen wir uns, warum und wie Matrixrechnung funktioniert.

Für das Rechnen mit Matrizen reicht uns zunächst einmal ein Ring, obwohl wir später meistens einen Körper, zum Beispiel $\mathbb{R}$, zugrunde legen werden. Die etwas größere Allgemeinheit verursacht keinen zusätzlichen Aufwand; außerdem müssen wir später gelegentlich mit Matrizen über Ringen arbeiten. Die zahlreichen Vorteile, die die Arbeit über Körpern (auch Schiefkörpern) mit sich bringt, lernen wir dann im nächsten Kapitel kennen.

Als erstes führen wir ein paar algebraische Grundbegriffe ein: Vektoren sind Elemente von Vektorräumen über Körpern oder Schiefkörpern. Etwas allgemeiner ist der Begriff eines Moduls über einem Ring. Und sowohl Ringen als auch Moduln liegen abelsche Gruppen zugrunde, mit denen wir daher beginnen werden. Nachdem wir Moduln eingeführt haben, betrachten wir spezielle „strukturerhaltende“ Abbildungen. Zum Schluss konstruieren wir neue Moduln aus gegebenen und überlegen uns ihre Eigenschaften.

2.1. Gruppen, Ringe, Körper

Wir definieren eine Reihe wichtiger algebraischer Strukturen. Unser Hauptziel sind Körper. Aber auch Gruppen und Ringe werden uns noch häufiger begegnen.

2.1. Definition. Eine *Gruppe* $(G, *)$ ist eine Menge G mit einer Verknüpfung $*\colon G \times G \to G$, für die ein neutrales Element $e \in G$ und für alle $g \in G$ ein inverses Element $g^{-1} \in G$ existiert, so dass für alle g, h und k die folgenden Gruppenaxiome gelten:

(G1) $g * (h * k) = (g * h) * k$ (*Assoziativgesetz*),

(G2) $e * g = g$ (*linksneutrales Element*),

(G3) $g^{-1} * g = e$ (*linksinverse Elemente*).

Eine Gruppe heißt *kommutativ* oder *abelsch,* wenn außerdem für alle g, $h \in G$ gilt

(G4) $g * h = h * g$ (*Kommutativgesetz*).

2.2. Beispiel. Wir kennen schon Beispiele von abelschen Gruppen.

(1) Die ganzen Zahlen $\mathbb{Z}$ bilden eine abelsche Gruppe $(\mathbb{Z}, +)$, genannt die *unendliche zyklische Gruppe,* siehe auch Satz 1.47.
(2) Sei $\Bbbk = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ oder $\mathbb{H}$. Dann ist $(\Bbbk, +)$ eine abelsche Gruppe, die sogenannte *additive Gruppe* von $\Bbbk$, siehe dazu die Sätze 1.50, 1.56 und 1.71, sowie Punkt (1) am Anfang von Abschnitt 1.4.
(3) Die natürlichen Zahlen $\mathbb{N}$ bilden keine Gruppe, denn es fehlen die inversen Elemente, siehe Übung 3(b) von Blatt 2.

Die Gruppenaxiome sind bewusst sparsam formuliert. Dadurch hat man relativ wenig zu tun, um nachzuweisen, dass eine bestimmte Verknüpfung auf einer Menge eine Gruppe definiert. Beim Rechnen in Gruppen hilft die folgende Definition.

2.3. Proposition. *Sei $(G, *)$ eine Gruppe, dann sind das neutrale Element e und das Inverse g^{-1} zu jedem $g \in G$ eindeutig bestimmt. Außerdem gilt für alle $g \in G$, dass*

(G2') $$g * e = g \ ,$$

(G3') $$g * g^{-1} = e \ .$$

Insbesondere muss man das neutrale Element und die Abbildung, die einem Gruppenelement sein Inverses zuordnet, in der Notation „$(G, *)$“ nicht mit angeben, da beide eindeutig festgelegt sind. Das spart etwas Schreibarbeit. Und wir dürfen tatsächlich von neutralen und inversen Elementen reden, nicht von linksneutralen und linksinversen Elementen.

Beweis. Wir leiten aus den Gruppenaxiomen der Reihe nach einige interessante Rechenregeln ab. Für alle g, h, $k \in G$ gilt

(1) Linkskürzungsregel: aus $g * h = g * k$ folgt $h = k$, denn

$$\begin{aligned} h = e * h = (g^{-1} * g) * h = g^{-1} * (g * h) \\ = g^{-1} * (g * k) = (g^{-1} * g) * k = e * k = k \ . \end{aligned}$$

(2) Die Aussage (G2') folgt aus der Linkskürzungsregel (1) und

$$g^{-1} * (g * e) = (g^{-1} * g) * e = e * e = e = g^{-1} * g \ .$$

(3) Eindeutigkeit des neutralen Elements: Es gelte $f * g = g$ für alle $g \in G$, dann folgt insbesondere

$$f = f * e = e \ .$$

Umgekehrt gelte $g * f = g$ für alle $g \in G$, dann folgt ebenfalls

$$f = e * f = e \ .$$

(4) Aussage (G3') folgt aus der Linkskürzungsregel (1) und

$$g^{-1} * (g * g^{-1}) = (g^{-1} * g) * g^{-1} = e * g^{-1} = g^{-1} = g^{-1} * e \ .$$

(5) Rechtskürzungsregel: aus $h * g = k * g$ folgt $h = k$, denn

$$\begin{aligned} h = h * e = h * (g * g^{-1}) &= (h * g) * g^{-1} \\ &= (k * g) * g^{-1} = k * (g * g^{-1}) = k * e = k \,. \end{aligned}$$

(6) Eindeutigkeit des Inversen: aus $g * h = e$ folgt $h = g^{-1}$ wegen der Linkskürzungsregel (1) und

$$g * h = e = g * g^{-1} \,,$$

umgekehrt folgt $k = g^{-1}$ aus $k * g = e$ wegen der Rechtskürzungsregel (2) und

$$k * g = e = g^{-1} * g \,. \qquad \square$$

2.4. Bemerkung. Wir erinnern uns an die Verkettung „$\circ$“ von Abbildungen aus Definition 1.19, an die Identität id_M aus Beispiel 1.18 (1) und an die Umkehrabbildungen aus Satz 1.23.

(1) Es seien K, L, M, N Mengen und $F\colon M \to N$, $G\colon L \to M$ und $H\colon K \to L$ Abbildungen,

$$K \xrightarrow{H} L \xrightarrow{G} M \xrightarrow{F} N \,.$$

Dann gilt $F \circ (G \circ H) = (F \circ G) \circ H$, denn für alle $k \in K$ ist

$$\begin{aligned} (F \circ (G \circ H))(k) &= F((G \circ H)(k)) = F(G(H(k))) \\ &= (F \circ G)(H(k)) = ((F \circ G) \circ H)(k) \,. \end{aligned}$$

(2) Für $F\colon M \to N$ wie oben gilt $\mathrm{id}_N \circ F = F$, denn für alle $m \in M$ gilt

$$(\mathrm{id}_N \circ F)(m) = \mathrm{id}_N(F(m)) = F(m) \,.$$

(3) Es sei F bijektiv. Dann existiert eine Umkehrabbildung S nach Satz 1.23, und es gilt

$$S \circ F = \mathrm{id}_M \,.$$

Diese Beziehungen sehen fast so aus wie die Gruppenaxiome (G1)–(G3). Man sollte aber beachten, dass die Abbildungen F, G, H, id_M, id_N und S im Allgemeinen von verschiedenen Typen sind. Das heißt, wenn die Mengen K, L, M, N paarweise verschieden sind, gehören keine zwei dieser Abbildungen zur gleichen Grundmenge, etwa $F \in \mathrm{Abb}(M, N)$, $\mathrm{id}_M \in \mathrm{Abb}(M, M)$, und so weiter.

2.5. Beispiel. Es sei M eine Menge. Wir definieren die Menge der *Automorphismen* von M als

$$\mathrm{Aut}(M) = \big\{\, F\colon M \to M \;\big|\; F \text{ ist bijektiv} \,\big\} \,.$$

Dann bildet $(\mathrm{Aut}(M), \circ)$ eine Gruppe. Dazu überlegen wir uns

(1) Seien F und G bijektiv, dann ist $F \circ G$ bijektiv nach Satz 1.22 (3). Also ist die Verknüpfung „$\circ$“ auf $\mathrm{Aut}(M)$ wohldefiniert.
(2) Es gilt das Assoziativgesetz (G1) nach Bemerkung 2.4 (1).
(3) Die Identität id_M aus Beispiel 1.18 (1) ist bijektiv. Nach Bemerkung 2.4 (2) ist id_M das neutrale Element in $(\mathrm{Aut}(M), \circ)$.

(4) Das Inverse zu $F \in \mathrm{Aut}(M)$ ist die Umkehrabbildung G aus Satz 1.23. Aus Satz 1.22 (4) und (5) folgt, dass G wieder bijektiv ist, und das Axiom (G3) ist gerade Punkt (3) in Bemerkung 2.4.

Später werden wir häufiger Gruppen begegnen, die aus speziellen bijektiven Abbildungen F einer Menge M in sich bestehen.

2.6. Definition. Ein *Ring* $(R, +, \cdot)$ ist eine Menge R mit zwei Verknüpfungen $+,\ \cdot : R \times R \to R$, so dass $(R, +)$ eine abelsche Gruppe bildet, und so dass für alle $r,\ s,\ t \in R$ die folgenden Ringaxiome gelten:

(R1) $$(r \cdot s) \cdot t = r \cdot (s \cdot t) \qquad (\textit{Assoziativgesetz}),$$

(R2) $$\begin{cases} r \cdot (s + t) = r \cdot s + r \cdot t \\ (r + s) \cdot t = r \cdot t + s \cdot t \end{cases} \qquad (\textit{Distributivgesetze}).$$

Ein Ring heißt *unitär* oder *Ring mit Eins,* wenn es ein neutrales Element 1_R gibt, so dass für alle $r \in R$ gilt:

(R3) $$1_R \cdot r = r \cdot 1_R = r \qquad (\textit{multiplikatives neutrales Element}).$$

Ein Ring heißt *kommutativ,* wenn für alle $r,\ s \in R$ gilt:

(R4) $$r \cdot s = s \cdot r \qquad (\textit{Kommutativgesetz}).$$

Man beachte, dass die Axiome (R3) und (R4) unabhängig voneinander erfüllt sein können. Wir werden in dieser Vorlesung fast nur Ringe mit Eins betrachten.

In allgemeinen Ringen haben wir kein Kommutativgesetz und auch keine Links- oder Rechtskürzungsregeln für die Multiplikation, da uns die multiplikativen Inversen fehlen. Aus diesem Grund brauchen wir beide Gleichungen in (R2) und (R3).

Die Gruppe $(R, +)$ heißt die additive Gruppe des Rings $(R, +, \cdot)$. Ihr neutrales Element wird mit 0 oder 0_R bezeichnet, und das additive Inverse von $r \in R$ wird $-r$ geschrieben. Die Bezeichnung r^{-1} ist für multiplikative Inverse reserviert (wenn sie existieren). Das Symbol für die Multiplikation wird häufig weggelassen, somit steht rs kurz für $r \cdot s$.

2.7. Beispiel. Wir kennen bereits einige Ringe.

(1) Die ganzen Zahlen $(\mathbb{Z}, +, \cdot)$ bilden einen kommutative Ring mit Eins, siehe Satz 1.47.
(2) Sei $\Bbbk = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ oder $\mathbb{H}$. Dann ist $(\Bbbk, +, \cdot)$ ein Ring mit Eins; siehe dazu die Sätze 1.50, 1.56 und 1.71, sowie Punkt (1) am Anfang von Abschnitt 1.4. Bis auf $\mathbb{H}$ sind diese Ringe auch kommutativ.
(3) Auf den natürlichen Zahlen $\mathbb{N}$ sind zwar Addition und Multiplikation erklärt, und (R1)–(R4) gelten. Aber da $(\mathbb{N}, +)$ keine Gruppe ist, ist $(\mathbb{N}, +, \cdot)$ kein Ring, siehe Beispiel 2.2 (3).

Auch aus den Ringaxiomen lassen sich Folgerungen ziehen.

2.8. Proposition. *Es sei $(R, +, \cdot)$ ein Ring. Dann gilt für alle r, $s \in R$, dass*

$$0_R \cdot r = r \cdot 0_R = 0_R \,, \tag{1}$$

$$r \cdot (-s) = (-r) \cdot s = -r \cdot s \,. \tag{2}$$

In einem Ring mit Eins ist die Eins eindeutig, und es gilt entweder $0_R \neq 1_R$, oder aber $R = \{0_R\}$.

Aufgrund der letzten Aussage wird bei einem Ring mit Eins manchmal zusätzlich $0_R \neq 1_R$ gefordert.

Beweis. Aus dem Distributivgesetz (R2) folgt

$$0_R \cdot r = (0_R + 0_R) \cdot r = 0_R \cdot r + 0_R \cdot r \,,$$

also $0_R = 0_R \cdot r$ nach der Kürzungsregel für die Addition. Genauso folgt $r \cdot 0_R = 0_R$.

Aussage (2) folgt aus

$$0_R = r \cdot 0_R = r \cdot (s + (-s)) = r \cdot s + r \cdot (-s) \,,$$

genauso erhält man die zweite Gleichung.

Die Eindeutigkeit der Eins folgt wie in Proposition 2.3.

Wenn in einem Ring mit Eins $0_R = 1_R$ gilt, folgt aus (R3) und (1) für alle $r \in R$, dass

$$r = 1_R \cdot r = 0_R \cdot r = 0_R \,. \qquad \square$$

Der Ring $R = \{0\}$ heißt auch *Nullring* oder „trivialer Ring“.

2.9. Beispiel. Sei $n \in \mathbb{N}$, $n \geq 1$. Wir definieren eine Relation „$\equiv \bmod n$“ auf $\mathbb{Z}$ durch

$$a \equiv b \mod n \qquad \Longleftrightarrow \qquad \text{es gibt } k \in \mathbb{Z} \text{ mit } a - b = kn \,,$$

lies: „a ist kongruent zu b modulo n“.

Wir wollen zeigen, dass es sich um eine Äquivalenzrelation handelt. Die Relation is reflexiv (Ä1), denn $a - a = 0 \cdot n$ für alle $a \in \mathbb{Z}$. Für a, $b \in \mathbb{Z}$ gelte $a - b = kn$ mit $k \in \mathbb{Z}$, dann folgt $b - a = (-k) \cdot n$, also ist die Relation symmetrisch (Ä2). Schließlich ist sie auch transitiv (Ä3), denn gelte $a - b = kn$ und $b - c = \ell n$ für a, b, c, k, $\ell \in \mathbb{Z}$, dann folgt $a - c = (\ell + k) \cdot n$.

Die Äquivalenzklasse von $a \in \mathbb{Z}$ heißt *Restklasse von a* und hat die Form

$$[a] = \{\, a + k \cdot n \mid k \in \mathbb{Z} \,\} = \{\ldots, a - n, a, a + n, \ldots\} \,.$$

Der Quotient heißt *Menge der Restklassen modulo n* und wird mit $\mathbb{Z}/n$ oder $\mathbb{Z}/n\mathbb{Z}$ bezeichnet. Indem wir $a \in \mathbb{Z}$ mit Rest durch n dividieren, erhalten wir b, $k \in \mathbb{Z}$ mit $0 \leq b < n$, so dass $a = kn + b$. Es folgt

$$\mathbb{Z}/n = \big\{[0], \ldots, [n-1]\big\} \,,$$

insbesondere hat $\mathbb{Z}/n$ die Mächtigkeit n.

Analog zu Abschnitt 1.3 wollen wir zeigen, dass Addition und Multiplikation in $\mathbb{Z}$ auf dem Quotienten $\mathbb{Z}/n$ wohldefinierte Rechenoperationen definieren. Es sei etwa $a - b = kn$ und $c - d = \ell n$, dann folgt

$$\begin{aligned} (a+c) - (b+d) &= (k+\ell) \cdot n \,, \\ (a \cdot c) - (b \cdot d) &= (a-b) \cdot c + b \cdot (c-d) = (kc + b\ell) \cdot n \\ \text{und} \qquad (-a) - (-b) &= (-k) \cdot n \,. \end{aligned}$$

Somit erhalten wir Verknüpfungen $+,\ \cdot : (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \to \mathbb{Z}/n\mathbb{Z}$ sowie $- \cdot : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ mit

$$[a] + [c] = [a+c] \,, \qquad [a] \cdot [c] = [a \cdot c] \qquad \text{und} \qquad -[a] = [-a] \,.$$

Schließlich wollen wir die Axiome (G1)–(G4) und (R1)–(R4) überprüfen, um zu zeigen, dass $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ein kommutativer Ring mit Eins ist. Dazu setzen mit $0_{\mathbb{Z}/n\mathbb{Z}} = [0]$ und $1_{\mathbb{Z}/n\mathbb{Z}} = [1]$. Jetzt folgt jedes einzelne der obigen Axiome aus der entsprechenden Rechenregel für $(\mathbb{Z}, +, \cdot)$, zum Beispiel

$$\begin{aligned} ([a] + [b]) + [c] &= [a+b] + [c] = [(a+b)+c] \\ &= [a + (b+c)] = [a] + [b+c] = [a] + ([b] + [c]) \,, \\ [a] \cdot ([b] + [c]) &= [a] \cdot [b+c] = [a \cdot (b+c)] \\ &= [ab + ac] = [ab] + [ac] = [a] \cdot [b] + [a] \cdot [c] \\ \text{und} \qquad [1] \cdot [a] &= [1 \cdot a] = [a] = [a \cdot 1] = [a] \cdot [1] \,. \end{aligned}$$

Somit ist $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ein kommutativer Ring mit Eins. Seine additive Gruppe $(\mathbb{Z}/n\mathbb{Z}, +)$ heißt auch die *zyklische Gruppe der Ordnung n.*

2.10. Definition. Ein *Schiefkörper* $(K, +, \cdot)$ ist ein Ring mit Eins 1_K und additivem neutralem Element 0_K, in dem für alle $k \in K \setminus \{0_K\}$ ein multiplikatives Inverses k^{-1} existiert, so dass für alle $k \in K \setminus \{0_K\}$ die folgenden Körperaxiome gelten:

(K1) $\quad k^{-1} \cdot k = 1_K \quad$ (*multiplikatives linksinverses Element*),

(K2) $\quad 1_K \neq 0_K \quad$ (*Nichttrivialität*).

Ein Schiefkörper heißt *Körper,* wenn der zugrundeliegende Ring kommutativ ist.

2.11. Beispiel. Wir kennen bereits einige Körper und Schiefkörper.

(1) Es sei $\mathbb{k} = \mathbb{Q}$, $\mathbb{R}$ oder $\mathbb{C}$, dann ist $(\mathbb{k}, +, \cdot)$ ein Körper, siehe dazu die Sätze 1.50, 1.56 sowie Punkt (1) am Anfang von Abschnitt 1.4. Insbesondere sind $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ auch Schiefkörper.
(2) Die Quaternionen bilden einen "echten", also nichtkommutativen Schiefkörper, siehe Satz 1.71.
(3) Die natürlichen Zahlen $(\mathbb{N}, +, \cdot)$ sind kein (Schief-) Körper, da sie noch nicht einmal einen Ring bilden. Die ganzen Zahlen $(\mathbb{Z}, +, \cdot)$ sind zwar ein kommutativer Ring mit Eins, aber kein (Schief-) Körper, da multiplikative Inverse fehlen.

Die Körperaxiome werden in der Literatur oft unterschiedlich formuliert. Manchmal fasst man (G1)–(G4), (R1)–(R4), (K1) und (K2) (oder kleine Variationen davon) zu Axiomen (K1)–(K10) zusammen. Es folgt eine weitere Möglichkeit.

2.12. Proposition. *Eine Menge K mit Verknüpfungen $+,\ \cdot : K \times K \to K$ und Elementen $0_K,\ 1_K \in K$ bildet genau dann einen Schiefkörper $(K, +, \cdot)$, wenn*

(1) *$(K, +)$ eine Gruppe bildet,*
(2) *$(K \setminus \{0_K\}, \cdot)$ eine Gruppe bildet, und*
(3) *die Distributivgesetze* (R2) *gelten.*

Falls die Gruppe $(K \setminus \{0_K\}, \cdot)$ abelsch ist, ist $(K, +, \cdot)$ ein Körper.

Beweis. $\Longrightarrow$: Sei $(K, +, \cdot)$ ein Körper, dann ist $(K, +)$ nach den Definitionen 2.6 und 2.10 eine abelsche Gruppe. Auch die Distributivgesetze (R2) haben wir vorausgesetzt, somit gelten (1) und (3).

Zu (2) betrachte $a,\ b \neq 0_K$. Es gilt $a^{-1} \neq 0$, denn ansonsten wäre

$$1_K = a^{-1} \cdot a = 0_K$$

nach Proposition 2.8 (1), im Widerspruch zu (K2). Es gilt auch $a \cdot b \neq 0_K$, denn sonst wäre

$$b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = 0_K$$

nach Proposition 2.8 (1). Somit definiert die Multiplikation eine Verknüpfung auf der Menge $K \setminus \{0_K\}$, und auch 1_K und die Inversen a^{-1} liegen in $K \setminus \{0_K\}$. Die Gruppenaxiome für $(K \setminus \{0_K\}, \cdot)$ folgen jetzt aus (R1), (R3) und (K1).

$\Longleftarrow$: Wenn (1)–(3) erfüllt sind, gelten zunächst einmal (G1)–(G3) und (R2) wegen (1) und (3).

Es gilt $a + b = b + a$ sicher, falls $a = 0$ oder $b = 0$ (wegen (G2) und (G2')), oder falls $a + b = 0$ (wegen (G3) und (G3')). Ansonsten folgt aus dem Axiom (G2) für $(K \setminus \{0_K\}, \cdot)$ und den Distributivgesetzen, dass

$$\begin{aligned} a + a + b + b &= (1 + 1) \cdot a + (1 + 1) \cdot b = (1 + 1) \cdot (a + b) \\ &= 1 \cdot (a + b) + 1 \cdot (a + b) = a + b + a + b\,. \end{aligned}$$

Die Kürzungsregeln (1) und (5) aus dem Beweis von Proposition 2.3 liefern (G4).

Das Assoziativgesetz (R1) folgt aus (G1) für die Gruppe $(K \setminus \{0_K\}, \cdot)$, falls $r,\ s,\ t \in K \setminus \{0_K\}$. Falls mindestens eines der drei Elemente 0_K ist, sind rechte und linke Seite von (R1) auch 0_k wegen Proposition 2.8 (1) — dabei benutzen wir, dass wir im Beweis von Proposition 2.8 das Assoziativgesetz noch nicht benutzt haben. Genauso folgt (R3) aus (G2) und aus (G2') in Proposition 2.3 falls $r \neq 0_K$, und aus Proposition 2.8 (1), falls $r = 0_K$.

Das Axiom (K1) ist gerade (G1) für $(K \setminus \{0_K\}, \cdot)$, und (K2) folgt, da $1_K \in K \setminus \{0_K\}$. Also ist $(K, +, \cdot)$ ein Körper. □

Wir schreiben $K^\times = K \setminus \{0_K\}$ und nennen $(K^\times, \cdot)$ die *multiplikative Gruppe* von K. Manche Autoren schreiben auch K^*; wir wollen uns das Sternchen aber für andere Zwecke aufsparen.

2.13. Bemerkung. In jedem Körper oder Schiefkörper $(K, +, \cdot)$ gilt Proposition 2.3 für die additive Gruppe $(K, +)$ sowie für die multiplikative Gruppe $(K^\times, \cdot)$. Im Fall $(K^\times, \cdot)$ gelten manche der Aussagen in Proposition 2.3 und ihrem Beweis immer noch, wenn einzelne Elemente 0_K sind. Zur Begründung benutzen wir wieder Proposition 2.8 (1).

(1) *Kürzungsregeln:* Aus $a \cdot b = a \cdot c$ oder $b \cdot a = c \cdot a$ folgt $b = c$ oder $a = 0_K$, genau wie in Satz 1.40 (5).
(2) *Nullteilerfreiheit:* Aus $a \cdot b = 0_K$ folgt $a = 0_K$ oder $b = 0_K$. Das ist äquivalent zu (1).
(3) *neutrales Element:* Es gilt $1 \cdot a = a \cdot 1 = a$ für alle $a \in K$;
(4) *Eindeutigkeit der Eins:* aus $a \cdot b = a$ oder $b \cdot a = a$ für *ein* $a \in K^\times$ und ein $b \in K$ folgt $b = 1$;
(5) *Eindeutigkeit des Inversen:* aus $a \cdot b = 1$ oder $b \cdot a = 1$ für a, $b \in K$ folgt a, $b \in K^\times$ und $b = a^{-1}$.

Unter *Nullteilern* in einem Ring $(R, +, \cdot)$ versteht man Elemente r, $s \in R \setminus \{0\}$ mit $r \cdot s = 0$. Körper sind also *nullteilerfrei* nach (2). In Ringen kann es Nullteiler geben, zum Beispiel gilt

$$[2] \cdot [3] = [6] = [0] \qquad \in \mathbb{Z}/6\mathbb{Z} \, .$$

2.14. Definition. Sei R ein Ring mit Eins. Falls es eine Zahl $n \in \mathbb{N} \setminus \{0\}$ gibt mit

$$\underbrace{1_R + \cdots + 1_R}_{n \text{ Summanden}} = 0_R \, , \tag{*}$$

dann heißt die kleinste solche Zahl die *Charakteristik* $\chi(R)$ von R. Andernfalls ist $\chi(R) = 0$.

Man beachte, dass aus $\chi(R) = n$ bereits für alle $r \in R$ folgt:

$$\underbrace{r + \cdots + r}_{n \text{ Summanden}} = \underbrace{\big(1_R + \cdots + 1_R\big)}_{n \text{ Summanden}} \cdot r = 0 \, .$$

2.15. Beispiel. Für einige Ringe kennen wir die Charakteristik.

(1) Aus dem ersten Peano-Axiom 1.28 (1) folgt für alle $n \in \mathbb{N} \setminus \{0\}$, dass

$$\underbrace{1 + \cdots + 1}_{n \text{ Summanden}} = n \neq 0 \, .$$

Da $\mathbb{N}$ eine Teilmenge von $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ und $\mathbb{H}$ ist, folgt

$$\chi(\mathbb{Z}) = \chi(\mathbb{Q}) = \chi(\mathbb{R}) = \chi(\mathbb{C}) = \chi(\mathbb{H}) = 0 \, .$$

(2) Der Ring $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ aus Beispiel 2.9 hat Charakteristik $\chi(\mathbb{Z}/n\mathbb{Z}) = n$.

Aus der Schule kenne wir den Begriff der *Primzahl*. Es sei $1 \leq n \in \mathbb{N}$. Wir nennen $a \in \mathbb{N}$ einen *Teiler* von n, kurz $a \mid n$, wenn es $b \in \mathbb{N}$ mit $ab = n$ gibt. Eine Primzahl ist eine Zahl $p \in \mathbb{Z}$ mit $p > 1$, deren einzige Teiler 1 und p sind. Die Zahl 1 selbst ist keine Primzahl.

2.16. Proposition. *Die Charakteristik eines Körpers ist entweder* 0 *oder eine Primzahl.*

Beweis. Wir wollen annehmen, dass $\chi(K) \neq 0$. Aus (K2) folgt $1_K \neq 0_K$, also ist $\chi(K) \neq 1$. Falls jetzt $\chi(K) = a \cdot b$ mit a, $b > 1$ gilt, betrachte die Gleichung

$$0 = \underbrace{1_K + \cdots + 1_K}_{a \cdot b \text{ Summanden}} = (\underbrace{1_K + \cdots + 1_K}_{a \text{ Summanden}}) \cdot (\underbrace{1_K + \cdots + 1_K}_{b \text{ Summanden}}) .$$

Da K als Körper nullteilerfrei ist, muss bereits einer der beiden Faktoren oben 0_K sein. Ohne Einschränkung dürfen wir annehmen, dass es sich um den ersten handelt (ansonsten vertausche a und b). Nun ist aber $a < a \cdot b$ da $1 < b$, und gleichzeitig ist $a \cdot b$ nach Definition 2.14 die kleinste Zahl mit der Eigenschaft (*). Aufgrund dieses Widerspruchs kann $\chi(K)$ kein echtes Produkt sein. □

2.17. Beispiel. Der Ring $\mathbb{Z}/n\mathbb{Z}$ aus Beispiel 2.9 kann also nur ein Körper sein wenn n also eine Primzahl ist.

Sei also p eine Primzahl und $K = \mathbb{Z}/p\mathbb{Z}$. Wir wissen schon, dass $\mathbb{Z}/p\mathbb{Z}$ ein kommutativer Ring mit Eins $[1] \neq [0]$ ist. Wir wollen noch die Existenz multiplikativer Inverser beweisen (K1). Jedes Element $[a] \in \mathbb{Z}/p \setminus \{[0]\}$ hat genau p verschiedene Vielfache in $\mathbb{Z}/p\mathbb{Z}$, denn sonst gäbe es $[b]$, $[c] \in \mathbb{Z}/p$ mit $[b] \neq [c]$ aber $[a] \cdot [b] = [a] \cdot [c]$, also $a \cdot (b - c) = k \cdot p$ für ein $k \in \mathbb{Z}$, aber weder a noch $b - c$ enthalten den Primteiler p, Widerspruch. Also ist die Abbildung $F \colon \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ mit $F([b]) = [a][b]$ injektiv, und daher auch surjektiv (Übung), somit existiert $[b]\mathbb{Z}/p\mathbb{Z}$ mit $[a][b] = [1]$, das heißt, $[a]$ hat ein multiplikatives Inverses.

Man kann (K1) auch expliziter beweisen, indem man ein Inverses angibt. Sei dazu $1 \leq a < p$, dann gibt es keine Zahl $c > 1$, die a und p teilt. Nach Satz 2.18 (2) unten für $a_0 = p > a_1 = a$ existieren Zahlen d_0 und $d_1 \in \mathbb{Z}$ mit

$$1 = d_1 a_0 + d_0 a_1 = d_1 p + d_0 a .$$

Dann ist $d_0 a \equiv 1$ modulo p, also ist $[d_0] = [a]^{-1} \in \mathbb{Z}/p\mathbb{Z}$ das multiplikative Inverse von $[a]$.

Für den folgenden Satz brauchen wir *Division mit Rest:* Zu je zwei Zahlen m, $n \in \mathbb{N}$ mit $n \neq 0$ gibt es eindeutige Zahlen q, $r \in \mathbb{N}$ mit $0 \leq r < n$, so dass

$$m = qn + r .$$

2.18. Satz (Euklidischer Algorithmus)**.** *Es seien* a_0, $a_1 \in \mathbb{N} \setminus \{0\}$ *mit* $a_1 \leq a_0$, *Dann existieren eindeutige Zahlen* $i_0 \in \mathbb{N}$, $a_1 > a_2 > \cdots > a_{i_0} > a_{i_0+1} = 0$ *und* $b_2, \ldots, b_{i_0+1} \in \mathbb{N}$, *so dass*

$$a_{i-1} = b_{i+1}a_i + a_{i+1} \qquad \text{für alle } 1 \leq i \leq i_0 \,. \tag{1}$$

Die Zahl a_{i_0} *ist die größte Zahl in* $\mathbb{N}$, *die* a_0 *und* a_1 *teilt.*

Setze $d_{i_0+1} = 1$, $d_{i_0} = 0$ *und bestimme* $d_{i_0-1}, \ldots, d_1, d_0 \in \mathbb{Z}$ *so, dass*

$$d_{i-1} = d_{i+1} - d_i b_{i+1} \qquad \text{für } i_0 \geq i \geq 1 \,. \tag{2}$$

Dann gilt $a_{i_0} = d_1 a_0 + d_0 a_1$.

Die Zahl a_{i_0} heißt der *größte gemeinsame Teiler* von a_0 und a_1, kurz $a_{i_0} = \mathrm{ggT}(a_0, a_1)$.

Beweis. Nach Definition der Division mit Rest existieren die Zahlen a_i und b_i, sind eindeutig bestimmt durch (1) und werden immer kleiner. Also erreichen wir $a_{i_0+1} = 0$ nach $i_0 \leq a_1$ vielen Schritten.

Es sei $0 < c \in \mathbb{N}$ eine Zahl, die a_0 und a_1 teilt, dann teilt c auch alle Zahlen $a_2, \ldots, a_{i_0}$ wegen (1). Also kann es keine Zahl größer als a_{i_0} geben, die a_0 und a_1 teilt. Aus (1) für i_0 folgt, dass a_{i_0} auch a_{i_0-1} teilt. Indem wir (1) für immer kleinere i benutzen, folgt, dass a_{i_0} auch $a_{i_0-2}, \ldots, a_1$ und a_0 teilt. Also ist $a_{i_0} = \mathrm{ggT}(a_0, a_1)$.

Seien jetzt d_i wie in (2) gegeben. Betrachte die Gleichung

$$a_{i_0} = d_{i+1}a_i + d_i a_{i+1} \,. \tag{3}$$

Wegen $a_{i_0+1} = 0$ und $d_{i_0+1} = 1$ gilt (3) für $i = i_0$. Aus den Gleichungen (1)–(3) für i erhalten wir

$$\begin{aligned} a_{i_0} &= d_{i+1}a_i + d_i(a_{i-1} - b_{i+1}a_i) \\ &= d_i a_{i-1} + (d_{i+1} - d_i b_{i+1})a_i = d_i a_{i-1} + d_{i-1}a_i \,. \end{aligned}$$

Also gilt (3) auch für $i - 1$. Für $i = 0$ erhalten wir die Behauptung. □

2.19. Bemerkung. Es gibt einen Körper mit n Elementen genau dann, wenn sich $n = p^a$ schreiben lässt, wobei p eine Primzahl ist und $a \geq 1$. Dieser Körper wird F_{p^a} genannt und hat die Charakteristik p. Sie lernen ihn in der Algebra-Vorlesung kennen. Es gibt auch Körper mit Charakteristik p und unendlich vielen Elementen.

Wir sollten in der linearen Algebra immer von Augen haben, dass es diese endlichen Körper gibt; insbesondere Körper der Charakteristik 2 erfordern ein wenig zusätzliche Aufmerksamkeit.

2.2. Moduln und Vektorräume

Gruppen, Ringe und Körper begegnen uns oft dadurch, dass sie auf anderen Strukturen "operieren". Uns interessiert hier zunächst der Fall von Ring- und Körperoperationen; Gruppenoperationen lernen wir später auch noch kennen.

2.20. Definition. Sei $(R, +, \cdot)$ ein Ring. Ein (*Rechts-*) *R-Modul* $(M, +, .)$ besteht aus einer abelschen Gruppe $(M, +)$ und einer *skalaren Multiplikation* $. : M \times R \to M$, so dass für alle $m, n \in M$ und alle $r, s \in R$ die folgenden Modulaxiome gelten

(M1) $m . (r \cdot s) = (m . r) . s$ (*Assoziativgesetz*),

(M2) $m . (r + s) = m . r + m . s$ (*Erstes Distributivgesetz*),

(M3) $(m + n) . r = m . r + n . r$ (*Zweites Distributivgesetz*).

Sei $(R, +, \cdot)$ ein Ring mit Eins 1. Ein *unitärer* (*Rechts-*) *R-Modul* $(M, +, .)$ ist ein Rechtsmodul $(M, +, .)$, so dass zusätzlich gilt:

(M4) $m . 1 = m$ (*Wirkung der Eins*).

Ist der Ring $R = K$ ein Schiefkörper oder Körper, so heißen unitäre Rechts-K-Moduln auch (*Rechts-*) *K-Vektorräume* oder (*Rechts-*) *Vektorräume über K*.

Man beachte, dass das Symbol „+" in (M2) zwei verschiedene Bedeutungen hat. Die Punkte für die Multiplikation kann man oft weglassen. Wir sprechen von Rechts-R-Moduln, weil R durch skalare Multiplikation „von rechts" auf M wirkt. Analog definiert man Links-R-Moduln mit einer skalaren Multiplikation $\cdot : R \times M \to M$. In diesem Fall dreht sich in (M1)–(M4) jeweils die Reihenfolge der Faktoren um, beispielsweise würde (M1) zu

$$(r \cdot s) \cdot m = r \cdot (s \cdot m) .$$

2.21. Beispiel. Wir können einige Moduln und Vektorräume angeben.

(1) $(R, +, .)$ ist ein Rechts-R-Modul, wobei "+" und "." die gleichen Verknüpfungen sind wie in R, jedoch aufgefasst als $+ : M \times M \to M$ und $. : M \times R \to M$. Nach Definition 2.6 ist nämlich $(R, +)$ eine abelsche Gruppe, (R1) liefert (M1), und die Distributivgesetze (R2) liefern (M2) und (M3). Falls R eine Eins 1 besitzt, ist M auch unitär, denn (M4) folgt dann aus (R3). Völlig analog kann man R zu einem Linksmodul machen.

(2) Der „kleinste" Rechts-R-Modul ist $(\{0\}, +, .)$ mit $0 . r = 0$ für alle $r \in R$. Er heißt der *Nullmodul*.

(3) Jede abelsche Gruppe A wird zu einem Rechts R-Modul mit $a . r = 0_A$ für alle $a \in A$ und alle $r \in R$. Damit reduzieren sich (M1)–(M3) zur trivialen Aussage $0_A = 0_A$. Dieser Modul ist allerdings nicht unitär, es sei denn, er wäre bereits der Nullmodul aus (2).

(4) Die Vektorräume $\mathbb{R}^n$, speziell $\mathbb{R}^2$ und $\mathbb{R}^3$ aus den Abschnitten 1.4–1.6 sind Vektorräume über $\mathbb{R}$.

(5) In der Analysis lernen Sie viele $\mathbb{R}$-Vektorräume kennen. So sind die Räume der Folgen und der Nullfolgen mit Werten in $\mathbb{R}$ Vektorräume über $\mathbb{R}$. Auch die Räume der stetigen oder der differenzierbaren Funktionen auf einem Intervall $I \subset \mathbb{R}$ sind $\mathbb{R}$-Vektorräume.

2.22. Proposition. *Es sei $(M, +, .)$ ein $(R, +, \cdot)$-Rechtsmodul. Dann gilt für alle $m \in M$ und $r \in R$, dass*

$$0_M \,.\, r = m \,.\, 0_R = 0_M \,, \tag{1}$$

$$m \,.\, (-s) = (-m) \,.\, s = -m \cdot s \,. \tag{2}$$

Analoge Aussagen gelten für Linksmoduln.

Beweis. All das folgt aus den Distributivgesetzen (M2), (M3) wie im Beweis von Proposition 2.8. □

2.23. Bemerkung. Sei $(R, +, \cdot)$ ein kommutativer Ring, zum Beispiel ein Körper. Dann kann man aus jedem Rechts-R-Modul $(M, +, .)$ einen Links-R-Modul $(M, +, \cdot)$ machen und umgekehrt, indem man $r \cdot m = m \,.\, r$ für alle $r \in R$ und $m \in M$ setzt. Das einzige fragliche Axiom ist (M1), und wir rechnen nach, dass

$$s \cdot (r \cdot m) = (m \,.\, r) \,.\, s = m \,.\, (r \cdot s) = (r \cdot s) \cdot m = (s \cdot r) \cdot m$$

für alle $r, s \in R$ und $m \in M$. Wir dürfen in diesem Fall also einfach von *Moduln* reden.

Da wir im letzten Schritt das Kommutativgesetz (R4) benutzt haben, zeigt diese Rechnung aber auch, dass wir über einem nicht kommutativen Ring genau zwischen Links- und Rechtsmoduln unterscheiden müssen.

Abbildung 1 gibt einen Überblick über die bis jetzt definierten algebraischen Strukturen. Der Übersicht halber haben wir nicht-unitäre Moduln von (Schief-) Körpern und Ringen mit Eins weggelassen.

Es sei $(A, +)$ eine abelsche Gruppe, $n \in \mathbb{N}$, und $a_1, \ldots, a_n \in A$. Wir setzen $s_0 = 0$ und definieren induktiv

$$s_i = s_{i-1} + a_i \in A \qquad \text{für } i = 1, \ldots, n \,.$$

Dann ist die *Summe der a_n für i von 1 bis n* definiert als

$$\sum_{i=1}^{n} a_i = s_n = a_1 + \cdots + a_n \in A \,.$$

Allgemeiner sei I eine Menge. Unter einer *Familie in A mit Indexmenge I* verstehen wir eine Abbildung $a\colon I \to A$, geschrieben $(a_i)_{i \in I}$, mit $i \mapsto a_i$. Wir schreiben $A^I = \mathrm{Abb}(I, A)$ für die Menge aller Familien. Beispielsweise ist eine *Folge* in A gerade eine Familie mit Indexmenge $\mathbb{N}$, und $\mathbb{R}^{\mathbb{N}}$ ist die Menge der reellwertigen Folgen. Wir sagen $a_i = 0$ *für fast alle* $i \in I$, wenn nur endlich viele $i \in I$ nicht auf 0_A abgebildet werden, das heißt, wenn die Menge

$$J = \{\, i \in I \mid a_i \neq 0 \,\}$$

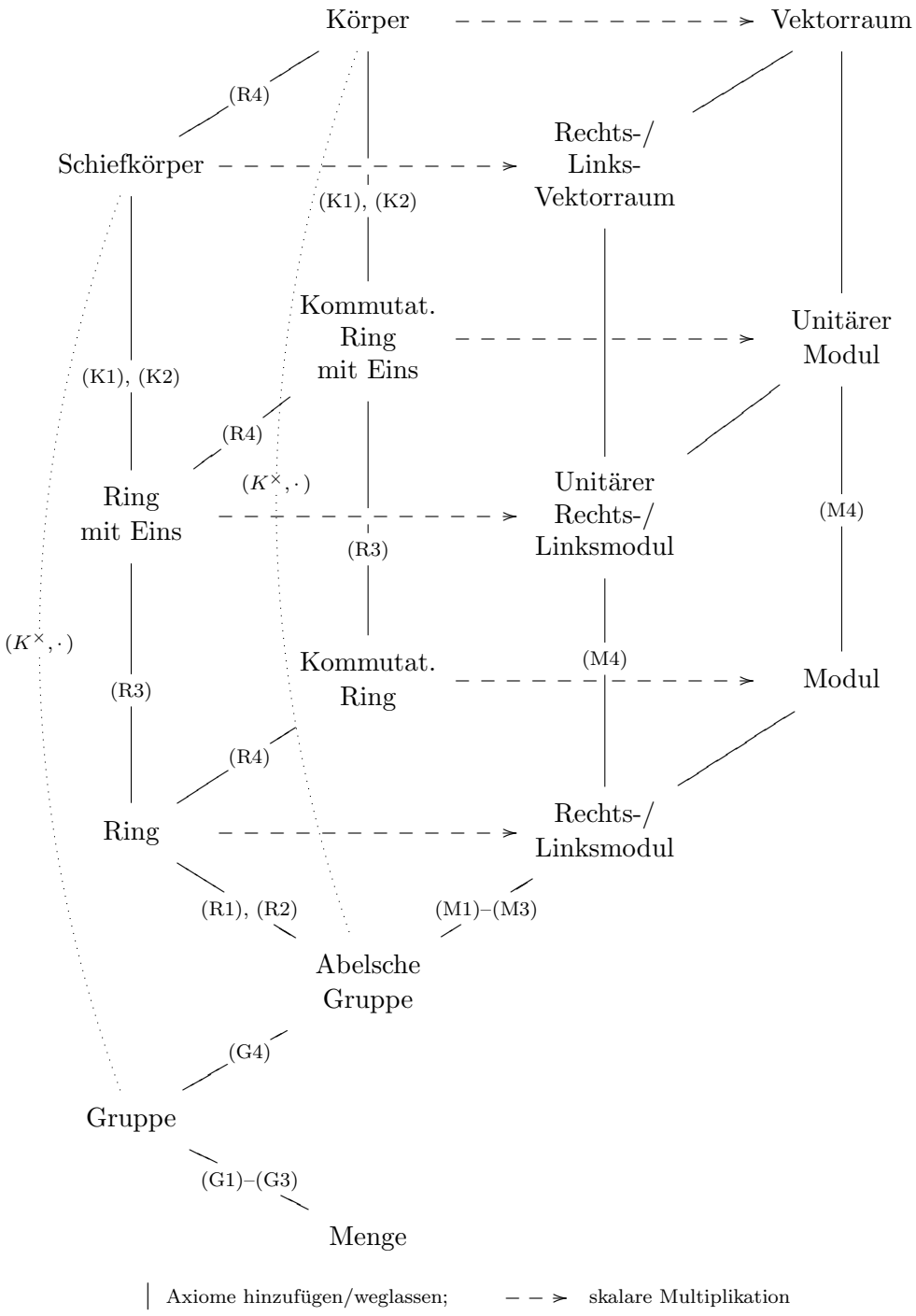


ABBILDUNG 1. Strukturen aus den Abschnitten 2.1 und 2.2

endlich ist. Dann sei $i\colon \{1,\dots,\#J\} \to J$ eine bijektive Abbildung und

$$\sum_{i\in I} a_i = s_n = \sum_{j=1}^{\#J} a_{i(j)} \in A\ .$$

Somit ist $\sum_{i\in I} a_i$ die (endliche) *Summe* derjenigen a_i mit $i \in I$, die von 0_A verschieden sind. Wegen des Kommutativgesetzes (G4) für die Addition in R kommt es dabei nicht auf Reihenfolge der Summation an. Das Ergebnis hängt also nicht von der Wahl der Abbildung i ab. Wir lesen „Summe der a_i für $i \in I$."

Obwohl wir unendliche Indexmengen erlauben, betrachten wir in Wirklichkeit nur endliche Summen, da wir verlangen, dass fast alle Summanden 0_A sind. Man beachte den Unterschied zur Analysis, wo auch gewisse unendliche Summen erlaubt sind.

2.24. Definition. Sei M ein Rechts-R-Modul, und sei $E \subset M$ eine Teilmenge. Sei $(r_e)_{e\in E} \in R^E$, so dass $r_e = 0_R$ für fast alle $e \in E$, dann heißt

$$\sum_{e\in E} e\,.\,r_e \qquad \in M$$

eine *Linearkombination* der $e \in E$. Ein Element $m \in M$ heißt *als Linearkomination der $e \in E$ darstellbar,* wenn es $(r_e)_{e\in E} \in R^E$ mit 0_R für fast alle $e \in E$ gibt, so dass $m = \sum_{e\in E} e\,.\,r_e$. Das *Erzeugnis* von E (*über R*) ist die Menge

$$\langle\, E\,\rangle = \left\{ \sum_{e\in E} e\,.\,r_e \;\middle|\; r_e \in R \text{ mit } r_e = 0_R \text{ für fast alle } e \in E \right\}.$$

Falls $M = \langle\, E\,\rangle$, heißt E eine *Erzeugermenge* von M, und E *erzeugt* M (*über R*). Falls es eine endliche Menge E gibt, die M erzeugt, heißt M *endlich erzeugt* (*über R*).

Hier haben wir immer die Summe der Familie $(e\,.\,r_e)_{e\in E}$ gebildet. Beachte also: falls E endlich ist, dürfen wir jede beliebige Familie $(r_e)_{e\in E}$ in R zur Bildung einer Linearkombination heranziehen. Falls E unendlich ist, müssen wir $r_e = 0$ für fast alle $e \in E$ fordern, damit die Summe endlich bleibt.

Das Erzeugnis einer Menge E wird manchmal auch mit $\operatorname{span}(E)$ bezeichnet.

2.25. Bemerkung. Linearkombinationen werden uns regelmäßig begegnen. Zum Beispiel haben wir im Beweis der Cauchy-Schwarz-Ungleichung 1.53 eine Linearkombination $y - (\langle x, y\rangle / \|x\|^2)\, x$ der Vektoren x und y betrachtet, die senkrecht auf x steht. Im Beweis von Satz 1.74 haben wir einen Vektor $w \in \mathbb{R}^3$ mit $\langle v, w\rangle = 0$ um die Achse durch v gedreht und das Ergebnis als Linearkombination der Vektoren w und $v \times w$ geschrieben.

2.26. Beispiel. Es sei R ein Ring mit Eins, und es sei M ein (Rechts-) R-Modul. Dann ist die zugrundeliegende Menge M selbst immer eine Erzeugermenge, denn

$$m = m\,.\,1 = \sum_{n\in M} n\,.\,\delta_{mn}\ .$$

Hierbei ist das *Kronecker-Symbol* δ definiert durch

$$\delta_{ij} = \begin{cases} 1_R & \text{falls } i = j, \text{ und} \\ 0_R & \text{sonst,} \end{cases}$$

insbesondere ist $\delta_{mn} = 0_R$ für fast alle $n \in M$.

2.27. Beispiel. Als Vektorraum über $\mathbb{C}$ wird $\mathbb{C}$ selbst erzeugt von der Menge $\{1\}$. Wir können $\mathbb{C} \cong \mathbb{R}^2$ aber auch als Vektorraum über $\mathbb{R}$ auffassen. Dann erzeugt $\{1\}$ über R nur die Teilmenge $\mathbb{R} \subset \mathbb{C}$, während $\{1, i\}$ eine Erzeugermenge über $\mathbb{R}$ ist. Aus diesem Grund ist es manchmal sinnvoll, den zugrundeliegenden Ring oder Körper mit anzugeben.

Noch schlimmer wird es, wenn wir $\mathbb{C}$ als Vektorraum über $\mathbb{Q}$ auffassen. Da $\mathbb{Q}$ abzählbar ist und $\mathbb{R}$ und $\mathbb{C}$ überabzählbar sind, ist $\mathbb{C}$ über $\mathbb{R}$ endlich erzeugt, aber nicht über $\mathbb{Q}$.

2.28. Definition. Es sei M ein Rechts-R-Modul und $E \subset M$. Falls

$$0_M = \sum_{e \in E} e \,.\, r_e \qquad \Longrightarrow \qquad r_e = 0_R \text{ für alle } e \in E$$

für alle Familien $(r_e)_{e \in E} \in R^E$ gilt, bei denen $r_e = 0$ für fast alle $e \in E$, dann heißt E *linear unabhängig.* Andernfalls heißt E *linear abhängig.*

Sei M ein Rechts-R-Modul. Eine (*ungeordnete*) *Basis* von M ist eine linear unabhängige Erzeugermenge $E \subset M$ von M. Ein Rechts-R-Modul M heißt *frei* (*über* R), wenn er eine Basis besitzt.

2.29. Beispiel. Es sei $n \geq 1$. Wir können $M = \mathbb{Z}/n\mathbb{Z}$ als unitären $\mathbb{Z}$-Modul auffassen. Dazu definieren wir eine skalare Multiplikation durch $[a] \,.\, r = [ar]$ für alle $a, r \in \mathbb{Z}$. Mit analogen Überlegungen wie in Beispiel 2.9 folgt, dass das wohldefiniert ist, und dass die Modulaxiome gelten.

Für alle $[a] \in \mathbb{Z}/n\mathbb{Z}$ gilt $[a] \,.\, n = [an] = [0]$, also ist jede nichtleere Teilmenge $E \subset \mathbb{Z}/n\mathbb{Z}$ linear abhängig. Genauer: sei $f = [a] \in E$, dann wähle $(r_e)_{e \in E} = (\delta_{ef} \cdot n)_{e \in E}$; es folgt

$$\sum_{e \in E} e \,.\, (\delta_{ef} \cdot n) = [a] \,.\, n = [0] \,,$$

da der Faktor δ_{ef} in einer Summe über e nach Definition des Kronecker-Symbols nur den Summanden mit $e = f$ übriglässt.

Auf der anderen Seite erzeugt die leere Menge den Modul $\mathbb{Z}/n\mathbb{Z}$ nur dann, wenn $n = 1$. Somit ist $\mathbb{Z}/n\mathbb{Z}$ nicht frei über $\mathbb{Z}$, wenn $n > 1$.

Allerdings ist $M = \mathbb{Z}/n\mathbb{Z}$ ein freier Modul über dem Ring $R = \mathbb{Z}/n\mathbb{Z}$ mit Basis $E = \{[1]\}$, denn E erzeugt M. Aus $[0] = [1] \,.\, r$ folgt $r = [0]$, da $[1]$ gleichzeitig das Einselement von R ist. Also ist E aus linear unabhängig über R. Aus diesem Grund empfiehlt es sich auch bei linearer Abhängigkeit, im Zweifelsfall den Grundring mit anzugeben.

2.30. Beispiel. Es sei I eine Menge und R ein Ring mit Eins. Wir definieren einen Rechts-R-Modul $R^{(I)}$ durch

$$\begin{aligned} R^{(I)} &= \left\{ (r_i)_{i\in I} \in R^I \;\middle|\; r_i = 0 \text{ für fast alle } i \in I \right\} , \\ (r_i)_{i\in I} + (s_i)_{i\in I} &= (r_i + s_i)_{i\in I} && \text{für alle } (r_i)_{i\in I},\, (s_i)_{i\in I} \in R^{(I)} , \\ (r_i)_{i\in I} \,.\, s &= (r_i \cdot s)_{i\in I} && \text{für alle } (r_i)_{i\in I} \in R^{(I)},\, s \in R \,. \end{aligned}$$

Addition und skalare Multiplikation nehmen wieder Werte in $R^{(I)}$ an: seien etwa $(r_i)_{i\in I}$, $(s_i)_{i\in I}$ wie oben, dann gibt es nur endlich viele Indizes $i \in I$, an denen $r_i \neq 0$ oder $s_i \neq 0$ gilt; an allen anderen Stellen gilt $r_i + s_i = 0_R$. Das neutrale Element ist die Familie $0_{R^{(I)}} = (0_R)_{i\in I}$, die an allen $i \in I$ den Wert 0_R hat. Jetzt lassen sich die Modulaxiome (M1)–(M3) leicht überprüfen. Wenn R ein Ring mit Eins ist, ist $R^{(I)}$ sogar unitär, das heißt, es gilt auch (M4).

Ab jetzt nehmen wir an, dass R ein Ring mit Eins ist. Für alle $j \in I$ sei

$$e_j = (\delta_{ij})_{i\in I} \in R^{(I)} \tag{1}$$

die Familie, die genau an der Stelle $j \in I$ den Wert 1_R hat, und sonst überall 0_R. Dann ist die Teilmenge

$$E = \left\{ e_j \in R^{(I)} \;\middle|\; j \in I \right\} \subset R^{(I)} .$$

eine Erzeugermenge, denn für alle $(r_i)_{i\in I} \in R^{(I)}$ gilt

$$\sum_{i\in I} e_i \,.\, r_i = \sum_{j\in I} e_j \,.\, r_j = \sum_{j\in I} (\delta_{ij})_{i\in I} \,.\, r_i = \left(\sum_{j\in I} \delta_{ij} \cdot r_j \right)_{i\in I} = (r_i)_{i\in I} \,. \tag{2}$$

Außerdem ist $r_i = 0$ für fast alle $i \in I$ nach Definition von $R^{(I)}$, so dass wir die obigen Summen bilden dürfen.

Die Teilmenge E ist auch *linear unabhängig,* denn sei

$$\sum_{j\in I} e_j \,.\, r_j = 0_{R^{(I)}} = (0_R)_{i\in I} \,,$$

dann folgt

$$\left(\sum_{j\in I} \delta_{ij} \cdot r_j \right)_{i\in I} = (0_R)_{i\in I} \,,$$

also ergibt jede einzelne Summe den Wert 0_R. Nach Definition von δ_{ij} folgt für den i-ten Eintrag, dass

$$0_R = \sum_{j\in I} \delta_{ij} \cdot r_j = r_i \,.$$

Da das für alle $i \in I$ gelten muss, gilt $r_i = 0$ für alle i, und somit ist E linear unabhängig.

Der Modul $R^{(I)}$ heißt auch der *von I erzeugte freie Rechts-R-Modul.* Er ist frei mit der *Standardbasis* E, und man beachte, dass jedem $i \in I$ genau ein Basiselement e_i entspricht. Mitunter identifiziert man i und e_i, schreibt also

$$(r_{i\in I})_{i\in I} = \sum_{i\in I} i \,.\, r_i \,;$$

das geht aber nur, wenn dadurch keine Misverständnisse entstehen.

Eine analoge Konstruktion liefert den von I erzeugten freien Links-R-Modul ${}^{(I)}R$; nach Bemerkung 2.23 dürfen wir beide identifizieren, falls R kommutativ ist.

Man beachte den Unterschied zwischen R^I und $R^{(I)}$. Beispielsweise ist $\mathbb{R}^{\mathbb{N}}$ der Vektorraum aller reellwertigen Folgen, während $\mathbb{R}^{(\mathbb{N})}$ nur diejenigen Folgen enthält, bei denen ab einer bestimmten Stelle alle Einträge 0 sind. Insbesondere ist die Menge $\{\,(\delta_{mn})_{n\in\mathbb{N}} \mid m \in \mathbb{N}\,\}$ der Folgen, bei denen genau ein Eintrag 1 und alle anderen 0 sind, nur eine Basis von $\mathbb{R}^{(\mathbb{N})}$, nicht vom Raum aller Folgen $\mathbb{R}^{\mathbb{N}}$. Man kann sogar zeigen, dass eine Basis von $\mathbb{R}^{\mathbb{N}}$ überabzählbar viele Elemente haben muss.

2.31. Beispiel. Wir betrachten den Spezialfall $I = \{1, \dots, n\}$ für $n \in \mathbb{N}$. In diesem Fall schreiben wir R^n für $R^{(I)}$, und stellen die Elemente als Spalten dar:

$$\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} = (r_i)_{i\in I} = (r_i)_{i=1,\dots,n} \quad \in \quad R^n = R^{(I)} \,.$$

Die Rechenoperationen sind dann gegeben durch

$$\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} + \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} = \begin{pmatrix} r_1 + s_1 \\ \vdots \\ r_n + s_n \end{pmatrix} \qquad \text{und} \qquad \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} . s = \begin{pmatrix} r_1 \cdot s \\ \vdots \\ r_n \cdot s \end{pmatrix} \,.$$

Die Basis $\{e_1, \dots, e_n\}$ heißt *Standardbasis* des R^n und besteht aus den *Standardbasisvektoren*

$$e_1 = \begin{pmatrix} 1_R \\ 0_R \\ \vdots \\ 0_R \end{pmatrix} , \dots , e_n = \begin{pmatrix} 0_R \\ \vdots \\ 0_R \\ 1_R \end{pmatrix} \,.$$

Der Vektor e_j hat also als j-ten Eintrag die 1_R, und sonst überall 0_R. Natürlich gilt

$$\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} = \begin{pmatrix} 1_R \\ 0_R \\ \vdots \\ 0_R \end{pmatrix} . r_1 + \dots + \begin{pmatrix} 0_R \\ \vdots \\ 0_R \\ 1_R \end{pmatrix} . r_n \,.$$

Analog schreiben wir ${}^{n}R$ für den freien Links-R-Modul ${}^{(I)}R$ und stellen die Elemente als Zeilen dar:

$$(r_1, \dots, r_n) = (r_i)_{i\in I} = (r_i)_{i=1,\dots,n} \quad \in \quad {}^{n}R = {}^{(I)}R \,.$$

Als Standardbasisvektoren erhalten wir entsprechend

$$\varepsilon_1 = (1, 0, \dots, 0) \,, \dots , \varepsilon_n = (0, \dots, 0, 1) \,.$$

In diesem Fall ist

$$(r_1, \dots, r_n) = r_1 \cdot (1, 0, \dots, 0) + \dots + r_n \cdot (0, \dots, 0, 1) \,.$$

2.32. Proposition. *Es sei M ein freier Rechts-R-Modul mit Basis B. Dann existiert zu jedem $m \in M$ genau eine Familie $(m_b)_{b\in B} \in R^B$ mit $m_b = 0_R$ für fast alle $b \in B$, so dass*

$$\sum_{b\in B} b \,.\, m_b = m \,. \tag{1}$$

Ein analoges Resultat gilt für freie Links-R-Moduln.

Beweis. Da B eine Basis ist, erzeugt B den Modul M. Also existiert eine Familie $(m_b)_{b\in B} \in R^B$ mit der Eigenschaft (1).

Sei jetzt $(n_b)_{b\in B} \in R^B$ eine weitere Familie mit $n_b = 0_R$ für fast alle $b \in B$, so dass

$$\sum_{b\in B} b \,.\, n_b = m \,.$$

Dann folgt

$$0_M = m - m = \sum_{b\in B} b \,.\, n_b - \sum_{b\in B} b \,.\, m_b = \sum_{b\in B} b \,.\, (n_b - m_b) \,,$$

und es gilt $n_b - m_b = 0_R$ für fast alle $b \in B$. Da B linear unabhängig ist, folgt $n_b - m_b = 0_R$ für alle $b \in B$. Also gilt $(m_b)_{b\in B} = (n_b)_{b\in B}$, das heißt, die Familie $(m_b)_{b\in B}$ ist auch eindeutig. □

Das bedeutet, dass wir mit Hilfe einer Basis ein beliebiges Element in einem freien Modul ersetzen können durch eine Ansammlung von Ringelementen. Das ist insbesondere zum Rechnen sehr hilfreich.

2.33. Definition. Es sei M ein freier Rechts-R-Modul mit Basis B, und es sei $m \in M$. Dann heißen die $(m_b)_{b\in B}$ in R aus Proposition 2.32 die *Koordinaten* von m bezüglich der Basis B. Die Abbildung $M \to R^{(B)}$ mit $m \mapsto (m_b)_{b\in B}$ heißt die *Koordinatenabbildung* zur Basis B. Umgekehrt ist die *Basisabbildung* von M zur Basis B die Abbildung $R^{(B)} \to M$ mit

$$(r_b)_{b\in B} \longmapsto \sum_{b\in B} b \,.\, r_b \,.$$

2.34. Bemerkung. Nach Proposition 2.32 ist die Basisabbildung bijektiv. Ihre Umkehrabbildung ist die Koordinatenabbildung.

2.3. Lineare Abbildungen

2.35. Definition. Sei $(R, +, \cdot)$ ein Ring und seien $(M, +, \cdot)$ und $(N, +, \cdot)$ Rechts-R-Moduln, dann heißt eine Abbildung $F\colon M \to N$ ein (*Rechts-R-*) *Modulhomomorphismus* oder (*rechts-*) *R-linear* (kurz: *linear*), falls für alle ℓ, $m \in M$ und alle $r \in R$ gilt

(L1) $\quad F(\ell + m) = F(\ell) + F(m) \qquad$ (*Additivität*),

(L2) $\quad F(m \,.\, r) = F(m) \,.\, r \qquad$ (*Homogenität*).

Falls R ein (Schief-) Körper ist, nennt man lineare Abbildungen zwischen (Rechts-R-) Vektorräumen auch *Vektorraumhomomorphismen.* Die Menge aller (rechts-) R-linearer Abbildungen von M nach N wird mit $\mathrm{Hom}_R(M,N)$ bezeichnet. Analog definieren wir *Links-R-Modulhomomorphismen.* Die Menge aller Links-R-Modulhomomorphismen von A nach B wird mit ${}_R\mathrm{Hom}(M,N)$ bezeichnet.

Für lineare Abbildungen gilt wegen Proposition 2.22 (1) insbesondere immer

$$F(0_M) = F(0_M \,.\, 0_R) = F(0_M) \,.\, 0_R = 0_N \,.$$

Wir bemerken, dass die Addition in (L1) einmal in M und einmal in N stattfindet. Genauso wird in (L2) einmal in M und einmal in N skalar multipliziert. Aus diesem Grund ist es wichtig, dass beide Moduln über demselben Ring R definiert sind. Wenn R kommutativ ist, gibt es nach Bemerkung 2.23 keinen Unterschied zwischen Links- und Rechts-R-Moduln. Wir sprechen dann nur noch von Modulhomomorphismen, und schreiben $\mathrm{Hom}(M,N)$ oder $\mathrm{Hom}_R(M,N)$ für die Menge aller linearer Abbildungen.

2.36. Beispiel. Wir kennen bereits Beispiele linearer Abbildungen.

(1) Wir haben bereits in den Abschnitten 1.5 und 1.6 benutzt (aber noch nicht bewiesen), dass Isometrien des $\mathbb{R}^2$ und des $\mathbb{R}^3$, die den Nullpunkt festhalten, $\mathbb{R}$-linear sind. Dazu gehören Drehungen um den Nullpunkt und Spiegelungen an Achsen durch den Nullpunkt im $\mathbb{R}^2$, siehe Bemerkung 1.65, sowie Drehungen um Achsen durch den Nullpunkt, die Punktspiegelung am Ursprung, sowie Spiegelungen an Ebenen durch den Nullpunkte im $\mathbb{R}^3$, siehe Bemerkung 1.75.

(2) Wir betrachten $M = N = \mathbb{C}$ zunächst als Modul über $\mathbb{C}$. Die komplexe Konjugation entspricht der Spiegelung an der reellen Achse. Wir überprüfen die Axiome (L1), (L2). Nach Bemerkung 1.60 gilt

$$\overline{z+w} = \overline{z} + \overline{w} \qquad \text{und} \qquad \overline{z \,.\, w} = \overline{z} \,.\, \overline{w} \,.$$

Also ist komplexe Konjugation additiv, aber nicht homogen, da im allgemeinen $w \neq \overline{w}$. Wenn wir aber $\mathbb{C}$ als $\mathbb{R}$-Modul auffassen, dann gilt auch (L2), da $w = \overline{w}$ genau dann, wenn $w \in \mathbb{R}$. Also kommt es auch bei Linearität auf den zugrundeliegenden Ring oder (Schief-) körper an.

(3) Sei $M = \mathbb{H}$ ein Rechts-$\mathbb{H}$-Vektorraum wie in Beispiel 2.21 (1), so dass $m \,.\, q = mq$ für $m \in M$, $q \in \mathbb{H}$. Es sei $f\colon M \to M$ rechts $\mathbb{H}$-linear und $p = f(1)$. dann folgt

$$f(m) = f(1 \,.\, m) = f(1) \,.\, m = pm \,,$$

also wird f durch Linksmultiplikation mit $p = f(1)$ gegeben. Umgekehrt ist Linksmultiplikation mit einem beliebigen Quaternion eine rechts-$\mathbb{H}$-lineare Abbildung.

(4) Sei $(M, +, \cdot\,)$ ein Links-$\mathbb{H}$-Vektorraum. Wir konstruieren daraus einen Rechts-$\mathbb{H}$-Vektorraum $(M, +, .\,)$ (und umgekehrt), so dass $m \,.\, q = \overline{q} \cdot m$

für alle $m \in M$ und $q \in \mathbb{H}$. Das Axiom (M1) ist erfüllt, denn wegen Satz 1.71 (6) gilt

$$m \,.\, (q \cdot r) = \overline{q \cdot r} \cdot m = \overline{r} \cdot \overline{q} \cdot m = (\overline{q} \cdot m) \,.\, r = (m \,.\, q) \,.\, r$$

für alle $m \in M$ und q, $r \in H$. Die anderen Modulaxiome lassen sich ebenso leicht nachprüfen.

Wir fassen jetzt $N = \mathbb{H}$ als Links-$\mathbb{H}$-Vektorraum auf und betrachten außerdem $M = \mathbb{H}$ wie in (3). Dann ist die Quaternionen-Konjugation $F = \overline{\cdot}\colon \overline{N} \to M$ rechts-$\mathbb{H}$-linear, denn

$$F(n \,.\, q) = F(\overline{q} \cdot n) = \overline{\overline{q} \cdot n} = \overline{n} \cdot \overline{\overline{q}} = \overline{n} \cdot q = F(n) \,.\, q \,.$$

2.37. Bemerkung. Auch in der Analysis spielen lineare Abbildungen eine wichtige Rolle. Beispielsweise dient die Ableitung einer Funktion $f\colon I \to \mathbb{R}$ auf einem offenen Intervall $I \subset \mathbb{R}$ dazu, die Funktion an einer Stelle $x_0 \in I$ zu beschreiben als

$$f(x) = f(x_0) + f'(x_0) \cdot (x - x_0) + o(x - x_0) \,, \tag{1}$$

dabei ist der zweite Term linear in $x - x_0$, und der Rest $o(x - x_0)$ geht für $x \to x_0$ schneller gegen 0 als jede lineare Funktion in $x - x_0$ außer der konstanten Funktion 0. Viele wichtige Eigenschaften von f lassen sich bereits von der „Linearisierung“ $f(x_0) + f'(x_0) \cdot (x - x_0)$ ablesen: wenn $f'(x_0) \neq 0$ ist, ist x_0 keine lokale Extremstelle von f, und f besitzt sogar lokal eine differenzierbare Umkehrfunktion.

Eine Funktion $f\colon U \to \mathbb{R}^m$ auf einer offenen Teilmenge $U \subset \mathbb{R}^n$ nähert man wieder wie in (1) an, dabei ist diesmal $f'(x_0)\colon \mathbb{R}^n \to \mathbb{R}^m$ selbst eine lineare Abbildung. Im Fall $m = 1$ folgt aus $f'(x_0) \neq 0$ wieder, dass x_0 keine lokale Extremstelle von f ist. Im Fall $m = n$ hat f genau dann eine differenzierbare lokale Umkehrfunktion, wenn $f'(x_0)$ als lineare Abbildung invertierbar ist. Ist $f'(x_0)$ injektiv, so ist das Bild der Einschränkung von f auf eine kleine Umgebung von x_0 eine „glatte“ Teilmenge des $\mathbb{R}^m$. Ist $f'(x_0)$ surjektiv, so ist das Urbild $f^{-1}\big(\{f(x_0)\}\big)$ nahe x_0 eine „glatte“ Teilmenge des $\mathbb{R}^n$.

Als Beispiel betrachten wir zwei Funktionen $f\colon \mathbb{R} \to \mathbb{R}^2$ und $F\colon \mathbb{R}^2 \to \mathbb{R}$ mit

$$f(t) = \begin{pmatrix} t^3 \\ t^2 \end{pmatrix} \qquad \text{und} \qquad F\left(\begin{pmatrix} x \\ y \end{pmatrix}\right) = x^2 - y^3 \,.$$

Dann ist $f'(t) = \binom{3y^2}{2t}\colon \mathbb{R} \to \mathbb{R}^2$ injektiv außer an der Stelle $t = 0$, und $F'\big(\binom{x}{y}\big) = (2x, -3y^2)\colon \mathbb{R}^2 \to \mathbb{R}$ ist surjektiv außer an der Stelle $\binom{x}{y} = 0$. Die Teilmenge

$$\operatorname{im} f = F^{-1}(\{0\}) \subset \mathbb{R}^2$$

ist glatt außer an der Stelle $\binom{0}{0} = f(0)$, wo die Ableitungen verschwinden.

Auch aufgrund dieser späteren Anwendungen lohnt es sich, lineare Abbildungen und ihre Eigenschaften genauer zu studieren.

2.38. Beispiel. Es sei M, N Rechts-R-Moduln. Dann sind die folgenden Abbildungen immer R-linear.

(1) Die Identität aus Beispiel 1.18 (1) ist immer linear, denn
$$\begin{aligned} \mathrm{id}_M(\ell + m) &= \ell + m = \mathrm{id}_M(\ell) + \mathrm{id}_M(m) \ , \\ \text{und} \quad \mathrm{id}_M(m \,.\, r) &= m \,.\, r = \mathrm{id}_M(m) \,.\, r \ . \end{aligned}$$

(2) Die *Nullabbildung* $0\colon M \to N$ mit $0(m) = 0_N$ für alle $m \in M$ ist ebenfalls linear, denn
$$\begin{aligned} 0(\ell + m) &= 0_N = 0_N + 0_N = 0(\ell) + 0(m) \ , \\ \text{und} \quad 0(m \,.\, r) &= 0_N = 0_N \,.\, r = 0(m) \,.\, r \ . \end{aligned}$$

2.39. Bemerkung. Es sei I eine Menge und N ein Rechts-R-Modul, dann wird auch $N^I = \mathrm{Abb}(I, N)$ zu einem Rechts-R-Modul mit den Rechenoperationen
$$(F + G)(i) = F(i) + G(i) \qquad \text{und} \qquad (F \,.\, r)(i) = F(i) \,.\, r \qquad \in N \ .$$
Auf diese Weise erhält man beispielsweise auch den Vektorraum $\mathbb{R}^{\mathbb{N}}$ der reellwertigen Folgen. Für die folgende Konstruktion ist wichtig, dass man Abbildungen mit Werten in einem Modul addieren kann, indem man die Bilder addiert.

2.40. Proposition. *Die Hintereinanderausführung von linearen Abbildungen ist linear. Die Umkehrabbildung einer bijektiven linearen Abbildung ist linear. Die Summe linearer Abbildungen ist linear.*

Beweis. Seien L, M und N Rechts-R-Moduln, und seien $F\colon M \to N$ und $G\colon L \to M$ R-linear. Dann folgt aus der Linearität von F und G für alle ℓ, $m \in L$ und alle $r \in R$, dass
$$\begin{aligned} (F \circ G)(\ell + m) &= F\big(G(\ell + m)\big) = F\big(G(\ell) + G(m)\big) \\ &= F\big(G(\ell)\big) + F\big(G(m)\big) = (F \circ G)(\ell) + (F \circ G)(m) \ , \\ \text{und} \quad (F \circ G)(\ell \,.\, r) &= F\big(G(\ell \,.\, r)\big) = F\big(G(\ell) \,.\, r\big) \\ &= F\big(G(\ell)\big) \,.\, r = (F \circ G)(\ell) \,.\, r \ . \end{aligned}$$
Also ist auch $F \circ G$ linear.

Sei jetzt $F\colon M \to N$ eine bijektive lineare Abbildung und $G\colon N \to M$ ihre Umkehrabbildung, siehe Satz 1.23. Es seien p, $q \in N$ beliebig und $\ell = G(p)$, $m = G(q) \in M$, so dass $F(\ell) = p$ und $G(m) = q$. Außerdem sei $r \in R$. Aus der Linearität von F folgt
$$\begin{aligned} G(p + q) &= G\big(F(\ell) + F(m)\big) = G\big(F(\ell + m)\big) = \ell + m = G(p) + G(q) \ , \\ \text{und} \quad G(q \,.\, r) &= G\big(F(m) \,.\, r\big) = G\big(F(m \,.\, r)\big) = m \,.\, r = G(q) \,.\, r \ . \end{aligned}$$
Also ist die Umkehrabbildung G linear.

Seien jetzt F, $G\colon M \to N$ linear, dann ist auch $F + G$ linear, denn für alle ℓ, $m \in M$ und alle $r \in R$ gilt
$$\begin{aligned} (F + G)(\ell + m) &= F(\ell + m) + G(\ell + m) = F(\ell) + F(m) + G(\ell) + G(m) \\ &= (F + G)(\ell) + (F + G)(m) \ , \\ (F + G)(m \,.\, r) &= F(m \,.\, r) + G(m \,.\, r) = F(m) \,.\, r + G(m) \,.\, r \\ &= (F + G)(m) \,.\, r \ . \end{aligned}$$
□

Achtung: im allgemeinen ist das Vielfache einer linearen Abbildung nicht linear. Betrachte dazu $F\colon M \to N$, $m \in M$ und r, s$\in R$.

$$(F\,.\,r)(m\,.\,s) = F(m\,.\,s)\,.\,r = F(m)\,.\,s\,.\,r\,, (F\,.\,r)(m)\,.\,s \quad = F(m)\,.\,r\,.\,s\,.$$

Diese beiden Ausdrücke sind im allgemeinen verschieden.

2.41. Definition. Es seien M, N Rechts-R-Moduln. Bijektive lineare Abbildungen $F\colon M \to N$ heißen (*Rechts-R-*) *Modulisomorphismen.* Lineare Abbildungen $F\colon M \to M$ heißen (*Rechts-R-*) *Modulendomorphismen,* und wenn sie bijektiv sind, (*Rechts-R-*) *Modulautomorphismen.* Falls R ein Körper ist, sprechen wir von *Vektorraumiso-, -endo- und -automorphismen.* Die Menge aller Modul- oder Vektorraumisomorphismen von M nach N wird mit $\mathrm{Iso}_R(M,N) \subset \mathrm{Hom}_R(M,N)$ bezeichnet, die Menge aller Modul- oder Vektorraumendo- oder -automorphismen von M mit $\mathrm{End}_R(M)$ beziehungsweise $\mathrm{Aut}_R M \subset \mathrm{End}_R M$. Analoge Bezeichnungen ${}_R\mathrm{Iso}(M,N)$, ${}_R\mathrm{End}\,M$ und ${}_R\mathrm{Aut}\,M$ führen wir für Links-R-Moduln oder -Vektorräume ein.

Bei Aut_R und End_R lässt man gelegentlich die Klammern weg, es ist also $\mathrm{End}_R M = \mathrm{End}_R(M)$. Analoge Bezeichnungen (Hom, End, Iso und Aut) werden in der Mathematik häufig für Abbildungen benutzt, die eine bestimmte „Struktur“ (hier die eines Moduls beziehungsweise Vektorraums) erhalten.

2.42. Folgerung (aus Prop2.40)**.** *Es sei R ein Ring, und M und N seien Rechts-R-Moduln.*

(1) *Die Automorphismen von M bilden eine Gruppe* $(\mathrm{Aut}_R M, \circ)$*, die* Automorphismengruppe *von M.*
(2) *Die Endomorphismen von M bilden einen Ring* $(\mathrm{End}_R M, +, \circ)$ *mit Eins* id_M*, den* Endomorphismenring *von M.*
(3) *Der Modul M ist ein Links-*$\mathrm{End}_R M$*-Modul, die skalare Multiplikation wirkt für alle $F \in \mathrm{End}_R M$ und alle $m \in M$ durch $F \cdot m = F(m) \in M$.*
(4) *Die Homomorphismen* $\mathrm{Hom}_R(M,N)$ *bilden einen unitären Recht-*$\mathrm{End}_R M$*-Modul, und einen unitären Links-*$\mathrm{End}_R N$*-Modul.*

Analoge Aussagen gelten, wenn M und N Links-R-Moduln sind.

Beweis. Der Beweis von (1) orientiert sich am Beispiel 2.5 der Automorphismengruppe einer Menge. Zunächst einmal ist die Verknüpfung zweier Automorphismen ein Automorphismus nach Proposition 2.40, genauso wie die Umkehrabbildung eines Automorphismus. Nach Beispiel 2.38 (1) ist auch die Identität ein Automorphismus. Die Gruppenaxiome ergeben sich wieder aus Bemerkung 2.4 (1)–(3).

Die Addition auf $\mathrm{End}_R(M)$ in (2) ist die gleiche wie in Bemerkung (2.39), Man überprüft leicht die Axiome (G1)-(G4). Aus Bemerkung 2.4 (1) und (2) folgen (R1), (R3). Als nächstes seien F, G, $H \in \mathrm{End}_R(M)$, dann gilt

$$(*) \quad (F+G)\circ H = F\circ H + G\circ H \quad \text{und} \quad F\circ(H+K) = F\circ H + F\circ K\,,$$

wie man durch Einsetzen von $m \in M$ leicht überprüft. Es folgt (R2) in (2). Also bildet $(\mathrm{End}_R M, +, \circ)$ einen Ring mit Eins $1_{\mathrm{End}_R M} = \mathrm{id}_M$.

Da M ein Rechts-R-Modul ist, ist $(M, +)$ eine abelsche Gruppe. Das Axiom (M1) für Linksmoduln folgt aus der Definition 1.19 der Verkettung, denn $(F \circ G)(m) = F(G(m))$ für alle F, $G \in \mathrm{End}_R(M)$ und alle $m \in M$. Axiom (M2) ist die Definition der Addition auf $\mathrm{End}_R(M)$ in Bemerkung (2.39), und (M3) ist gerade die Additivität (L1) der Endomorphismen. Schließlich ist M unitär, da die Eins in $\mathrm{End}_R M$ gerade id_M ist.

Es sei $F \in \mathrm{Hom}_R(M, N)$, $G \in \mathrm{End}_R M$ und $H \in \mathrm{End}_R M$. Dann folgt

$$F \circ G \in \mathrm{Hom}_R(M, N) \qquad \text{und} \qquad H \circ F \in \mathrm{Hom}_R(M, N)\ .$$

Also wirkt $\mathrm{End}_R M$ von rechts und $\mathrm{End}_R N$ von links auf $\mathrm{Hom}_R(M, N)$. Der Beweis von (4) funktioniert danach im wesentlichen genauso wie der von (2). Beispielsweise zeigt man die Distributivgesetze (M2), (M3) genau wie in (*), und (M1), (M4) folgen aus Bemerkung 2.4 (1) und (2). □

Wir betrachten $\mathrm{Hom}_R(M, R)$ als Spezialfall von (4), so dass $N = R$ als Rechts-R-Modul wie in Beispiel 2.21 (1). Dann ist $\mathrm{Hom}_R(M, R)$ ein Links-$\mathrm{End}_R R$-Modul. Für alle $r \in R$ ist Linksmultiplikation mit r rechts-R-linear, denn

$$r \cdot (s + t) = r \cdot s + r \cdot t \qquad \text{und} \qquad r \cdot (s\,.\,t) = (r \cdot s)\,.\,t$$

für alle s, $t \in R$. Also gilt $R \subset \mathrm{End}_R R$. Wenn R unitär ist, dann folgt wie in Beispiel (2.36) (3) sogar $\mathrm{End}_R R = R$. In jedem Fall können wir $\mathrm{Hom}_R(M, R)$ als Links-R-Modul auffassen.

2.43. Definition. Sei M ein Rechts-R-Modul, dann ist $M^* = \mathrm{Hom}_R(M, R)$ der zu M *duale* Links-R-Modul, beziehungsweise der zu M duale Links-R-Vektorraum, falls R ein (Schief-) Körper ist. Analog definieren wir den dualen Rechts R=Modul ${}^*N$ zu einem Links-R-Modul N.

Sie lernen einige duale Moduln in den Übungen kennen.

2.4. Unterräume und Quotienten

In diesem Abschnitt lernen wir, wie man aus gegebenen Moduln neue konstruieren kann.

2.44. Definition. Es sei $(M, +, .)$ ein Rechts-R-Modul und $U \subset M$ eine Teilmenge. Dann heißt U ein (*Rechts-R-*) *Untermodul,* falls für alle u, $v \in U$ und alle $r \in R$ die folgenden Untermodulaxiome gelten:

(U1) $\quad 0_M \in U \qquad\qquad$ (*Neutrales Element*) ,

(U2) $\quad u + v \in U\ , \quad -u \in U \quad$ (*abgeschlossen unter Addition*) ,

(U3) $\quad u\,.\,r \in U \qquad\qquad$ (*abgeschlossen unter skalarer Multiplikation*) .

Analog definieren wir Links-R-Untermoduln von Links-R-Moduln. Falls R ein (Schief-) Körper ist, sprechen wir stattdessen von (*Rechts-/Links-*) *Untervektorräumen*, kurz *Unterräumen.*

Anstelle von (U1) hätte es gereicht zu fordern, dass $U \neq \emptyset$. Denn sei $u \in U$, dann folgt $0_M = u \,.\, 0_R \in U$ aus (U3) und Proposition 2.22.

2.45. Beispiel. Wir kennen bereits Beispiele von Untervektorräumen.

(1) Wir fassen die Quaternionen $\mathbb{H}$ als $\mathbb{R}$-Vektorraum auf. In Abschnitt 1.6 haben wir die Unterräume $\mathbb{R} \subset \mathbb{H}$ der reellen und $\mathbb{R}^3 \subset \mathbb{H}$ der imaginären Quaternionen betrachtet.
(2) In der Analysis trifft man häufig auf Untervektorräume. Beispielsweise bilden die Nullfolgen einen Unterraum des Vektorraums aller Folgen. Für ein offenes Intervall I bilden die stetigen Funktionen auf I einen Unterraum des Raumes aller Funktionen auf I, und die differenzierbaren Funktionen einen Unterraum des Raumes der stetigen Funktionen auf I.

2.46. Bemerkung. Jeder Untermodul U eines Rechts-R-Moduls $(M, +, .)$ ist selbst ein Rechts-R-Modul. Zunächst einmal existiert ein Nullelement 0_M und die Verknüpfungen $+ \colon U \times U \to U$ und $. \colon U \times R \to U$ sind wohldefiniert dank (U1)–(U3). Da die Axiome (G1)–(G4) und (M1)–(M3) gelten, wenn man für die Variablen Elemente aus M einsetzt, gelten sie erst recht, wenn man nur Elemente aus U zulässt. Beispielsweise gilt $0_M + u = u$ in M für alle $u \in U$, also auch in U.

Die Inklusion $U \to M$ aus Bemerkung 1.21 ist linear, da (L1) und (L2) offensichtlich gelten.

Wenn R ein Ring mit Eins und M ein unitärer Modul ist, dann ist auch jeder Untermodul U unitär mit der gleichen Begründung wie oben. In diesem Fall darf man auf die Forderung $-u \in U$ in (U2) verzichten, da $-u = u \,.\, (-1)$.

Auf völlig analoge Weise kann man *Untergruppen* und *Unterringe* definieren. Beispielsweise sollte ein Unterring $U \subset R$ das Element 0_R enthalten, und die Summe und das Produkt von Elementen von U sollte wieder in U liegen. Bei Körpern bevorzugt man aus naheliegenden Gründen den Begriff *Teilkörper.*

Wir wollen nun Quotientenmoduln in Analogie zu Beispiel 2.9 konstruieren. Dazu sei $(M, +, .)$ ein Rechts-R-Modul und $U \subset M$ ein Untermodul. Dann definieren wir eine Relation „$\sim$“ auf M für alle $m, n \in M$ durch

$$m \sim n \qquad \Longrightarrow \qquad n - m \in U \,.$$

Das ist eine Äquivalenzrelation, denn (Ä1)–(Ä3) folgen für $\ell, m, n \in M$ aus

$$m - m \in U \,, \qquad n - m \in U \quad \Longrightarrow \quad m - n = -(n - m) \in U \,,$$
$$\text{sowie} \quad m - \ell \in U \text{ und } n - m \in U \quad \Longrightarrow \quad n - \ell = (n - m) + (m - \ell) \in U \,.$$

2.47. Definition. Der Quotient $M/U = M/\sim$ heißt der *Quotientenmodul* von M nach U (lies „M modulo U“). Falls R ein Körper ist heißt M/U der *Quotientenvektorraum,* kurz *Quotientenraum.*

Man beachte hier, dass wir zur Definition der Äquivalenzrelation „$\sim$“ und der Menge M/U nur die additive Struktur des Moduls M benutzt haben. Die

skalare Multiplikation können wir nachträglich definieren. Es sei $p\colon M \to M/\!\sim$ die Quotientenabbildung, siehe Definition 1.42.

2.48. Proposition. *Es sei $(M, +, .)$ ein Rechts-R-Modul und $U \subset M$ ein Untermodul. Dann induzieren „$+$“ und „$.$“ Verknüpfungen*

$$+\colon M/U \times M/U \to M/U \qquad \text{und} \qquad .\colon M/U \times R \to M/U\ ,$$

und $(M/U, +, .)$ ist ein Rechts-R-Modul. Die Quotientenabbildung $p\colon M \to M/U$ ist rechts-R-linear. Wenn R ein Ring mit Eins und M ein unitärer Modul ist, ist auch M/U ein unitärer Modul.

Beweis. Wir gehen vor wie in Beispiel 2.9. Seien $m, n, p, q \in M$ mit $n-m \in U$ und $q - p \in U$, und sei $r \in R$, dann folgt

$$\begin{aligned} (n+q) - (m+p) &= (n-m) + (q-p) && \in U\ , \\ (n\,.\,r) - (m\,.\,r) &= (n-m)\,.\,r && \in U \\ \text{und} \qquad (-n) - (-m) &= -(n-m) && \in U\ , \end{aligned}$$

also sind Addition und skalare Multiplikation auf M/U wohldefiniert durch

$$[m] + [p] = [m+p]\ , \qquad -[m] = [-m] \qquad \text{und} \qquad [m]\,.\,r = [m\,.\,r]\ .$$

Wir setzen $0_{M/U} = [0_M]$. Jetzt können wir die Axiome (G1)–(G4), (M1)–(M3) und gegebenenfalls (M4) auf die entsprechenden Axiome in M zurückführen. Beispielsweise gilt (M1), denn

$$([m]\,.\,r)\,.\,s = [m\,.\,r]\,.\,s = [(m\,.\,r)\,.\,s] = [m\,.\,(r \cdot s)] = [m]\,.\,(r \cdot s)\ .$$

Schließlich zur Linearität der Quotientenabbildung: für alle $m, n \in M$ und r, $s \in R$ gilt

$$p(m\,.\,r + n\,.\,s) = [m\,.\,r + n\,.\,s] = [m]\,.\,r + [n]\,.\,s = p(m)\,.\,r + p(n)\,.\,s\ . \qquad \square$$

2.49. Beispiel. Wir betrachten $M = \mathbb{Z}$ als $\mathbb{Z}$-Modul und

$$U = n\mathbb{Z} = \langle\, \{n\} \,\rangle = \big\{\, an \;\big|\; a \in \mathbb{Z} \,\big\} = \{\, \ldots, -n, 0, n, \ldots \,\}\ .$$

Dann ist U ein Untermodul, und der Quotient $M/U = \mathbb{Z}/n\mathbb{Z}$ ist gerade der Modul aus Beispiel 2.29.

2.50. Bemerkung. In Bemerkung 2.46 haben wir gesehen, dass geeignete Teilmengen von Gruppen, Ringen oder (Schief-) Körpern selbst wieder Gruppen, Ringe beziehungsweise Körper sind. Die Quotientenkonstruktion ist leider nicht so allgemein: Der Quotient einer Gruppe nach einer Untergruppe U beziehungsweise eines Ringes nach einem Unterring ist nur dann wieder Gruppe beziehungsweise Ring, wenn U gewisse zusätzliche Bedingungen erfüllt (siehe Übungen). Körper und Schiefkörper haben keine Quotienten.

2.51. Definition. Es seien M und N Rechts-R-Moduln, und es sei $F\colon M \to N$ rechts-R-linear. Dann definieren wir den *Kern* $\ker F$ durch

$$\ker F = F^{-1}(\{0_N\}) = \big\{\, m \in M \;\big|\; F(m) = 0 \,\big\}\ .$$

Wir erinnern uns auch an das Bild $\operatorname{im} F$, siehe Definition 1.15.

2.52. Proposition. *Es seien M und N Rechts-R-Moduln, und $F\colon M \to N$ sei rechts-R-linear.*

(1) *Der Kern* $\ker F$ *ist ein Untermodul von M, und F ist genau dann injektiv, wenn* $\ker F = \{0_M\}$.
(2) *Das Bild* $\operatorname{im} F$ *ist ein Untermodul von N, und F ist genau dann surjektiv, wenn* $\operatorname{im} F = N$.

Die letzte Aussage in (2) ist klar nach Definition 1.17. Wir haben sie nur angefügt, um die Analogie zu (1) herzustellen.

Beweis. Die Untermodulaxiome folgen aus der Linearität von F, denn für alle m, $n \in M$ und alle $r \in R$ gilt

$$\begin{aligned} & F(0_M) = 0_N \,, \\ F(m) = F(n) = 0_N \quad & \Longrightarrow \quad F(m+n) = F(m) + F(n) = 0 \,, \\ F(m) = 0_N \quad & \Longrightarrow \quad F(m \,.\, r) = F(m) \,.\, r = 0 \end{aligned}$$

Wenn F injektiv ist, hat insbesondere $\ker F = F^{-1}(\{0\})$ höchstens ein Element. Aus $F(0_M) = 0_N$ folgt dann $\ker F = \{0_M\}$.

Sei umgekehrt $\ker F = \{0_M\}$ und $F(m) = F(n) \in N$, dann folgt

$$F(m-n) = F(m) - F(n) = 0_N$$

aus der Additivität (L1) von F, somit ist $m - n \in \ker F$, also nach Voraussetzung $m - n = 0$, das heißt $m = n$. Also ist F injektiv, und (1) ist gezeigt.

Die Untermodulaxiome für $\operatorname{im} F \subset N$ folgen wieder aus der Linearität von F: für alle m, $n \in N$, p, $q \in N$ und $r \in R$ gilt

$$\begin{aligned} & 0_N = F(0_M) \,, \\ p = F(m) \,, \quad q = F(n) \quad & \Longrightarrow \quad p + q = F(m+n) \,, \\ p = F(m) \quad & \Longrightarrow \quad p \,.\, r = F(p \,.\, r) \,. \end{aligned}$$

□

Der folgende Satz entspricht Proposition 1.43 (3).

2.53. Proposition (Universelle Eigenschaft des Quotienten)**.** *Es seien M und N Rechts-R-Moduln, es sei $U \subset M$ ein Untermodul mit Quotientenabbildung $p\colon M \to M/U$, und es sei $F\colon M \to N$ eine rechts-R-lineare Abbildung. Dann existiert genau dann eine Abbildung $\overline{F}\colon M/U \to N$ mit $F = \overline{F} \circ p$, wenn $U \subset \ker F$. In diesem Fall ist $\overline{F}$ eindeutig bestimmt und rechts-R-linear. Es gilt*

$$\operatorname{im} \overline{F} = \operatorname{im} F \qquad \textit{und} \qquad \ker \overline{F} = \ker F/U \,.$$

Wenn $\overline{F}$ existiert, erhalten wir folgendes Diagramm:

$$\begin{array}{ccc} M & \xrightarrow{F} & N \\ {\scriptstyle p}\downarrow & \nearrow_{\overline{F}} & \\ M/U \,. & & \end{array}$$

BEWEIS. Zu „$\Longrightarrow$“ nehmen wir an, dass $\overline{F}$ existiert. Für alle $u \in U$ gilt $[u] = 0_{M/U}$, somit

$$F(u) = \overline{F}([u]) = \overline{F}(0_{M/U}) = F(0_M) = 0_N \ ,$$

es folgt $U \subset \ker F$.

Zu „$\Longleftarrow$“ nehmen wir an, dass $U \subset \ker F$. Seien m, $n \in M$ mit $[m] = [n] \in M/U$, dann folgt

$$m - n \in U \subset \ker F \quad \Longrightarrow \quad F(m) - F(n) = F(m-n) = 0_N \ ,$$

also gilt $F(m) = F(n)$, und $\overline{F}([m]) = F(m)$ ist wohldefiniert.

Die Eindeutigkeit von $\overline{F}$ folgt aus Proposition 1.43 (3). Außerdem ist $\overline{F}$ linear, denn

$$\begin{aligned} \overline{F}([m] + [n]) = F(m+n) = F(m) + F(n) = \overline{F}([m]) + \overline{F}([n]) \ , \\ \overline{F}([m] \,.\, r) = F(m \,.\, r) = F(m) \,.\, r = \overline{F}([m]) \,.\, r \end{aligned}$$

für alle m, $n \in M$ und alle $r \in R$.

Wir sehen leicht, dass $\operatorname{im} \overline{F} = \operatorname{im} F$. Es gilt $[m] \in \ker \overline{F} \subset M/U$ genau dann, wenn $m \in \ker F$, somit folgt

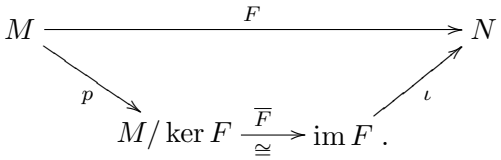
$$\ker \overline{F} = \ker F / U \ . \qquad \square$$

2.54. Folgerung (Homomorphiesatz)**.** *Es seien M und N Rechts-R-Moduln und $F\colon M \to N$ linear. Dann induziert F einen Isomorphismus*

$$\overline{F}\colon M/\ker F \to \operatorname{im} F \ .$$

BEWEIS. Wir wenden Proposition 2.52 an mit $U = \ker F$. Da $\operatorname{im} \overline{F} = \operatorname{im} F$ gilt, dürfen wir $\overline{F}$ als Abbildung mit Bildbereich $\operatorname{im} F$ auffassen. Dann ist $\overline{F}$ linear. Da $\ker \overline{F} = \ker F / \ker F = \{[0_M]\}$, ist $\overline{F}$ injektiv nach Proposition 2.52 (1). Außerdem ist $\overline{F}$ surjektiv, da $\operatorname{im} \overline{F} = \operatorname{im} F$. Also ist $\overline{F}$ ein Isomorphismus. $\square$

Wir können also jede lineare Abbildung $F\colon M \to N$ wie folgt zerlegen:



Dabei ist p die Quotientenabbildung und ι die Inklusion. Um F zu verstehen, bieten sich die folgenden Schritte an.

(1) Bestimme $\ker F$ als Untermodul von M.
(2) Bestimme $\operatorname{im} F$ als Untermodul von N.
(3) Bestimme den Isomorphismus $\overline{F}\colon M/\ker F \to \operatorname{im} F$.

2.55. Beispiel. Wir betrachten eine Ebene $V \subset \mathbb{R}^3$ und eine Gerade $U \subset \mathbb{R}^3$, so dass sich U und V nur in einem Punkt schneiden. Wir wollen annehmen, dass das der Nullpunkt ist; dann sind U und V Unterräume. Unsere Anschauung sagt uns, dass es durch jeden Punkt $x \in \mathbb{R}^3$ genau eine zu V parallele Gerade gibt, und dass diese Gerade die Ebene U genau in einem Punkt schneidet. Wir definieren $F\colon \mathbb{R}^3 \to U$ so, dass $F(x)$ gerade dieser Schnittpunkt ist. Diese Abbildung ist $\mathbb{R}$-linear — all das wird im nächsten Kapitel klarer werden.

Nach Konstruktion werden genau die Punkte auf der Geraden V auf den Schnittpunkt 0 von U und V abgebildet, also ist $\ker F = V$. Jeder Punkt in der Ebene U wird auf sich abgebildet, also ist F insbesondere surjektiv. Aus dem Homomorphiesatz 2.54 folgt

$$\mathbb{R}^3/V = \mathbb{R}^3/\ker F \cong \operatorname{im} F = U \ .$$

Das Besondere hier ist, dass U selbst ein Unterraum von $\mathbb{R}^3$ ist mit $F|_U = \mathrm{id}_U$.

Sei jetzt wieder $x \in \mathbb{R}^3$ beliebig. Nach Konstruktion ist $x - F(x) \in V$, da eine zu V parallele Gerade durch x und $F(x)$ geht. Es folgt

$$x = u + v \qquad \text{mit} \qquad u = F(x) \in U \qquad \text{und} \qquad v = x - F(x) \in V \ .$$

Diese Zerlegung ist eindeutig, denn wäre $x = u' + v'$ eine weitere Zerlegung, dann würde folgen

$$u' + v' = u + v \qquad \longrightarrow \qquad u' - u = v - v' \in U \cap V = \{0\} \ ,$$

also $u = u'$ und $v = v'$. Somit liefern die Unterräume U und V ein Beispiel für die folgende Definition.

2.56. Definition. Es sei M ein Rechts-R-Modul und $U, V \subset M$ Untermoduln. Die *Summe* von U und V ist gegeben durch

$$U + V = \left\{ u + v \;\middle|\; u \in U, v \in V \right\} \subset M \ .$$

Falls $U \cap V = \{0\}$ heißt die Summe *direkt,* und wir schreiben statt $U + V$ auch $U \oplus V$. Falls M die direkte Summe $U \oplus V$ ist, sagen wir, dass V ein *Komplement* von U in M ist (und umgekehrt), oder, dass U und V *komplementäre Untermoduln* sind. Wenn R ein (Schief-) Körper ist, sprechen wir analog von *komplementären Unterräumen.*

Man beachte, dass wegen (U1) stets $0_M \in U \cap V$ gilt. Einen kleineren Durchschnitt als $\{0_M\}$ können zwei Untermoduln also nicht haben.

2.57. Beispiel. Wir geben Beispiele von direkten Summen und komplentären Untermoduln an.

(1) In den Übungen zeigen Sie, dass $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$. Also sind die Untermoduln

$$U = 2\mathbb{Z}/6\mathbb{Z} = \{[0], [2], [4]\} \cong \mathbb{Z}/3\mathbb{Z}$$
$$\text{und} \qquad V = 3\mathbb{Z}/6\mathbb{Z} = \{[0], [3]\} \cong \mathbb{Z}/2\mathbb{Z}$$

von $M = \mathbb{Z}/6\mathbb{Z}$ zueinander komplementär.

(2) Ähnlich wie in (1) betrachte

$$V = 2\mathbb{Z}/4\mathbb{Z} = \{[0],[2]\} \subset M = \mathbb{Z}/4\mathbb{Z}\ .$$

Dann ist $V \cong \mathbb{Z}/2\mathbb{Z}$. Es gibt keinen komplementären Untermodul U, denn dieser müsste mindestens ein Element aus $M \setminus V$ enthalten, also entweder [1] oder [3]. In beiden Fällen wäre $[2] \in U$, denn $[2] = [1] + [1] = [3] + [3]$, und somit $U \cap V \neq \{[0]\}$. Also existiert nicht immer ein komplementärer Untermodul.

Es sei $V \subset M$ ein Untermodul. Wir erinnern uns an die Quotientenabbildung $p\colon M \to M/V$ aus Proposition 2.48.

2.58. Proposition. *Es seien U, V Untermoduln eines Rechts-R-Moduls M.*

(1) *Die Summe $U + V \subset M$ ist ein Untermodul.*
(2) *Wenn die Summe direkt ist, existiert eine bijektive Abbildung*

$$U \times V \to U \oplus V \qquad \textit{mit} \qquad (u,v) \mapsto u + v\ .$$

(3) *Es sei $p\colon M \to M/V$ die Quotientenabbildung. Wenn U und V komplementäre Untermoduln sind, dann ist $p|_U\colon U \to M/V$ ein Modulisomorphismus.*

Beweis. Die Unterraumaxiome für $U + V$ gelten, da

$$\begin{aligned} 0_M = 0_M + 0_M &\qquad \in U+V\ , \\ (t+v)+(u+w) = (t+u)+(v+w) &\qquad \in U+V \\ \text{und} \qquad (u+v)\,.\,r = u\,.\,r + v\,.\,r &\qquad \in U+V \end{aligned}$$

für alle t, $u \in U$, v, $w \in V$ und $r \in R$.

Die Abbildung in (2) ist immer surjektiv nach Definition der Summe. Wenn die Summe direkt ist, ist für jedes Element $s \in U \oplus V$ die Zerlegung $s = u + v$ mit $u \in U$ und $v \in V$ eindeutig, denn aus $s = u' + v'$ mit $u' \in U$, $v' \in V$ folgt

$$u' - u = v - v' \in U \cap V \quad \Longrightarrow \quad u' - u = v - v' = 0_M\ .$$

Also ist die Abbildung in (2) auch injektiv.

Die Quotientenabbildung $p\colon M \to M/V$ ist linear nach Proposition 2.48. Die Inklusion $\iota\colon U \to M$ ist linear nach Bemerkung 2.46. Also ist auch die Abbildung $p|_U = p \circ \iota$ in (3) linear nach Proposition 2.40.

Aus $p(u) = p(u') \in M/V$ folgt, dass ein $v \in V$ existiert mit $u' = u + v$. Wie in (2) folgt aus $v = u - u' \in U \cap V$, dass $u = u'$. Also ist $p|_U$ injektiv.

Sei schließlich $[m] \in M/V$ mit $m \in M$, dann existieren $u \in U$, $v \in V$ mit $m = u + v$, da $M = U \oplus V$. Da $p(u) = [u] = [m]$, ist $p|_U$ auch surjektiv. □

2.59. Bemerkung. Wir können also den Quotientenmodul M/V mit Hilfe von $p|_U$ mit einem komplementären Untermodul U identifizieren, falls ein solcher existiert. Wenn U ein zu V komplementärer Untermodul ist, gibt es meistens noch andere komplementäre Untermoduln, siehe etwa Beispiel 2.55, wo in

Richtung von V auf verschiedene Ebenen in $\mathbb{R}^3$ projizieren kann. Das bedeutet, dass die Identifikation $M/V \cong U$ von der Wahl des Komplements abhängt. Obwohl man oft leichter mit dem komplementären Untermodul U als mit dem Quotienten M/V arbeiten kann, ist es daher manchmal sinnvoll, den Quotienten M/V zu betrachten.

Die direkte Summe erfüllt gleich zwei „universelle Eigenschaften“. Sei dazu $M = U \oplus V$, dann betrachten wir die Inklusionsabbildungen $\iota_U \colon U \to M$ und $\iota_V \colon V \to M$. Wenn wir wie oben $M/U \cong V$ und $M/V \cong U$ identifizieren, erhalten wir auch Projektionen $p_U \colon M \to U$ und $p_V \colon M \to V$, so dass insbesondere

$$m = p_U(m) + p_V(m)$$

für alle $m \in M$.

2.60. Proposition (Universelle Eigenschaften der direkten Summe)**.** *Es sei M ein Rechts-R-Moduln und U, $V \subset M$ Untermoduln, so dass $M = U \oplus V$.*

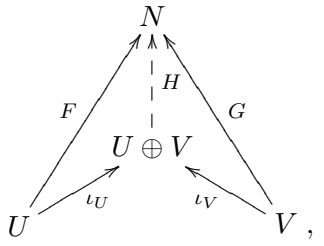
(1) *Die Inklusions- und Projektionsabbildungen erfüllen*

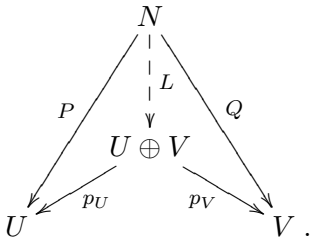
$$p_U \circ \iota_U = \mathrm{id}_U \,, \qquad p_U \circ \iota_V = 0 \colon V \to U \,,$$
$$p_V \circ \iota_U = 0 \colon U \to V \qquad \textit{und} \qquad p_V \circ \iota_V = \mathrm{id}_V \,.$$

(2) Universelle Eigenschaft des Koproduktes: *Sei N ein weiterer Rechts-R-Modul und seien $F \colon U \to N$ und $G \colon V \to N$ linear, dann existiert genau eine lineare Abbildung $H \colon U \oplus V \to N$, so dass $F = H \circ \iota_U$ und $G = H \circ \iota_V$.*

(3) Universelle Eigenschaft des Produktes: *Sei N ein weiterer Rechts-R-Modul und seien $P \colon N \to U$ und $Q \colon N \to V$ linear, dann existiert genau eine lineare Abbildung $L \colon N \to U \oplus V$, so dass $P = p_U \circ L$ und $Q = p_V \circ L$.*

Wie eng diese beiden Eigenschaften miteinander verwandt sind, zeigen die folgenden Diagramme, die sich nur in der Richtung der Pfeile unterscheiden. Man sagt auch, die Diagramme sind zueinander *dual*.





Beweis. Zu (1) sei $u \in U$, dann folgt

$$(p_U \circ \iota_U)(u) = p_U(u + 0_M) = u = \mathrm{id}_U(u) \,,$$
$$(p_V \circ \iota_U)(u) = p_V(u + 0_M) = 0 = 0(u) \in V \,.$$

Also gilt $p_U \circ \iota_U = \mathrm{id}_U$ und $p_V \circ \iota_U = 0$. Die beiden anderen Gleichungen folgen genauso.

Zu (2) zeigen wir zunächst die Eindeutigkeit. Sei also eine lineare Abbildung H gegeben mit $H \circ \iota_U = F$ und $H \circ \iota_V = G$. Für $m = u + v$ folgt

$$\begin{aligned} H(m) = H(u) + H(v) &= H(\iota_U(u)) + H(\iota_V(v)) \\ &= F(u) + G(v) = F(p_U(m)) + G(p_V(m)) \ , \end{aligned}$$

also ist H eindeutig bestimmt.

Auf der anderen Seite ist die Abbildung $F \circ p_U + G \circ p_V$ linear nach Proposition 2.40. Sie leistet das Gewünschte, denn wegen (1) gilt

$$\begin{aligned} \big(F \circ p_U + G \circ p_V\big) \circ \iota_U &= F \circ \underbrace{p_U \circ \iota_U}_{=\mathrm{id}_U} + G \circ \underbrace{p_V \circ \iota_U}_{=0} = F \ , \\ \big(F \circ p_U + G \circ p_V\big) \circ \iota_V &= F \circ p_U \circ \iota_V + G \circ p_V \circ \iota_V = G \ . \end{aligned}$$

Der Beweis zu (3) verläuft analog. Es sei $n \in N$ und $m = L(n) = u + v$ mit $u \in U$ und $v \in V$, dann folgt $u = p_U(L(n)) = P(n)$ und $v = p_V(L(n)) = Q(n)$, also ist L eindeutig bestimmt.

Umgekehrt ist die Abbildung

$$\iota_U \circ P + \iota_V \circ Q \colon N \to M = U \oplus V$$

linear nach Proposition 2.40. Mithilfe von (1) überprüft man wieder, dass

$$p_U \circ \big(\iota_U \circ P + \iota_V \circ Q\big) = P \qquad \text{und} \qquad p_V \circ \big(\iota_U \circ P + \iota_V \circ Q\big) = Q \ . \qquad \square$$

Wir können Summen auch für mehr als zwei Unterräume definieren. Sei etwa M ein Rechts-R-Modul, sei I eine Indexmenge, und sei $(U_i)_{i\in I}$ eine Familie von Untermoduln, aufgefasst als Familie in der Potenzmenge von M, siehe Definition 1.11. Dann definieren wir ihre Summe als

$$\sum_{i\in I} U_i = \left\{ \sum_{i\in I} u_i \;\middle|\; u_i \in U_i \text{ für alle } i \in I,\ u_i = 0_M \text{ für fast alle } i \in I \right\} \subset M \ .$$

Wenn $U_i \cap \sum_{j\in I, j\neq i} U_i = \{0_M\}$ für alle $i \in I$, nennen wir diese Summe wieder direkt und schreiben

$$\bigoplus_{i\in I} U_i = \sum_{i\in I} U_i \ .$$

Manchmal definiert man auch eine direkte Summe von beliebigen Rechts-R-Moduln, die nicht Untermoduln eines festen Moduls M sind.

2.61. Definition. Es seien M_i Rechts-R-Modul. Dann definieren wir ihre *direkte Summe* und ihr *direktes Produkt* als

$$\begin{aligned} \coprod_{i\in I} M_i &= \left\{ (m_i)_{i\in I} \;\middle|\; m_i \in M_i \text{ für alle } i \in I,\ u_i = 0_{M_i} \text{ für fast alle } i \in I \right\} , \\ \prod_{i\in I} M_i &= \big\{ (m_i)_{i\in I} \;\big|\; m_i \in M_i \text{ für alle } i \in I \big\} \ . \end{aligned}$$

Wir erhalten für alle $j \in I$ Inklusionen $\iota_j \colon M_j \to \coprod_{i\in I} M_i$ beziehungsweise $\iota_j \colon M_j \to \prod_{i\in I} M_i$ mit

$$\iota_j(m) = (m_i)_{i\in I}\,, \qquad \text{mit} \qquad m_i = \begin{cases} m & \text{falls } i = j, \text{ und} \\ 0 & \text{falls } i \neq j, \end{cases}$$

und Projektionen $p_j \colon \coprod_{i\in I} M_i \to M_j$ beziehungsweise $p_j \colon \prod_{i\in I} M_i \to M_j$ mit

$$p_j\big((m_i)_{i\in I}\big) = m_j \in M_j\,.$$

Man überzeugt sich leicht, dass beides wieder Moduln sind. Dabei geht man ähnlich vor wie in Beispiel 2.30. In der Tat gilt

$$R^{(I)} = \coprod_{i\in I} R \qquad \text{und} \qquad R^I = \prod_{i\in I} R\,.$$

Die folgenden universellen Eigenschaften werden analog zu Proposition 2.60 bewiesen:

2.62. Proposition. *Es sei M_i ein Rechts-R-Modul für alle $i \in I$.*

(1) *Für die Inklusions- und Projektionsabbildungen gilt*

$$p_i \circ \iota_i = \mathrm{id}_{M_i} \qquad \textit{und} \qquad p_i \circ \iota_j = 0 \colon M_j \to M_i$$

für alle i, $j \in I$ mit $i \neq j$.

(2) Universelle Eigenschaft des Koproduktes: *Sei N ein weiterer Rechts-R-Modul und sei $F_j \colon M_j \to N$ linear für alle $j \in I$, dann existiert genau eine lineare Abbildung $H \colon \coprod_{i\in I} M_i \to N$, so dass $F_j = H \circ \iota_j$ für alle $j \in I$.*

(3) Universelle Eigenschaft des Produktes: *Sei N ein weiterer Rechts-R-Modul und seien $P_j \colon N \to M_j$ linear für alle $j \in I$, dann existiert genau eine lineare Abbildung $L \colon N \to \prod_{i\in I} M_i$, so dass $P_j = p_j \circ L$ für alle $j \in I$.*

2.5. Matrizen

Wir wollen jetzt verstehen, wie man lineare Abbildungen durch Matrizen beschreiben kann. Das ist zum Beispiel dann wichtig, wenn man numerische Berechnungen durchführen will (also Berechnungen mit „echten“ Zahlen, nicht abstrakte Überlegungen mit Variablen). Auf der anderen Seite sollten wir Matrizen nur als nützliche Rechenhilfen verstehen. Im Vordergrund des Interesses werden weiterhin lineare Abbildungen stehen.

Vorab überlegen wir uns, dass $(R^{(I)})^J$ gerade die Menge derjenigen Familien $(a_{ij})_{i\in I, j\in J}$ in R bezeichnet, so dass für jedes $j \in J$ nur endlich viele $i \in I$ mit $a_{ij} \neq 0_R$ existieren.

2.63. Proposition. *Es sei R ein Ring mit Eins, I, J seien Mengen und $R^{(I)}$, $R^{(J)}$ die von ihnen erzeugten freien Rechts-R-Moduln. Für alle $j \in J$ bezeichne e_j den Basisvektor aus Beispiel 2.30 (1). Dann existiert zu jeder linearen Abbildung $A\colon R^{(J)} \to R^{(I)}$ eine Familie $(a_{ij})_{i\in I, j\in J} \in (R^{(I)})^J$, so dass*

$$(a_{ij})_{i\in I} = A(e_j) \in R^{(I)} \qquad \text{für alle } j \in J\ . \tag{1}$$

Für alle $(b_{ij})_{i\in I, j\in J} \in (R^{(I)})^J$ existiert eine lineare Abbildung $B\colon R^{(J)} \to R^{(I)}$, so dass

$$B\big((r_j)_{j\in J}\big) = \left(\sum_{j\in J} b_{ij}\cdot r_j\right)_{i\in I}\ . \tag{2}$$

Die in (1) und (2) konstruierten Abbildungen $\Phi\colon \mathrm{Hom}_R\big(R^{(J)}, R^{(I)}\big) \to (R^{(I)})^J$ und $\Psi\colon (R^{(I)})^J \to \mathrm{Hom}_R\big(R^{(J)}, R^{(I)}\big)$ sind zueinander invers und daher bijektiv.

Beweis. Da $A(e_j) \in R^{(I)}$, gibt es für jedes $j \in J$ nur endlich viele $i \in I$ mit $a_{ij} \neq 0_R$, und es folgt (1). Wir erhalten also eine Abbildung $\Phi\colon \mathrm{Hom}_R(R^{(J)}, R^{(I)}) \to (R^{(I)})^J$ mit $A \mapsto (a_{ij})_{i\in I, j\in J}$.

Es seien jetzt $(b_{ij})_{i\in I, j\in J} \in (R^{(I)})^J$ und $(r_j)_{j\in J} \in R^{(J)}$ gegeben. Dann ist

$$\left(\sum_{j\in J} b_{ij}\cdot r_j\right)_{i\in I} = \sum_{j\in J} (b_{ij}\cdot r_j)_{i\in I} = \sum_{j\in J} (b_{ij})_{i\in I}\cdot r_j$$

eine Linearkombination aus Elementen $(b_{ij})_{i\in I} \in R^{(I)}$, also erhalten wir in (2) eine Abbildung $B\colon R^{(J)} \to R^{(I)}$.

Für alle $(r_j)_{j\in J}$, $(s_j)_{j\in J} \in R^{(J)}$ und alle $t \in R$ folgt

$$\begin{aligned}
B\big((r_j)_{j\in J} + (s_j)_{j\in J}\big) &= B\big((r_j + s_j)_{j\in J}\big) = \left(\sum_{j\in J} b_{ij}\cdot (r_j + s_j)\right)_{i\in I} \\
&= \left(\sum_{j\in J} b_{ij}\cdot r_j + \sum_{j\in J} b_{ij}\cdot s_j\right)_{i\in I} \\
&= \left(\sum_{j\in J} b_{ij}\cdot r_j\right)_{i\in I} + \left(\sum_{j\in J} b_{ij}\cdot s_j\right)_{i\in I} \\
&= B\big((r_j)_{j\in J}\big) + B\big((s_j)_{j\in J}\big)\ ,
\end{aligned}$$

und

$$\begin{aligned}
B\big((r_j)_{j\in J}\cdot t\big) &= B\big((r_j\cdot t)_{j\in J}\big) = \left(\sum_{j\in J} b_{ij}\cdot (r_j\cdot t)\right)_{i\in I} \\
&= \left(\sum_{j\in J} (b_{ij}\cdot r_j)\cdot t\right)_{i\in I} = \left(\sum_{j\in J} b_{ij}\cdot r_j\right)_{i\in I}\cdot t \\
&= B\big((r_j)_{j\in J}\big)\cdot t\ .
\end{aligned}$$

Also ist die Abbildung B in (2) auch rechts-R-linear. Wir erhalten also eine Abbildung $\Psi\colon (R^{(I)})^J \to \mathrm{Hom}_R\big(R^{(J)}, R^{(I)}\big)$ mit $(b_{ij})_{i\in I, j\in J} \mapsto B$.

Sei wieder $(b_{ij})_{i\in I,j\in J} \in (R^{(I)})^J$ und $B = \Psi\big((b_{ij})_{i\in I,j\in J}\big)$. Für die Familie $(a_{ij})_{i\in I,j\in J} = \Phi(B)$ folgt

$$(a_{ij})_{i\in I} = B(e_j) = \left(\sum_{k\in J} b_{ik}\cdot\delta_{kj}\right)_{i\in I} = (b_{ij})_{i\in I}$$

für alle $j \in J$, also gilt $\Phi\circ\Psi = \mathrm{id}_{(R^{(I)})^J}$.

Sei umgekehrt $A \in \mathrm{Hom}_R\big(R^{(J)}, R^{(I)}\big)$ und $(a_{ij})_{i\in I,j\in J} = \Phi(A)$. Es sei $B = \Psi\big()$, dann folgt aus der Linearität von A und aus Beispiel (2.30) (2), dass

$$\begin{aligned} B\big((r_j)_{j\in J}\big) &= \left(\sum_{j\in J} a_{ij}\cdot r_j\right)_{i\in I} = \sum_{j\in J}(a_{ij})_{i\in I}\,.\,r_j \\ &= \sum_{j\in J} A(e_j)\,.\,r_j = A\Big(\sum_{j\in J} e_j\,.\,r_j\Big) = A\big((r_j)_{j\in J}\big)\,. \end{aligned}$$

Also gilt auch $\Psi\circ\Phi = \mathrm{id}_{\mathrm{Hom}_R\left(R^{(J)},R^{(I)}\right)}$, somit sind Φ und Ψ zueinander invers und insbesondere bijektiv nach Satz 1.22 (4), (5). □

Diese Proposition ist die Grundlage für das Rechnen mit Matrizen, wie wir jetzt sehen werden.

2.64. Definition. Es sei R ein Ring und m, $n \in \mathbb{N}$. Eine $m\times n$-*Matrix* über R ist eine Familie $A = (a_{ij})_{i=1\ldots m,j=1\ldots n}$ in R, geschrieben

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}\,. \tag{1}$$

Die Menge aller $m\times n$-Matrizen über R wird mit $M_{m,n}(R)$ bezeichnet.

Wir definieren die *Matrixaddition* $+\colon M_{m,n}(R)\times M_{m,n}(R)\to M_{m,n}(R)$ durch

$$A + B = (a_{ij}+b_{ij})_{i=1\ldots m,j=1\ldots n} \in M_{m,n}(R) \tag{2}$$

für alle $B = (b_{ij})_{i=1\ldots m,j=1\ldots n} \in M_{m,n}(R)$, und die *Matrizenmultiplikation* $\cdot\colon M_{\ell,m}(R)\times M_{m,n}(R)\to M_{\ell,n}(R)$ mit $\ell\in\mathbb{N}$ durch

$$C\cdot A = \left(\sum_{j=1}^{m} c_{ij}\cdot a_{jk}\right)_{i=1\ldots\ell,k=1\ldots n} \in M_{\ell,n}(R) \tag{3}$$

für alle $C = (c_{ij})_{i=1\ldots\ell,j=1\ldots m} \in M_{\ell,m}(R)$.

Wenn die Größe einer Matrix bekannt ist, schreiben wir auch kurz $(a_{ij})_{ij} \in M_{m,n}(R)$ — daraus ergibt sich, dass $1\le i\le m$ und $1\le j\le n$.

Die Matrixaddition erfolgt komponentenweise, genau wie in Beispiel (2.30). Zwei Matrizen kann man nur addieren, wenn sie die gleiche Anzahl von Zeilen und die gleiche Anzahl von Spalten haben.

Zwei Matrizen lassen sich multiplizieren, wenn die erste soviele Spalten hat wie die zweite Zeilen. Die Matrixmultiplikation lässt sich am besten am folgenden Schema verdeutlichen:

$$\begin{pmatrix} \cdot & \cdots & \cdot \\ \vdots & & \vdots \\ a_{i1} & \cdots & a_{in} \\ \vdots & & \vdots \\ \cdot & \cdots & \cdot \end{pmatrix} \begin{pmatrix} \cdot & \cdots & b_{1k} & \cdots & \cdot \\ \vdots & & \vdots & & \vdots \\ \cdot & \cdots & b_{nk} & \cdots & \cdot \end{pmatrix} = \begin{pmatrix} \cdot & \cdots & | & \cdots & \cdot \\ \vdots & & | & & \\ — & & a_{i1}b_{1k} + \cdots + a_{in}b_{nk} & & \vdots \\ \vdots & & | & & \\ \cdot & & \cdots & & \cdot \end{pmatrix}$$

Hierbei steht die Matrix A links, die Matrix B oben, und das Produkt $A \cdot B$ unten rechts. Der Eintrag an der Stelle (i, k) sieht also genauso aus wie das „Skalarprodukt“ aus der Zeile i der Matrix A und der Spalte k der Matrix B, vergleiche Definition 1.51 (1).

2.65. Bemerkung. Wir betrachten die folgenden Spezialfälle.

(1) Wenn $m = 0$ oder $n = 0$ ist, enthält $M_{m,n}(R)$ nur ein Element, die leere Matrix ( ).
(2) Für $m = 1 = n$ identifizieren wir $M_{1,1}(R)$ mit R. Addition und Multiplikation von 1×1-Matrizen entsprechen genau der Addition und Multiplikation in R:
$$(r) + (s) = (r + s) \qquad \text{und} \qquad (r) \cdot (s) = (r \cdot s) \, .$$
(3) Es sei $n = 1$, dann ist $M_{m,1}(R) = R^m$ der „Raum der Spalten“ der Länge m, und Addition funktioniert genau wie in Beispiel 2.31. Wir können von rechts mit einer 1×1-Matrix aus (2) multiplizieren und erhalten die skalare Multiplikation
$$\begin{pmatrix} r_1 \\ \vdots \\ r_m \end{pmatrix} \cdot (s) = \begin{pmatrix} r_1 \cdot s \\ \vdots \\ r_m \cdot s \end{pmatrix} = \begin{pmatrix} r_1 \\ \vdots \\ r_m \end{pmatrix} . \, s \, .$$
Aus diesem Grund ist es sinnvoll, Spalten von rechts mit Skalaren zu multiplizieren.
(4) Für $m = 1$ ist $M_{1,n}(R) = {}^nR$ der „Raum der Zeilen“ der Länge n. Addition funktioniert wieder wie in Beispiel 2.31, Multiplikation mit einer 1×1-Matrix von links entspricht der Multiplikation mit einem Skalar.

Die nächsten zwei Spezialfälle sind so wichtig, dass wir sie separat formulieren.

2.66. Folgerung (aus Proposition 2.63)**.** *Es sei R ein Ring mit Eins und m, $n \in \mathbb{N}$. Dann existiert eine natürliche Bijektion*

$$\Phi \colon \operatorname{Hom}_R(R^n, R^m) \to M_{m,n}(R) \, . \tag{1}$$

Dabei steht das Bild des Basisvektors e_j von R^n unter $A\colon R^n \to R^m$ in der j-ten Spalte der Matrix $(a_{ij})_{i,j} = \Phi(A)$. Matrixmultiplikation $\cdot\colon M_{m,n}(R) \times R^n \to R^m$ entspricht dem Anwenden einer linearen Abbildung, genauer

$$A\left(\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix}\right) = \Phi(A) \cdot \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} \in R^m \ . \tag{2}$$

Die Matrixaddition entspricht der Addition linearer Abbildungen, für A, $B \in \operatorname{Hom}_R(R^n, R^m)$ gilt also

$$\Phi(A + B) = \Phi(A) + \Phi(B) \ . \tag{3}$$

Für ℓ, m, $n \in \mathbb{N}$ seien $A\colon R^m \to R^\ell$ und $B\colon R^n \to R^m$ rechts-R-linear. Dann gilt

$$\Phi(A \circ B) = \Phi(A) \cdot \Phi(B) \in M_{\ell,n}(R) \ , \tag{4}$$

das heißt, die Matrixmultiplikation $\cdot : M_{\ell,m}(R) \times M_{m,n}(R) \to M_{\ell,n}(R)$ entspricht der Verkettung linearer Abbildungen.

Beweis. Wir setzen $I = \{1, \dots, m\}$ und $J = \{1, \dots, n\}$ in Proposition 2.63. Dann ist

$$R^{(I)} = R^m \ , \qquad R^{(J)} = R^n \qquad \text{und} \qquad (R^{(I)})^J = M_{m,n}(R) \ .$$

Beachte, dass I und J hier endliche Mengen sind, es gibt also keine zusätzlichen Bedingungen an die Zahlen a_{ij}, wenn $(a_{ij})_{i,j} \in (R^{(I)})^J = M_{m,n}(R)$. Also liefert Proposition 2.63 (1) die Abbildung in (1). Die j-te Spalte der Matrix ist dabei wie gefordert

$$A(e_j) = (a_{ij})_{i=1,\dots,m} = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} \ .$$

Es sei wieder $(a_{ij})_{i,j} = \Phi(A)$. Wir schreiben $(r_j)_{j=1,\dots,n}$ für die Spalte aus (2). Aus Proposition 2.63 (2) folgt

$$A\left(\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix}\right) = A\big((r_j)_{j=1,\dots,n}\big) = \Big(\sum_{j=1}^{n} a_{ij} \cdot r_j\Big)_{i=1,\dots,m} = (a_{ij})_{i,j} \cdot \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} \ .$$

Die letzte Gleichung ist gerade die Definition 2.64 (3) der Matrixmultiplikation in dem Fall, dass der zweite Faktor $(r_j)_{j=1,\dots,n}$ eine Spalte ist.

Zu (3) seien $(a_{ij})_{i,j} = \Phi(A)$, $(b_{ij})_{i,j} = \Phi(B) \in M_{m,n}(R)$. Wir bestimmen $\Phi(A + B)$, indem wir die Bilder der Vektoren $e_k \in R^n$ berechnen. Nach Definition von $A + B$ in Bemerkung 2.39 und Proposition 2.63 (1) gilt

$$(A + B)(e_k) = A(e_k) + B(e_k) = \begin{pmatrix} a_{1k} \\ \vdots \\ a_{mk} \end{pmatrix} + \begin{pmatrix} b_{1k} \\ \vdots \\ b_{mk} \end{pmatrix} = \begin{pmatrix} a_{1k} + b_{1k} \\ \vdots \\ a_{mk} + b_{mk} \end{pmatrix} \in R^m \ ,$$

und das ist genau die k-te Spalte der Matrix $\Phi(A) + \Phi(B)$.

Zu (4) sei $(a_{ij})_{i,j} = \Phi(A) \in M_{\ell,m}(R)$ und $(b_{jk})_{j,k} = \Phi(B) \in M_{m,n}(R)$. Um die Matrix $\Phi(A \circ B)$ zu erhalten, müssen wir die Bilder der Vektoren $e_k \in R^n$ bestimmen. Nach Proposition 2.63 (1) ist

$$B(e_k) = (b_{jk})_{j=1,\dots,m} .$$

Nach Proposition 2.63 (2) gilt

$$A\big(B(e_k)\big) = \left(\sum_{j=1}^{m} a_{ij} \cdot b_{jk}\right)_{i=1,\dots,\ell} = \begin{pmatrix} a_{11} \cdot b_{1k} + \dots + a_{1m} \cdot b_{mk} \\ \vdots \\ a_{\ell 1} \cdot b_{1k} + \dots + a_{\ell m} \cdot b_{mk} \end{pmatrix} \in R^{\ell} ,$$

Also hat $\Phi(A \circ B)$ die gleiche k-te Spalte wie das Matrixprodukt $\Phi(A) \cdot \Phi(B)$. Daraus folgt unsere Behauptung. □

2.67. Bemerkung. Nach Folgerung 2.66 bietet es sich an, Matrizen $A = (a_{ij})_{i,j} \in M_{m,n}(R)$ mit den zugehörigen Abbildungen $A\colon R^n \to R^m$ zu identifizieren. Somit ist

$$\mathrm{Hom}_R(R^n, R^m) = M_{m,n}(R) .$$

Die Abbildungen Φ und Ψ aus Proposition 2.63 brauchen wir dann natürlich nicht mehr.

Man beachte: auf die Rechts-R-Moduln R^n wirken Matrizen von links. Auf diese Weise kommt die skalare Multiplikation der Matrix nicht „in die Quere“, das heißt, die Multiplikation mit einer Matrix von links ist rechts-R-linear.

Bei Zeilen ist es genau spiegelbildlich: hier operieren Skalare von links wegen Bemerkung 2.65 (4) und Matrizen von rechts, es folgt also

$${}_R\mathrm{Hom}({}^mR, {}^nR) = M_{m,n}(R) .$$

Wenn man die Verkettung linearer Abbildungen als Matrixprodukt schreibt, dreht sich die Reihenfolge der Faktoren um. Aus diesem Grund ist es einfacher, mit Rechts-R-Moduln zu arbeiten.

Tatsächlich kann man einige Fehler vermeiden, wenn man Skalare konsequent von rechts wirken lässt — selbst dann, wenn man über einem kommutativen Ring oder Körper arbeitet, bei dem es nach Bemerkung 2.23 eigentlich keinen Unterschied zwischen Rechts- und Linksmoduln gibt.

2.68. Folgerung. *Die Matrixmultiplikation ist assoziativ.*

Beweis. Diese Behauptung könnte man beispielsweise mit Hilfe der Definition 2.64 (3) der Matrixmultiplikation mit etwas Aufwand nachrechnen.

Einfacher ist es, Matrizen $A \in M_{\ell,m}(R) = \mathrm{Hom}_R(R^m, R^\ell)$, $B \in M_{m,n}(R) = \mathrm{Hom}_R(R^n, R^m)$ und $C \in M_{n,p}(R) = \mathrm{Hom}_R(R^p, R^n)$ mit den entspechenden linearen Abbildungen zu identifizieren. Da die Verkettung von Abbildungen assoziativ ist nach Bemerkung 2.4 (1), folgt aus Folgerung 2.66 (4), dass

$$A \cdot (B \cdot C) = A \circ (B \circ C) = (A \circ B) \circ C = (A \cdot B) \cdot C) . \qquad \square$$

2.69. Definition. Es sei R ein Ring mit Eins. Eine $m \times n$-Matrix über R heißt *quadratisch,* wenn $m = n$. Der Raum der quadratischen $n \times n$-Matrizen über R wird mit $M_n(\mathbb{R})$ bezeichnet. Die quadratische Matrix $E_n = (\delta_{ij})_{i,j} \in M_n(R)$ heißt *Einheitsmatrix.* Eine quadratische Matrix $A \in M_n(R)$ heißt *invertierbar,* wenn es eine Matrix $B \in M_n(R)$ mit $A \cdot B = B \cdot A = E_n$ gibt. In diesem Fall heißt B die zu A *inverse Matrix;* sie wird auch mit A^{-1} bezeichnet.

2.70. Bemerkung. Identifiziere $M_n(R)$ mit $\operatorname{End}_R R^n = \operatorname{Hom}_R(R^n, R^n)$ wie in Bemerkung 2.67.

(1) Die Einheitsmatrix entspricht der Identität id_{R^n}, denn für alle $m = (r_j)_j \in R^n$ gilt

$$E_n \cdot m = \left(\sum_{j=1}^{n} \delta_{ij}\, r_j \right)_i = (r_i)_i = m \; .$$

(2) Es sei $A\colon R^n \to R^n$ eine lineare Abbildung, $A \in M_n(R)$. Wegen Folgerung 2.66 (4) ist A genau dann als lineare Abbildung umkehrbar, also ein Isomorphismus, wenn A als Matrix invertierbar ist. In diesem Fall wird die Umkehrabbildung von A genau durch die inverse Matrix A^{-1} beschrieben. Aus Folgerung 2.71 (1) unten folgt mit Proposition 2.3, dass die inverse Matrix eindeutig bestimmt ist.

2.71. Folgerung (aus Folgerungen 2.42 und 2.66)**.** *Es sei R ein Ring mit Eins.*

(1) *Die invertierbaren $n \times n$-Matrizen bilden eine Gruppe $(GL(n, R), \cdot)$, die* allgemeine lineare Gruppe, *und es gilt $GL(n, R) \cong \operatorname{Aut}_R R^n$.*
(2) *Die quadratischen $n \times n$-Matrizen bilden einen Ring $(M_n(R), +, \cdot)$ mit Eins E_n, den* Matrixring, *und es gilt $M_n(R) \cong \operatorname{End}_R R^n$.*
(3) *Der Raum der Spalten R^n wird durch Matrixmultiplikation zu einem unitären $M_n(R)$-Linksmodul.*
(4) *Der Raum $M_{m,n}(R)$ wird durch Matrixmultiplikation zu einem unitären Rechts-$M_n(R)$-Modul und zu einem unitären Links-$M_m(R)$-Modul.*

Beweis. Nach Bemerkung 2.67 gilt $\operatorname{End}_R R^n = M_n(R)$, und nach Bemerkung 2.70 (1) ist $E_n = \mathrm{id}_{R^n}$ die Eins. Es folgt (2).

Nach Bemerkung 2.70 (2) entsprechen die invertierbaren Matrizen genau den umkehrbaren linearen Abbildungen, und es folgt (1).

Die Punkte (3) und (4) folgen aus den entsprechenden Punkten in Folgerung 2.42 und Folgerung 2.66 (2) und (4). □

2.72. Bemerkung. Es sei R Ring mit Eins und M ein Rechts-R-Modul. In Definition 2.43 haben wir den dualen Links-R-Modul

$$M^* = \operatorname{Hom}_R(M; R)$$

eingeführt. Im Spezialfall $M = R^m$ folgt nach den Identifikation aus Bemerkung 2.67 und 2.65 (4), dass

$$(R^m)^* = \operatorname{Hom}_R(R^m, R) = M_{1,m}(R) = {}^mR \; .$$

Somit der Links-R-Modul der m-elementigen Zeilen dual zum Rechts-R-Modul der m-elementigen Spalten.

Es sei $(e_1, \dots, e_m)$ die Standardbasis des R^m. Als Basis der Zeilen wählen wir $\varepsilon_1, \dots, \varepsilon_m$, wobei an der i-ten Stellen von ε_i eine 1 steht und sonst nur Nullen. Diese Basis nennen wir die *Standardbasis* von ${}^mR$. Zwischen den Basen $(e_j)_j$ und $(\varepsilon_i)_i$ besteht die folgenden Beziehung:

$$\varepsilon_i(e_j) = \sum_{k=1}^{m} \delta_{ik}\delta_{kj} = \delta_{ij} \ ;$$

wir sagen dazu, dass die Basis $(\varepsilon_i)_i$ *dual* zur Basis $(e_j)_j$ ist.

Für Links-Moduln N können wir analog den Dualraum ${}^*N = {}_R\mathrm{Hom}(N, R)$ definieren. Analog zu oben folgt ${}^*({}^mR) = R^m$, und wiederum ist die Basis $(e_j)_j$ zur Basis $(\varepsilon_i)_i$ dual.

Zum Schluss dieses Abschnitts wollen wir auch in freien Moduln mit festen Basen mit Koordinaten und Matrizen rechnen. Dafür ist es praktisch, den Begriff einer Basis etwas anders zu fassen als in Definition 2.28.

2.73. Definition. Es sei R ein Ring mit Eins und M ein Rechts-R-Modul. Ein Tupel $(b_1, \dots, b_m)$ aus Elementen von M heißt

(1) *Erzeugendensystem,* wenn $\{b_1, \dots, b_m\}$ eine Erzeugermenge bildet;
(2) *linear abhängig,* wenn es $(r_1, \dots, r_m) \in R^m \setminus \{0\}$ gibt, so dass
$$b_1 \,.\, r_1 + \dots + b_m \,.\, r_m = 0 \ ,$$
und sonst *linear unabhängig;*
(3) (*angeordnete*) *Basis* von M, wenn es ein linear unabhängiges Erzeugendensystem bildet.

Der Hauptunterschied ist, dass wir hier mit Tupeln anstelle von Mengen arbeiten. Insbesondere hat jedes Basiselement jetzt einen Index aus $\{1, \dots, m\}$, und wegen (2) darf kein Vektor doppelt vorkommen, was in einer Menge wie in Definition 2.28 gar nicht möglich ist. Im Folgenden seien alle Basen angeordnet.

2.74. Bemerkung. Es sei M ein freier Rechts-R-Modul mit Basis $B = (b_1, \dots, b_m)$. Wie in Definition 2.33 erhalten wir eine Basisabbildung $B\colon R^m \to M$ mit

$$B\left(\begin{pmatrix} r_1 \\ \vdots \\ r_m \end{pmatrix}\right) = \sum_{i=1}^{m} b_i \,.\, r_i \ .$$

Wir benutzen hier den gleichen Buchstaben wie für die Basis B, und tatsächlich verhält sich die Basisabbildung oben formal wie die Matrixmultiplikation der „Zeile“ B aus Modulementen mit der Spalte $(r_i)_i \in R^m$.

Wie Bemerkung 2.34 ist die Basisabbildung bijektiv, und ihre Umkehrabbildung ist die Koordinatenabbildung $M \to R^m$. Die Basisabbildung ist auch

linear, also ein Isomorphismus, denn für alle $(r_i)_i$, $(s_i)_i \in R^m$ und alle $t \in R$ gilt

$$\begin{aligned} B\big((r_i)_i + (s_i)_i\big) &= \sum_{i=1}^{m} b_i \,.\, (r_i + s_i) \\ &= \sum_{i=1}^{m} b_i \,.\, r_i + \sum_{i=1}^{m} b_i \,.\, s_i = B\big((r_i)_i\big) + B\big((s_i)_i\big) \\ \text{und} \quad B\big((r_i)_i \,.\, t\big) &= \sum_{i=1}^{m} b_i \,.\, (r_i \cdot t) = \left(\sum_{i=1}^{m} b_i \,.\, r_i\right) . t = B\big((r_i)_i\big) \,.\, t \,. \end{aligned}$$

Nach Proposition 2.40 ist die Koordinatenabbildung dann ebenfalls linear. Die Linearität dieser Abbildungen bedeutet, dass wir mit den Koordinaten genauso rechnen dürfen wie mit den Modulelementen selbst. Es ist also egal, ob wir erst Vektoren addieren und mit Skalaren multiplizieren und dann Koordinaten bilden, oder erst Koordinaten der einzelnen Modulelemente nehmen und dann mit ihnen weiterrechnen.

Sei jetzt umgekehrt M ein beliebiger Rechts-R-Modul, sei $B\colon R^m \to M$ eine lineare Abbildung und $b_i = B(e_i) \in M$ für $i = 1, \ldots, m$. Dann bildet $(b_1, \ldots, b_m)$ genau dann ein Erzeugendensystem, wenn B surjektiv ist, und genau dann linear unabhängig, wenn B injektiv ist. Also entsprechen die m-elementigen Basen von M genau den Isomorphismen $B\colon R^m \to M$.

2.75. Folgerung. *Es sei R ein Ring mit Eins, es sei M ein freier Rechts-R-Modul mit Basis $B = (b_1, \ldots, b_m)$ und N ein freier Rechts-R-Modul mit Basis $C = (c_1, \ldots, c_n)$. Dann entspricht jeder linearen Abbildung $F\colon N \to M$ genau eine Matrix A, die* Abbildungsmatrix von F bezüglich B und C *so dass das folgende Diagramm kommutiert.*

$$\begin{array}{ccc} N & \xrightarrow{F} & M \\ {\scriptstyle C}\uparrow & & \uparrow{\scriptstyle B} \\ R^n & \xrightarrow{A} & R^m \end{array}$$

Dabei stehen in der j-ten Spalte von A die B-Koordinaten des Bildes des j-ten Basisvektors c_j. Für jedes Element $v = C((r_i)_i) \in N$ hat das Bild $F(v)$ also die Koordinaten $A \cdot (r_i)_i$.

Beweis. Wir bezeichnen die Umkehrabbildung der Basisabbildung B mit B^{-1} und setzen

$$A = B^{-1} \circ F \circ C \,,$$

dann kommutiert das Diagramm offensichtlich. Die restlichen Aussagen ergeben sich aus Folgerung 2.66. □

2.76. Bemerkung. Der Spezialfall $M = N$ und $F = \mathrm{id}_M$ ist interessant. In diesem Fall erhalten wir das kommutative Diagramm

$$\begin{array}{ccc} & M & \\ {\scriptstyle C}\nearrow & & \nwarrow{\scriptstyle B} \\ R^n & \xrightarrow{\ A\ } & R^n \end{array} .$$

Multiplikation mit der Matrix A macht aus C-Koordinaten B-Koordinaten. Also besteht die j-te Spalte von $A = (a_{ij})_{i,j}$ aus den B-Koordinaten des Vektor c_j, das heißt

$$c_j = \sum_{i=1}^{n} b_i a_{ij} \ .$$

Anders formuliert erhalten wir die Vektoren der Basis C, indem wir die „Zeile“ B mit den Spalten von A multiplizieren. Aus diesem Grund nennt man die Matrix A auch *Basiswechselmatrix.* Die obigen Sachverhalte sind zwei Lesarten der „Gleichung“ $C = BA$. Man beachte, dass die „Richtung“ des Basiswechsels für die Koordinaten („von C nach B“) und für die Basisvektoren („von B nach C“) genau umgekehrt ist. Um Fehler zu vermeiden, sollte man daher immer das obige kommutative Diagramm vor Augen haben.

2.77. Proposition. *Es sei M ein freier R-Modul mit Basis $B(b_1, \ldots, b_m)$. Dann besteht eine Bijektion zwischen der Menge der m-elementigen Basen von M und der allgemeinen linearen Gruppe $GL(n, R)$, die jeder Basis $C = B \cdot A$ die Basiswechselmatrix A zuordnet.*

Beweis. Zunächst sei $C = (c_j)_j$ eine weitere Basis von M. Dann erhalten wir eine Basiswechselmatrix A wie in Bemerkung 2.76. Da die Basisabbildungen zu B und C Isomorphismen sind, ist $A = B^{-1} \circ C$ ebenfalls ein Isomorphismus, also ist die zugehörige Matrix nach Bemerkung 2.70 (2) invertierbar. Außerdem wird sie durch B und C eindeutig festgelegt.

Sei jetzt A eine invertierbare Matrix, dann ist $C = B \circ A \colon R^m \to M$ ein Isomorphismus. Die Bilder $c_1, \ldots, c_m$ der Standardbasisvektoren $e_1, \ldots, e_m$ von R^m bilden eine Basis von M, und C ist die zugehörige Basisabbildung. Denn sei $m \in M$ ein Element mit den B-Koordinaten $r_1, \ldots, r_m$, dann folgt

$$m = B((r_j)_j) = \big(C \circ A^{-1}\big)((r_j)_j) = C\big(A^{-1} \cdot (r_j)_j\big) = \sum_{i=1}^{m} c_i \cdot s_i \ ,$$

wobei s_i die i-te Komponente der Spalte $A^{-1} \cdot (r_j)_j$ sei. Mithin lässt sich jedes Element von M als Linearkombination der c_i schreiben, das heißt, die Elemente $c_1, \ldots, c_m$ erzeugen M.

Wenn eine dieser Linearkombinationen das Nullelement $0 \in M$ ergibt, folgt umgekehrt, dass

$$0 = \sum_{i=1}^{m} c_i \cdot s_i = B\big(A \cdot (s_i)_i\big) \ ,$$

also ist $A \cdot (s_i)_i = 0$ und wegen Invertierbarkeit von A auch $(s_i)_i$. Also ist das Tupel $(c_1, \ldots, c_m)$ linear unabhängig und bildet daher eine Basis. □

2.78. Bemerkung. Wir können jetzt auch überlegen, wie sich die Abbildungsmatrix aus Proposition 2.75 verhält, wenn wir eine der beiden Basen durch eine andere ersetzen. Wir betrachten dazu die kommutativen Diagramme

Hier ist D eine neue Basis von M und $P \in GL(m, R)$ die zugehörige Basiswechselmatrix, und E ist eine Basis von N und $Q \in GL(n, R)$ die zugehörige Basiswechselmatrix.

Es sei wieder $(\varepsilon_i)_i$ die Standardbasis des Raumes ${}^mR = \mathrm{Hom}_R(R^m, R)$ der Zeilen der Länge R.

2.79. Proposition. *Es sei R ein Ring mit Eins und M ein freier Modul mit Basis $B = (b_1, \ldots, b_m)$. Dann bilden die einzelnen Komponentenfunktionen $\beta_i = \varepsilon_i \circ B^{-1} \colon M \to R$ der Koordinatenabbildung $B^{-1} \colon M \to R^m$ eine Basis $(\beta_i)_i$ des dualen Moduls B^*. Sie ist* dual *zur Basis B, das heißt, für alle i, j gilt*

$$\beta_i(b_j) = \delta_{ij} \; . \tag{1}$$

Beweis. Die Abbildungen β_i sind offensichtlich Elemente des dualen Moduls M^*. Da $b_j = B(e_j)$ gilt, folgt (1), denn

$$\beta_i(b_j) = \big(\varepsilon_i \circ B^{-1}\big)(B(e_j)) = \varepsilon_i(e_j) = \delta_{ij}$$

nach Bemerkung 2.72.

Aus (1) folgt, dass $(\beta_i)_i$ eine Basis von M^* ist. Sei etwa $F \in M^* = \mathrm{Hom}_R(M, R)$, und sei $m = B((r_j)_j) \in M$ ein Element mit den B-Koordinaten $(r_j)_j \in R^m$, dann gilt

$$\begin{aligned} F(m) = \sum_{j=1}^{m} F(b_j) \cdot r_j &= \sum_{i,j=1}^{m} F(b_i) \cdot \delta_{ij} \cdot r_j \\ &= \sum_{i,j=1}^{m} F(b_i) \cdot \beta_i(b_j) \cdot r_j = \left(\sum_{i=1}^{m} F(b_i) \cdot \beta_i \right)(m) \; , \end{aligned}$$

somit $F = \sum_{i=1}^{m} F(b_i) \cdot \beta_i$, und die Elemente β_i erzeugen M^*.

Sie sind auch linear unabhängig, denn wäre $\sum_{i=1}^{m} s_i \cdot \beta_i = 0$, so würde für alle j folgen, dass

$$s_j = \sum_{i=1}^{m} s_i \cdot \delta_{ij} = \sum_{i=1}^{m} s_i \cdot \beta_i(b_j) = 0 \; .$$

Also ist das Tupel $(\beta_1, \ldots, \beta_m)$ linear unabhängig und bildet daher eine Basis. □

Zum Schluss betrachten wir als Spezialfall bestimmte Basen des $\mathbb{R}^n$, mit denen man besonders gut arbeiten kann. Außerdem brauchen wir den Begriff der transponierten und der adjungierten Matrix.

2.80. Definition. Es sei $A = (a_{ij})_{i,j} \in M_{m,n}(R)$ eine Matrix, dann definieren wir die zu A *transponierte Matrix* $A^t \in M_{n,m}(R)$ durch $A^t = (a_{ij})_{ji}$. Falls $R = \mathbb{C}$ oder $\mathbb{H}$, definieren wir die zu A *adjungierte Matrix* $A^* \in M_{n,m}(R)$ durch $A^* = (\bar{a}_{ij})_{j,i}$.

Transponierten macht zum Beispiel aus Zeilen Spalten und umgekehrt. In Büchern wird häufig $(r_1, \ldots, r_n)^t$ für die Spalte $\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix}$ geschrieben.

Wir können das Standardskalarprodukt auf $\mathbb{R}^n$ zweier Spaltenvektoren $v = (v_i)_i$ und $w = (w_i)_i$ aus Definition 1.51 (1) jetzt auch schreiben als

$$\langle v, w \rangle = \sum_{i=1}^{n} v_i \cdot w_i = v^t \cdot w \ .$$

2.81. Definition. Eine *Orthonormalbasis* des $\mathbb{R}^n$ ist ein Tupel $B = (b_1, \ldots, b_n)$ von Vektoren im $\mathbb{R}^n$, so dass für alle i, j gilt

$$\langle b_i, b_j \rangle = \delta_{ij} \ .$$

2.82. Proposition. *Es sei $B = (b_1, \ldots, b_n)$ eine Orthonormalbasis des $\mathbb{R}^n$. Dann ist B eine Basis, und für jeden Vektor $v \in \mathbb{R}^n$ gilt*

$$v = \sum_{i=1}^{n} b_i \,.\, \langle b_i, v \rangle \ .$$

Die Matrix B mit den Spalten b_1, …, b_n ist invertierbar mit $B^{-1} = B^t$.

Man beachte, dass die Matrix B jetzt tatsächlich die Matrix der Basisabbildung B ist, so dass die obige Merkregel aus Bemerkung 2.74 hier wirklich richtig ist. Im Spezialfall einer Orthonormalbasis wird die Koordinatenabbildung also gegeben durch $B^{-1} = B^t$. Im Allgemeinen lässt sich das Inverse einer Matrix nicht so leicht bestimmen, und allgemeine Verfahren zum Invertieren von Matrizen lernen wir erst in den nächsten zwei Kapiteln kennen.

Beweis. Wir schreiben $b_j = (b_{ij})_i$, so dass $B = (b_{ij})_{i,j}$. Dann gilt also

$$\langle e_i, b_j \rangle = \sum_{k=1}^{n} \delta_{ki} b_{kj} = b_{ij} \ .$$

Wir versuchen, den Vektor e_i als Linearkombination der b_j darzustellen. Dazu setzen wir

$$r_i = e_i - \sum_{j=1}^{n} b_j \,.\, \langle b_j, e_i \rangle \in \mathbb{R}^n \ .$$

Es folgt

$$\begin{aligned}\|r_i\|^2 &= \left\langle e_i - \sum_{j=1}^n b_j \,.\, \langle b_j, e_i\rangle, e_i - \sum_{k=1}^n b_k \,.\, \langle b_k, e_i\rangle \right\rangle \\ &= \|e_i\|^2 - 2\sum_{j=1}^n \langle e_i, b_j\rangle \cdot \langle b_j, e_i\rangle + \sum_{j,k=1}^n \underbrace{\langle b_j, b_k\rangle}_{=\delta_{jk}} \cdot \langle b_j, e_i\rangle \cdot \langle b_k, e_i\rangle \\ &= 1 - \sum_{j=1}^n b_{ij}^2 \,.\end{aligned}$$

Nun ist $\|r_i\|^2 \geq 0$ nach Bemerkung 1.52 (3). Auf der anderen Seite liefert Summieren über i, dass

$$\sum_{i=1}^n \|r_i\|^2 = n - \sum_{i=1}^n \sum_{j=1}^n b_{ij}^2 = n - \sum_{j=1}^n \sum_{i=1}^n b_{ij}^2 = n - \sum_{j=1}^n \langle b_j, b_j\rangle = 0 \,,$$

so dass $\|r_i\|^2 = 0$ und daher $r_i = 0$ für alle i, und somit gilt

$$e_i = \sum_{j=1}^n b_j \,.\, \langle b_j, e_i\rangle = \sum_{j=1}^n b_j \,.\, b_{ij} \,.$$

Wir stellen den Vektor $v = (r_i)_i$ in Koordinaten dar und erhalten

$$v = \sum_{i=1}^n e_i \,.\, r_i = \sum_{i,j=1}^n b_j \,.\, \langle b_j, e_i\rangle \,.\, r_i = \sum_{j=1}^n b_j \,.\, \langle b_j, v\rangle \,.$$

Also erzeugen die Vektoren $b_1, \ldots, b_n$ den $\mathbb{R}^n$.

Sie sind auch linear unabhängig, denn aus $b_1 \,.\, r_1 + \cdots + b_n \,.\, r_n = 0$ mit $r_1, \ldots, r_n \in \mathbb{R}$ folgt für alle i, dass

$$r_i = \sum_{j=1}^n \delta_{ij} \cdot r_j = \left\langle b_i, \sum_{i=1}^n b_j \,.\, r_j \right\rangle = \langle b_i, 0\rangle = 0 \,.$$

Also bildet $(b_1, \ldots, b_n)$ eine Basis.

Schließlich berechnen wir noch

$$E_n = (\delta_{ij})_{i,j} = (\langle b_i, b_j\rangle)_{i,j} = \left(\sum_{k=1}^n b_{ki} b_{kj}\right)_{i,j} = B^t \cdot B$$

und

$$\begin{aligned}E_n &= (\delta_{ij})_{i,j} = (\langle e_i, e_j\rangle)_{i,j} \\ &= \left(\left\langle \sum_{k=1}^n b_k \,.\, b_{ik}, \sum_{\ell=1}^n b_\ell \,.\, b_{j\ell} \right\rangle\right)_{i,j} = \left(\sum_{k=1}^n b_{ik} b_{jk}\right)_{i,j} = B \cdot B^t\end{aligned}$$

und schließen daraus, dass $B^{-1} = B^t$. □

Es folgt eine kurze Zwischenbilanz zum Ende des Abschnitts: In Abschnitt 2.1 haben wir Gruppen, Ringe und Körper kennengelernt. Uns interessieren dabei am meisten Ringe mit Eins, darunter fallen auch Körper und Schiefkörper.

Im Abschnitt 2.2 haben wir Moduln betrachtet. In Zukunft werden wir fast nur noch mit unitären Moduln arbeiten, dazu gehören auch die Vektorräume über Körpern und Schiefkörpern. In den Beispielen 2.30 und 2.31 haben wir die frei erzeugten Moduln $R^{(I)}$ und speziell den Raum R^n der Spalten kennengelernt kennengelernt. Freie Moduln werden besondern wichtig werden, vor allem, da Vektorräume immer freie Moduln sind.

Der Inhalt von Abschnitt 2.3 waren lineare Abbildungen. Wir haben gesehen, wie man lineare Abbildungen $R^n \to R^m$ und allgemeiner zwischen endlich erzeugten freien Moduln durch Matrizen darstellen kann. Außerdem haben wir Folgerung 2.42 mit Hilfe von Matrizen neu interpretiert. Als Spezialfall haben wir den dualen Modul aus Definition 2.43 betrachtet.

In Abschnitt 2.4 ging es um Unterräume, Quotienten und (direkte) Summen. Diese Konstruktionen schauen wir uns näher an, sobald wir mehr über Basen von Vektorräumen wissen.

Schließlich haben wir in Abschnitt 2.5 Matrixrechnung kennengelernt. Sie hat zweierlei Aufgaben: zum einen erlaubt sie es, mit linearen Abbildungen zu rechnen, indem man sie durch Systeme von Zahlen darstellt. Dieser Aspekt ist später zum Beispiel in der Numerik sehr wichtig. Dazu muss man zunächst für jedes Modul eine Basis wählen — im Fall R^m wird das häufig die Standardbasis sein. Zum anderen haben wir Matrizen aber auch benutzt, um den Raum aller linearen Abbildungen besser zu verstehen. Dieser Aspekt wird im Folgenden häufig wichtig sein.

KAPITEL 3

Vektorräume über Körpern und Schiefkörpern

In diesem Kapitel lernen wir typische Eigenschaften von Vektorräumen über (Schief-) Körpern kennen. Insbesondere hat jeder Vektorraum eine Basis, ist also als Modul frei. Außerdem lernen wir das Gauß-Verfahren zum Lösen linearer Gleichungssysteme kennen. Solche linearen Gleichungssystem treten sowohl in der Praxis als auch in der Theorie häufig auf. So können wir das Gauß-Verfahren auch benutzen, um festzustellen, ob eine Matrix invertierbar ist, und gegebenenfalls die inverse Matrix zu bestimmen.

Alles, was in diesem Abschnitt passiert, beruht darauf, dass wir in einem Schiefkörper dividieren können. Auf der anderen Seite benötigen wir das Kommutativgesetz in diesem Abschnitt (noch) nicht. Für den Rest dieses Kapitels sei $\Bbbk$ ein Schiefkörper, also zum Beispiel $\Bbbk = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ oder $\mathbb{Z}/p\mathbb{Z}$ für p prim. Wenn nichts anderes angegeben wird, seien alle $\Bbbk$-Vektorräume nach wie vor Rechts-Vektorräume, und alle Basen seien angeordnet wie in Definition 2.73.

3.1. Basen

Wir haben spätestens im Abschnitt 2.5 gesehen, dass wir in freien Moduln weitaus leichter rechnen können als in beliebigen. Und wir haben auch gesehen, dass wir dadurch die Struktur dieser Moduln und der linearen Abbildungen gut beschreiben und verstehen können. Das soll diesen Abschnitt motivieren, in dem wir uns Gedanken über die Existenz von Basen machen wollen. Die beiden Sätze von Steinitz gehören zu den wichtigsten Ergebnissen dieser Vorlesung.

Für das folgende Lemma führen wir noch folgende Notation ein. Es sei $(a_1, \dots, a_n)$ ein Tupel und $1 \leq i \leq n$. Dann erhalten wir ein neues Tupel durch Weglassen von a_i, das wir bezeichnen wollen als

$$\big(a_1, \dots, \widehat{a_i}, \dots, a_n\big) = (a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n) \,.$$

3.1. Lemma. *Es sei V ein $\Bbbk$-Vektorraum und $(v_1, \dots, v_n)$ ein linear abhängiges Tupel von Vektoren aus V. Dann existiert ein $j \in \{1, \dots, n\}$, so dass sich v_j als Linearkombination der Vektoren $\big(v_1, \dots, \widehat{v_j}, \dots, v_n\big)$ darstellen lässt. Falls das Tupel $(v_1, \dots, v_r)$ linear unabhängig ist für ein $r < n$, können wir $j > r$ wählen.*

Beweis. Da das Tupel $(v_1, \dots, v_n)$ linear abhängig ist, existieren k_1, …, $k_n \in \Bbbk$, so dass

$$\sum_{i=1}^{n} v_i \, k_i = 0 \in V \,.$$

Wäre $k_{r+1} = \cdots = k_n = 0$, so erhielten wir eine nicht-triviale Linearkombination des Tupels $(v_1, \ldots, v_r)$, die den Nullvektor darstellt. Da $(v_1, \ldots, v_r)$ nach Voraussetzung linear unabhängig ist, ist das nicht möglich. Wir finden also $j > r$ mit $k_j \neq 0$. Aus der obigen Gleichung folgt jetzt

$$v_j = -\sum_{i \neq j} v_i \, (k_i \, k_j^{-1}) \; . \qquad \square$$

3.2. Bemerkung. Man beachte, dass wir im Beweis durch k_j dividiert haben. Wir können daher nicht erwarten, dass das Lemma für Moduln über beliebigen Ringen gilt. Als Gegenbeispiel betrachte $\mathbb{Z}$ als $\mathbb{Z}$-Modul. Das Tupel $(2, 3)$ ist linear abhängig, da $2 \cdot 3 - 3 \cdot 2 = 0$. Aber weder ist 2 eine Linearkombination, also ein Vielfaches, der 3, noch umgekehrt. Die Voraussetzung, dass $\Bbbk$ ein (Schief-) Körper ist, ist also notwendig. Für die meisten Aussagen in diesem und im nächsten Abschnitt finden wir Gegenbeispiele in Moduln über beliebigen Ringen.

3.3. Satz (Basisergänzungssatz von Steinitz)**.** *Es sei V ein $\Bbbk$-Vektorraum. Es sei $(v_1, \ldots, v_r)$ ein Tupel linear unabhängiger Vektoren, und $\{w_1, \ldots, w_s\} \subset V$ sei eine endliche Erzeugermenge. Dann gibt es $n \geq r$ und Zahlen $i(r+1), \ldots, i(n) \in \{1, \ldots, s\}$, so dass das Tupel*

$$(v_1, \ldots, v_r, w_{i(r+1)}, \ldots, w_{i(n)})$$

eine Basis von V bildet.

Wir bezeichnen das Erzeugnis der Vektoren eines Tupels B mit $\langle B \rangle$, siehe Definition 2.24.

Beweis. Wir setzen zunächst $n = r$ und $i(r) = 0$, und starten mit dem Tupel $B = (v_1, \ldots, v_r)$. Dann gehen wir die Vektoren w_i für $i = 1, \ldots, s$ der Reihe nach durch.

Wenn wir uns um w_i kümmern, nehmen wir an, dass wir bereits ein linear unabhängiges Tupel

$$B = (v_1, \ldots, v_r, w_{i(r+1)}, \ldots, w_{i(n)})$$

konstruiert haben mit $i(1) < \cdots < i(n) < i$, so dass

$$\{w_1, \ldots, w_{i-1}\} \subset \langle B \rangle$$

für alle $j < i$.

Dann gibt es zwei Möglichkeiten. Falls das Tupel

$$(v_1, \ldots, v_r, w_{i(r+1)}, \ldots, w_{i(n)}, w_i)$$

linear abhängig ist, ist nach Lemma 3.1 der Vektor w_i eine Linearkombination der Vektoren aus B, das heißt, es gilt $w_i \in \langle B \rangle$. Es folgt also

$$\{w_1, \ldots, w_i\} \subset \langle B \rangle \; ,$$

und wir können den Vektor w_i überspringen.

Falls das obige Tupel linear unabhängig ist, wird es unser neues B, also

$$B = (v_1, \ldots, v_r, w_{i(r+1)}, \ldots, w_{i(n)}, w_i) \; .$$

Selbstverständlich gilt nun auch $w_i \in \langle B \rangle$. Wir setzen also $i(n+1) = i$ und erhöhen anschließend n um 1.

Am Schluss erhalten wir ein lineares Tupel

$$B = (v_1, \ldots, v_r, w_{i(r+1)}, \ldots, w_{i(n)})$$

mit der Eigenschaft, dass

$$\{w_1, \ldots, w_s\} \subset \langle B \rangle \; .$$

Nach Voraussetzung ist jeder Vektor $v \in V$ eine Linearkombination der Vektoren $w_1, \ldots, w_s$. Jeder dieser Vektoren ist wiederum eine Linearkombination der Vektoren aus B. Indem wir diese Darstellungen der w_j in die obige Darstellung von v einsetzen, erhalten wir v als Linearkombination der Vektoren aus B. Also ist B nun auch ein Erzeugendensystem, und somit eine Basis. □

3.4. Satz (Basisaustauschsatz von Steinitz)**.** *Es sei V ein $\Bbbk$-Vektorraum, es sei $(v_1, \ldots, v_r)$ ein linear unabhängiges Tupel, und $(w_1, \ldots, w_s)$ sei ein Erzeugensystem. Dann gilt $r \leq s$.*

Beweis. Wir dürfen annehmen, dass $B_0 = (v_1, \ldots, v_r)$ bereits eine Basis von V ist. Anderfalls ergänzen wir nach Satz 3.3 zu einer Basis

$$(v_1, \ldots, v_r, w_{i(r+1)}, \ldots, w_{i(n)}) \; .$$

Das folgende Argument wird uns $n \leq s$ liefern. Da $r \leq n$, folgt erst recht $r \leq s$.

Wir gehen die Indizes $j = 1, \ldots, r$ der Reihe nach durch. Wenn wir j behandeln, nehmen wir an, dass

$$B_{j-1} = \big(v_j, \ldots, v_r, w_{i(r+1)}, \ldots, w_{i(n_{j-1})}\big)$$

bereits eine Basis von V ist mit der Länge

$$(r - (j-1)) + (n_j - r) = n_{j-1} - (j-1) \geq r \; .$$

Durch Weglassen von v_j entsteht ein Tupel

$$B'_j = \big(v_{j+1}, \ldots, v_r, w_{i(r+1)}, \ldots, w_{i(n_{j-1})}\big) \; ,$$

das nach wie vor linear unabhängig ist. Wäre $v_j \in \langle B'_j \rangle$, also

$$v_j = \sum_{\ell=j+1}^{r} v_\ell \, k_\ell + \sum_{\ell=r+1}^{n_{j-1}} w_{i(\ell)} \, k_\ell$$

für geeignete $k_1, \ldots, k_{n_{j-1}} \in \Bbbk$, dann erhielten wir eine nichttriviale Linearkombination

$$0 = v_j - \sum_{\ell=j+1}^{r} v_\ell \, k_\ell - \sum_{\ell=r+1}^{n_{j-1}} w_{i(\ell)} \, k_\ell \; ,$$

was nicht möglich ist, da B_{j-1} nach Annahme linear unabhängig ist.

Es folgt $v_j \notin \langle B'_j \rangle$, also ist B'_j keine Basis. Nach Satz 3.3 können wir B'_j zu einer Basis

$$B_j = \big(v_{j+1}, \dots, v_r, w_{i(r+1)}, \dots, w_{i(n_j)}\big)$$

ergänzen, indem wir mindestens einen weiteren Vektor aus $\{w_1, \dots, w_s\}$ ergänzen. Es folgt also $n_j \geq n_{j-1} + 1$, und somit

$$r \leq n_{j-1} - (j-1) \leq n_j - j \; .$$

Zum Schluss erhalten wir eine Basis

$$B_r = \big(w_{i(r+1)}, \dots, w_{i(n_r)}\big)$$

der Länge $n_r - r \geq r$. Für $j \neq k$ folgt $i(j) \neq i(k)$, ansonsten erhielten wir die nichttriviale Linearkombination

$$0 = w_{i(j)} - w_{i(k)} \; .$$

Also enthält das ursprüngliche Tupel $(w_1, \dots, w_s)$ mindestens $n_r - r \geq r$ verschiedene Elemente, es folgt $r \leq s$. □

3.5. Folgerung. *Es sei V ein endlich erzeugter $\mathbb{k}$-Vektorraum. Dann existiert eine Basis $B = (v_1, \dots, v_n)$ von V, und alle anderen Basen von V haben ebenfalls n Elemente.*

Selbstverständlich gelten analoge Aussagen auch für Links-$\mathbb{k}$-Vektorräume.

Beweis. Es sei $(w_1, \dots, w_s)$ ein Erzeugendensystem von V. Der Basisergänzungssatz 3.3 liefert uns, ausgehend vom leeren Tupel () mit $r = 0$, eine Basis $B = (v_1, \dots, v_n)$ von V, deren Länge $n \leq s$ endlich ist.

Sei nun $C \subset V$ eine beliebige ungeordnete Basis von V. Wir können jeden Vektor w_i als Linearkombination von Vektoren aus C darstellen, dazu benötigen wir aber nur endlich viele. Da $(w_1, \dots, w_s)$ Erzeugendensystem ist, ist jeder Vektor $v \in V$ als Linearkombination der w_i darstellbar. In diese Linearkombination setzen wir die obigen Darstellungen der w_i ein. Insgesamt erhalten wir v als Linearkombination der Vektoren aus C, wobei wir aber nur eine feste endliche Teilmenge $C_0 \subset C$ benötigen, nämlich nur diejenigen Elemente von C, die in einer der Darstellungen der w_i mit Koeffizient $\neq 0$ vorkommen. Alle anderen Vektoren $c \in C \setminus C_0$ lassen sich als Linearkombination der w_i darstellen, also auch als Linearkombination der Vektoren aus C_0. Wäre $C \neq C_0$, so wäre C insbesondere linear abhängig. Wir schließen also, dass die Basis C endlich ist.

Jetzt können wir C anordnen zu $(u_1, \dots, u_s)$. Indem wir B als linear unabhängiges Tupel und C als Erzeugendensystem auffassen, erhalten wir $n \leq s$ aus dem Basisaustauschsatz 3.4. Wir können die Rolle der beiden Basen auch vertauschen, und erhalten $s \leq n$. Also haben B und C gleich viele Elemente. □

3.6. Bemerkung. Man kann analoge Sätze auch für beliebige, nicht notwendig endlich erzeugte $\mathbb{k}$-Vektorräume beweisen. Dazu braucht man allerdings ein weiteres Axiom für die zugrundeliegende Mengenlehre, das *Auswahlaxiom.* Es ist äquivalent zum folgenden *Lemma von Zorn* (zuerst formuliert von Kuratowski):

Es sei M eine Menge mit einer Halbordnung $\preceq \subset M \times M$, siehe Definition 1.34. Wenn zu jeder total geordneten Teilmenge, also zu jeder Teilmenge $U \subset M$, für die die Einschränkung $\preceq \cap (U \times U)$ eine Ordnung ist, eine obere Schranke existiert, also ein Element $m \in M$ mit $u \preceq m$ für alle $u \in U$, dann gibt es ein maximales Element in M, also ein Element $m_0 \in M$, so dass $m_0 \preceq n$ für kein $n \in M \setminus \{m_0\}$ gilt.

Um jetzt beispielsweise den Basisergänzungssatz 3.3 zu verallgemeinern, starten wir mit einer linear unabhängigen Teilmenge $U \subset V$ und einer Erzeugermenge $W \subset V$. Wir betrachten die Menge

$$\mathcal{M} = \left\{ A \subset V \;\middle|\; A \text{ ist linear unabhängig und } U \subset A \subset U \cup W \right\} \subset \mathcal{P}(V)$$

mit der Halbordnung „$\subset$“. Sei $\mathcal{U} \subset \mathcal{M}$ eine total geordnete Teilmenge, dann betrachten wir

$$M = \bigcup \mathcal{U} = \left\{ v \in V \;\middle|\; \text{es gibt ein } A \in \mathcal{U} \text{ mit } v \in A \right\} .$$

Wenn eine Linearkombination von Elementen aus M den Nullvektor darstellt, gibt es nur endlich viele Elemente $a_1, \ldots, a_n \in M$, deren Koeffizienten von 0 verschieden sind. Jeder Vektor a_i liegt in einer Menge $A_i \in \mathcal{U}$. Da $\mathcal{U}$ total geordnet ist, dürfen wir (nach Umnummerieren) annehmen, dass

$$A_1 \subset \cdots \subset A_n \subset M .$$

Aber A_n ist linear unabhängig, also verschwinden auch alle Koeffizienten der Vektoren $a_1, \ldots, a_n$ in der obigen Linearkombination. Das zeigt, dass M linear unabhängig ist, und damit eine obere Schranke für $\mathcal{U}$ in $\mathcal{M}$.

Jetzt wenden wir das Zornsche Lemma auf $\mathcal{M}$ an und erhalten ein maximales Element $B \in \mathcal{M}$. Also ist B eine linear unabhängige Teilmenge von V mit $U \subset B \subset U \cup W$. Maximalität bedeutet, dass die Hinzunahme eines weiteren Vektors $w \in W \setminus B$ die lineare Unabhängigkeit zerstört. Mit ähnlichen Argumenten wie in Lemma 3.1 folgt daraus, dass B bereits den Vektorraum V erzeugt.

Der Nachteil im obigen Beweis besteht darin, dass man im Allgemeinen keine Chance hat, eine Basis explizit anzugeben. Ein Beispiel dafür ist der Raum $\mathbb{R}^{\mathbb{N}}$ aller reellwertigen Folgen, siehe dazu den Kommentar nach Beispiel 2.30. Dennoch kann aus dem allgemeinen Basisergänzungssatz interessante Schlussfolgerungen ziehen, siehe unten.

3.2. Dimension und Rang

Wir benutzen die Basissätze, um ein paar interessante Aussagen über Vektorräume und ihre Unterräume, Quotienten und über lineare Abbildungen zu beweisen.

Aufgrund von Folgerung 3.5 ist die folgende Definition sinnvoll.

3.7. Definition. Es sei V ein endlich erzeugter $\Bbbk$-Vektorraum. Dann ist die *Dimension* $\dim V$ von V die Länge n einer Basis $(v_1, \dots, v_n)$ von V, und wir nennen V *endlichdimensional.* Wenn V keine Basis endlicher Länge besitzt, heißt V *unendlichdimensional.*

Die Begriffe „endlichdimensional“ und „endlich erzeugt“ für Vektorräume sind nach Folgerung 3.5 äquivalent.

3.8. Folgerung. *Sei endlichdimensionale $\Bbbk$-Vektorräume V und W sind genau dann isomorph, wenn $\dim V = \dim W$.*

Beweis. Zu „$\Longrightarrow$“ sei $F\colon V \to W$ ein Isomorphismus. Wir wählen eine Basis $C = (c_1, \dots, c_n)$ von V, wobei $n = \dim V$, und identifizieren wieder C mit der zugehörigen Basisabbildung. Dann ist die Abbildung $B = F \circ C\colon \Bbbk^n \to W$ ein Isomorphismus, und das Diagramm

$$\begin{array}{ccc} V & \xrightarrow{F} & W \\ {\scriptstyle C}\uparrow & & \uparrow{\scriptstyle B} \\ \Bbbk^n & \xrightarrow[E_n]{\mathrm{id}_{\Bbbk^n}} & \Bbbk^n \end{array}$$

kommutiert. Wie im Beweis von Proposition 2.77 überzeugt man sich leicht, dass $b_1 = B(e_1)$, …, $b_n = B(e_n)$ eine Basis von W bilden, so dass insbesondere $\dim W = n = \dim V$.

Zu „$\Longleftarrow$“ sei $n = \dim V = \dim W$. Wir wählen Basen von V und W mit Basisabbildungen $B\colon \Bbbk^n \to W$ und $C\colon \Bbbk^n \to V$. Nach Bemerkung 2.74 sind Basisabbildungen Isomorphismen. Wir erhalten also einen Isomorphismus $F = B \circ C^{-1}\colon V \to W$, so dass das obige Diagramm wieder kommutiert. □

Wir erinnern uns an die Begriffe „direkte Summe“ und „komplementärer Unterraum“ aus Definition 2.56.

3.9. Proposition. *Es sei V ein $\Bbbk$-Vektorraum von endlicher Dimension und $U \subset V$ ein Unterraum. Dann besitzt U ein Komplement $W \subset V$, und es gilt die Dimensionsformel*

$$\dim V = \dim U + \dim W \ .$$

Beweis. Wir beginnen mit einer Basis B von U. Da B als Tupel in V linear unabhängig ist, hat B eine Länge $r = \dim U \leq n = \dim V$. Es sei also $B = (v_1, \dots, v_r)$. Wir ergänzen B zu einer Basis $(v_1, \dots, v_n)$ von V mit dem Basisergänzungssatz 3.3.

Es sei $W = \langle v_{r+1}, \dots, v_n \rangle$, dann ist das Tupel $(v_{r+1}, \dots, v_n)$ eine Basis von W, denn es erzeugt W und ist als Teil einer Basis von V auch linear unabhängig. Insbesondere gilt

$$\dim V = \dim U + \dim W \ .$$

Außerdem gilt

$$U + W = \langle v_1, \dots, v_n \rangle = V \ .$$

Sei nun $v \in U \cap W$. Dann existieren $k_1, \ldots, k_r \in \Bbbk$ und $\ell_{r+1}, \ldots, \ell_n \in \Bbbk$ mit

$$\sum_{i=1}^{r} v_i \, k_i = v = \sum_{j=r+1}^{n} v_j \, \ell_j \ .$$

Beides sind Darstellung als Linearkombination der Basis $(v_1, \ldots, v_n)$. Nach Proposition 2.32 sind die Koordinaten von v eindeutig, also gilt $k_1 = \cdots = k_r = 0 = \ell_{r+1} = \cdots = \ell_n$. Insbesondere folgt $U \cap W = \{0\}$, also $V = U \oplus W$. □

3.10. Folgerung. *Es seien U und W zwei Unterräume eines endlichdimensionalen $\Bbbk$-Vektorraums V. Dann sind äquivalent*

$$V = U \oplus W \ , \tag{1}$$

$$V = U + W \quad \textit{und} \quad \dim U + \dim W \leq \dim V \ , \tag{2}$$

$$U \cap W = \{0\} \quad \textit{und} \quad \dim U + \dim W \geq \dim V \ . \tag{3}$$

Beweis. Die Richtungen „(1) $\Longrightarrow$ (2)“ und „(1) $\Longrightarrow$ (3)“ folgen sofort aus der Definition 2.56 der direkten Summe und Proposition 3.9.

In den Übungen beweisen Sie die Dimensionsformel für Summen

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

Aus (2) schließen wir, dass

$$0 \leq \dim(U \cap W) = \dim U + \dim W - \dim V \leq 0 \ ,$$

aber also wird $U \cap W$ von einer Basis der Länge 0 erzeugt, das heißt $U \cap W = \{0\}$, und es folgt (1).

Aus (3) schließen wir, dass

$$\dim V \geq \dim(U + W) = \dim U + \dim W - \dim\{0\} \geq \dim V \ ,$$

also hat $U + W$ eine Basis der Länge $\dim V$. Wäre $U + W$ eine echte Teilmenge von V, so könnten wir zu einer Basis von V der Länge $\geq \dim V + 1$ ergänzen, im Widerspruch zu Folgerung 3.5. Also gilt $U + W = V$, und wieder folgt (1). □

3.11. Folgerung. *Es sei V ein $\Bbbk$-Vektorraum von endlicher Dimension und $U \subset V$ ein Unterraum. Dann gilt*

$$\dim(V/U) = \dim V - \dim U \ .$$

Beweis. Wir wählen einen zu U komplementären Unterraum $W \subset V$. Aus den Propositionen 2.58 und 3.9 folgt

$$\dim(V/U) = \dim W = \dim V - \dim U \ . \qquad \square$$

3.12. Bemerkung. Wenn V unendlichdimensional ist, können wir mit dem allgemeineren Basisergänzungssatz aus Bemerkung 3.6 immer noch zu jedem Unterraum einen komplementären Unterraum konstruieren. Da man aber unendliche Dimensionen nicht subtrahieren kann, ist die Dimensionsformel in Proposition 3.9 nicht geeignet, um die Dimension des Komplements zu bestimmen.

Als Beispiel betrachten wir den Raum $V = \mathbb{R}^{(\mathbb{N})}$ der endlichen reellwertigen Folgen mit der Basis $(e_j)_{j\in\mathbb{N}}$, wobei wieder $e_j = (\delta_{ij})_{i\in\mathbb{N}}$, siehe dazu den Kommentar nach Beispiel 2.30. Wir betrachten zwei unendlichdimensionale Unterräume

$$U = \langle e_r, e_{r+1}, e_{r+2}, \dots \rangle \qquad \text{und} \qquad W = \langle e_0, e_2, e_4, \dots \rangle \;.$$

Beide sind als Vektorräume isomorph, denn wir können einen Isomorphismus $F\colon U \to W$ angeben mit $F(e_{r+j}) = e_{2j}$ für alle $j \in \mathbb{N}$. Aber U besitzt ein endlichdimensionales Komplement $\langle e_0, \dots, e_{r-1}\rangle$, während W ein unendlichdimensionales Komplement $\langle e_1, e_3, e_5, \dots \rangle$ hat. Und da nach Proposition 2.58 alle Komplemente von U zu V/U isomorph sind, und alle Komplemente von W zu V/W, können wir die Dimension des Komplementes nun nicht mehr aus der Dimension der Räume selbst ablesen.

Übrigens hat auch $\mathbb{R}^{(\mathbb{N})}$ selbst im Raum $\mathbb{R}^{\mathbb{N}}$ aller reellwertigen Folgen ein Komplement. Da wir das aber wieder mit Hilfe des Zornschen Lemma beweisen müssen, können wir das Komplement nicht explizit angeben.

Mit den gleichen Methoden wie oben können wir auch lineare Abbildungen studieren. Unter einer *Blockmatrix* verstehen wir eine Matrix, die durch das Neben- und Untereinanderschreiben von Matrizen passender Größe gebildet wird. Seien etwa $A \in M_{p,r}(\Bbbk)$, $B \in M_{p,s}(\Bbbk)$, $C \in M_{q,r}(\Bbbk)$ und $D \in M_{q,s}(\Bbbk)$, dann ist

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} a_{11} & \dots & a_{1r} & b_{11} & \dots & b_{1s} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{p1} & \dots & a_{pr} & b_{p1} & \dots & b_{ps} \\ c_{11} & \dots & c_{1r} & d_{11} & \dots & d_{1s} \\ \vdots & & \vdots & \vdots & & \vdots \\ c_{q1} & \dots & c_{qr} & d_{q1} & \dots & d_{qs} \end{pmatrix} \in M_{p+q,r+s}(\Bbbk) \;.$$

3.13. Satz (Rangsatz)**.** *Es seien V und W endlich-dimensionale $\Bbbk$-Vektorräume, und es sei $F\colon V \to W$ linear. Dann existieren Basen B von W und C von V, so dass die Abbildungsmatrix A von F bezüglich dieser Basen die* Normalform

$$A = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$$

als Blockmatrix hat, wobei $r = \dim \operatorname{im} F$. Insbesondere gilt die Dimensionsformel

$$\dim \ker F + \dim \operatorname{im} F = \dim V \;.$$

Beweis. Es sei $n = \dim V$ und $r = n - \dim \ker F$. Wir wählen zunächst eine Basis $(c_{r+1}, \dots, c_n)$ von $\ker F$ und ergänzen dann zu einer Basis $(c_1, \dots, c_n)$ von V. Dann ist $U = \langle c_1, \dots, c_r\rangle$ ein Komplement von $\ker F$ in V. Nach dem Homomorphiesatz 2.54 und Proposition 2.58 erhalten wir einen Isomorphismus

$$U \xrightarrow{\cong} V/\ker F \xrightarrow{\cong} \operatorname{im} F \qquad (\text{Komposition: } F|_U)$$

einen Isomorphismus $U \to V/\ker F$. Somit induziert die Basis $(c_1, \ldots, c_r)$ von U eine Basis $(b_1, \ldots, b_r)$ von $\operatorname{im} F$ mit $b_i = F(c_i)$ für alle $1 \leq i \leq r$. Schließlich ergänzen wir zu einer Basis $(b_1, \ldots, b_m)$ von W. Für die Abbildung F gilt also

$$F(c_j) = \begin{cases} b_j & \text{falls } j \leq r, \text{ und} \\ 0 & \text{falls } j > r. \end{cases}$$

Daraus ergibt sich die angegebene Form der Abbildungsmatrix. Außerdem folgt

$$\dim V = \dim \ker F + \dim U = \dim \ker F + \dim \operatorname{im} F \,. \qquad \square$$

3.14. Definition. Es sei $F\colon V \to W$ linear, dann definieren wir den *Rang* von F durch $\operatorname{rg} F = \dim \operatorname{im} F$, falls $\operatorname{im} F$ endlichdimensional ist, ansonsten nennen wir F *von unendlichem Rang.*

Es sei $A \in M_{m,n}(\Bbbk)$ eine Matrix mit den Spalten $a_1, \ldots, a_n \in \Bbbk^m$, dann definieren wir den *Spaltenrang* von A durch $\operatorname{rg}_S A = \dim\langle a_1, \ldots, a_n\rangle$. Analog definieren wir den *Zeilenrang* von A durch $\operatorname{rg}_Z A = \operatorname{rg}_S(A^t)$.

Da wir eine Matrix $A \in M_{m,n}(\Bbbk)$ auch als lineare Abbildung $A\colon \Bbbk^n \to \Bbbk^m$ auffassen können, ist auch $\operatorname{rg} A$ definiert. Manchmal heißt auch die folgende Proposition „Rangsatz“.

3.15. Proposition. *Es sei $A \in M_{m,n}(\Bbbk)$.*

(1) *Der Rang von A ändert sich nicht, wenn man von links oder rechts mit einer invertierbaren Matrix multipliziert.*
(2) *Es gilt $\operatorname{rg}_S A = \operatorname{rg} A = \operatorname{rg}_Z A$.*

Beweis. Es sei zunächst $B \in GL(m, \Bbbk)$ eine invertierbare Matrix. Die zugehörige lineare Abbildung $B\colon \Bbbk^n \to \Bbbk^n$ ist also ein Automorphismus, insbesondere also bijektiv. Es gilt

$$\operatorname{im}(B \circ A) = \operatorname{im}(B|_{\operatorname{im} A}) \,.$$

Die Abbildung $B|_{\operatorname{im} A}\colon \operatorname{im} A \to \operatorname{im}(B \circ A)$ ist sicherlich immer noch injektiv und linear. Sie ist auch surjektiv, da wir das Bild entsprechend eingeschränkt haben. Somit sind $\operatorname{im} A$ und $\operatorname{im}(B \circ A)$ isomorph, und es folgt

$$\operatorname{rg}(B \circ A) = \dim \operatorname{im}(B \circ A) = \dim \operatorname{im} A = \operatorname{rg} A \,.$$

Sei jetzt $C \in GL(n, \Bbbk)$ invertierbar, insbesondere ist $\operatorname{im} C = \Bbbk^n$. Dann gilt

$$\operatorname{im}(A \circ C) = \operatorname{im}(A|_{\operatorname{im} C}) = \operatorname{im}(A|_{\Bbbk^n}) = \operatorname{im} A \,,$$

und es folgt

$$\operatorname{rg}(A \circ C) = \dim \operatorname{im}(A \circ C) = \dim \operatorname{im} A = \operatorname{rg} A \,.$$

Damit ist (1) bewiesen.

Es seien wieder $a_1, \ldots, a_n \in \Bbbk^m$ die Spalten von A. Dann gilt

$$\langle a_1, \ldots, a_n\rangle = \langle A(e_1), \ldots, A(e_n)\rangle = \operatorname{im}(A|_{\langle e_1, \ldots, e_n\rangle}) = \operatorname{im} A \,,$$

also auch

$$\operatorname{rg}_S A = \dim\langle a_1, \ldots, a_n\rangle = \dim \operatorname{im} A = \operatorname{rg} A \,.$$

Insbesondere ist also auch der Spaltenrang invariant unter Multiplikation mit invertierbaren Matrizen von links oder rechts.

Sei wieder $B \in GL(m, \Bbbk)$ invertierbar, und sei $D \in GL(m, \Bbbk)$ die Inverse. Aus den Übungen wissen wir, wie sich das Matrixprodukt unter Transposition verhält. Insbesondere gilt

$$B^t \cdot D^t = (D \cdot B)^t = E_m^t = E_m = (B \cdot D)^t = D^t \cdot B^t \ ,$$

das heißt, die Transponierte B^t ist ebenfalls invertierbar mit Inverser D^t. Seien also $B \in GL(m, \Bbbk)$ und $C \in GL(n, \Bbbk)$, dann gilt für den Zeilenrang

$$\operatorname{rg}_Z(B \cdot A \cdot C) = \operatorname{rg}_S(C^t \cdot A^t \cdot B^t) = \operatorname{rg}_S(A^t) = \operatorname{rg}_Z(A) \ ,$$

genau wie für den Rang und den Spaltenrang.

Wir wählen jetzt Basen B von $\Bbbk^m$ und C von $\Bbbk^n$ wie in Satz 3.13 und erhalten

$$\begin{aligned} \operatorname{rg}_S(A) = \operatorname{rg}_S(B^{-1} \cdot A \cdot C) = \operatorname{rg}_S \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} = r \\ = \operatorname{rg}_Z \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} = \operatorname{rg}_Z(B^{-1} \cdot A \cdot C) = \operatorname{rg}_Z A \ . \end{aligned}$$

Damit ist auch (2) bewiesen. □

3.16. Folgerung. *Es seien $F\colon V \to W$ und $G\colon X \to Y$ zwei lineare Abbildungen zwischen endlich-dimensionalen $\Bbbk$-Vektorräumen. Dann gibt es genau dann Isomorphismen $P\colon V \to X$ und $: W \to Y$, so dass das Diagramm*

(1)
$$\begin{array}{ccc} V & \xrightarrow{F} & W \\ {\scriptstyle P}\downarrow{\scriptstyle \cong} & & {\scriptstyle \cong}\downarrow{\scriptstyle Q} \\ X & \xrightarrow{G} & Y \end{array}$$

kommutiert, wenn

(2) $\quad \dim V = \dim X \ , \qquad \dim W = \dim Y \ , \qquad$ *und* $\qquad \operatorname{rg} F = \operatorname{rg} G \ .$

Beweis. Zu „$\Longrightarrow$“ nehmen wir an, dass Isomorphismen P, Q existieren, so dass das Diagramm (1) kommutiert. Dann folgt die Gleichheit der Dimensionen in (2) bereits aus Folgerung 3.8. Außerdem gilt

$$\operatorname{im} G = \operatorname{im}(G \circ P) = \operatorname{im}(Q \circ F) = \operatorname{im}(Q|_{\operatorname{im} F}) \ ,$$

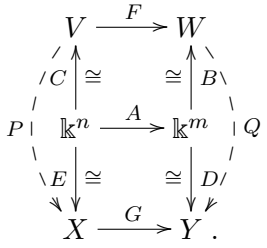
und $Q|_{\operatorname{im} F}\colon \operatorname{im} F \to \operatorname{im}(Q|_{\operatorname{im} F}) = \operatorname{im} G$ ist ein Isomorphismus ist. Also folgt

$$\operatorname{rg} G = \dim \operatorname{im} G = \dim \operatorname{im} F = \operatorname{rg} F \ .$$

Zu „$\Longleftarrow$“ nehmen wir an, dass alle Gleichungen in (2) gelten. Dann wählen wir Basen B von W, C von V, D von Y und E von X wie im Rangsatz 3.13, so dass F und G jeweils durch die gleiche Blockmatrix

$$A = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} \in M_{m,n}(\Bbbk)$$

dargestellt werden, wobei $m = \dim W = \dim Y$, $n = \dim V = \dim X$ und $r = \operatorname{rg} F = \operatorname{rg} G$. Indem wir wieder Basen und Basisabbildungen mit dem gleichen Buchstaben bezeichnen, erhalten wir das kommutative Diagramm



Es folgt (1) für $P = E \circ C^{-1}$ und $Q = D \circ B^{-1}$. □

3.17. Bemerkung. Anhand dieser Folgerung können wir gut erklären, was *Normalformen* und *vollständige Invarianten* sind. Wir geben uns eine Klasse von Objekten vor, in unserem Falle lineare Abbildungen zwischen endlichdimensionalen Vektorräumen. Außerdem sagen wir, wann zwei Objekte „isomorph“ sein sollen, in unserem Falle dann, wenn (1) aus Folgerung 3.16 gilt. Jetzt suchen wir in jeder Isomorphieklasse ein möglichst einfaches Objekt, in unserem Fall die lineare Abbildung $A\colon \Bbbk^n \to \Bbbk^m$ aus dem Rangsatz 3.16. Das heißt, wir bringen eine lineare Abbildung $F\colon V \to W$ „in Normalform“, indem wir die isomorphe Abbildung vom Typ aus Satz 3.13 bestimmen. Dabei kommt es nur darauf an, dass diese Normalform eindeutig bestimmt ist; die benötigten Isomorphismen müssen nicht eindeutig sein. Manchmal ist die Normalform durch eine vollständige Invariante festgelegt, in unserem Fall durch das Tripel

$$(\dim V, \dim W, \dim F) \in \left\{ (m,n,r) \;\middle|\; m,\, n,\, r \in \mathbb{N} \text{ und } r \leq \min(m,n) \right\} .$$

Wenn wir den Wertebereich unser Invarianten wie oben vorgeben, existiert zu jedem möglichen Wert der Invarianten genau eine lineare Abbildung in Normalform.

Ein weiteres Beispiel sind endlich-dimensionale $\Bbbk$-Vektorräume V: hier wäre die „Normalform“ der Spaltenraum $\Bbbk^n$; hier ist die vollständige Invariante die Dimension $\dim V \in \mathbb{N}$. Jeder Vektorraum V ist zu einem eindeutigen $\Bbbk^n$ isomorph, und der Isomorphismus ist die Basisabbildung. Nach Proposition 2.77 ist die Basis nicht eindeutig, sondern die Menge aller Basen von V steht in Bijektion zu $GL(n, \Bbbk)$. Das bedeutet insbesondere, dass man nicht sagen kann, welche Spalte $x \in \Bbbk^n$ einem vorgegebenen Vektor v in der Normalform entspricht, da die Koordinaten x von v von der Wahl der Basis abhängen.

Ein noch einfacheres Beispiel ist die Klasse der endlichen Mengen, siehe Definition 1.30. Wir nennen zwei endliche Mengen M und N *gleichmächtig,* falls es eine bijektive Abbildung $f\colon M \to N$ gibt. Als Normalform erhalten wir die Mengen $\underline{n} = \{\underline{0}, \ldots, \underline{n-1}\}$ aus Bemerkung 1.29 für $n \in \mathbb{N}$ (man könnte auch die Mengen $\{1, \ldots, n\}$ nehmen), und die zugehörige vollständige Invariante ist die Mächtigkeit $\#M$. Die Analogie zwischen Mächtigkeit und Dimension geht relativ weit, beispielsweise gilt für zwei Unterräume U, $W \subset V$ eine ähnliche Formel für $\dim(U+W)$ wie für die Mächtigkeit der Vereinigung zweier endlicher Mengen.

3.3. Lineare Gleichungssysteme

3.18. Definition. Es sei V ein $\Bbbk$-Vektorraum. Eine Teilmenge $A \subset V$ heißt *affiner Unterraum* von V, wenn es einen Untervektorraum $U \subset V$ und ein Element $a_0 \in A$ gibt, so dass

$$A = a_0 + U = \left\{ a_0 + u \;\middle|\; u \in U \right\} .$$

Ein affiner Unterraum $A = a+U$ heißt *endlichdimensional* mit $\dim A = \dim U$, wenn U endlichdimensional ist, sonst *unendlichdimensional.* Seien U, $W \subset V$ Untervektoräume, dann heißen zwei affine Unterräume $a+U$ und $b+W$ *parallel,* wenn $U = W$.

Man beachte, dass in manchen Büchern auch die leere Menge $\emptyset$ als affiner Unterraum der Dimension $\dim \emptyset = -\infty$ betrachtet wird. Wir wollen die leere Menge hier separat betrachten.

3.19. Bemerkung. Ein affiner Unterraum ist also das Bild eines Untervektorraums unter der Verschiebung um a_0.

(1) In der Definition kommt es nicht darauf an, welches $a_0 \in A$ wir wählen. Denn sei $a_1 = a_0 + u_1 \in A$, dann gilt nach dem Unterraumaxiom (U2), dass
$$a_1 + U = a_0 + (u + U) = a_0 + U .$$
(2) Ein affiner Unterraum ist genau dann ein Untervektorraum, wenn $0 \in A$. Die Richtung „$\Longrightarrow$“ folgt aus (U1), und „$\Longleftarrow$“ folgt aus (1), denn aus $0 \in A$ folgt $A = 0 + U = U$ für einen Untervektorraum $U \subset V$. Insbesondere ist jeder Untervektorraum auch ein affiner Unterraum.
(3) Es sei $U \subset V$ ein Untervektorraum. Die Menge aller zu U parallelen affinen Unterräume von V ist gerade der Quotientenraum V/U aus Definition 2.47.
(4) In der Euklidischen Geometrie betrachtet man affine Unterräume des $\mathbb{R}^3$ der Dimensionen 0 (Punkte), 1 (Geraden) und 2 (Ebenen).

Wir kommen zu *linearen Gleichungssystemen*. Gegeben eine Matrix $A \in M_{m,n}(\Bbbk)$, die sogenannte *linke Seite* und einen Vektor $b \in \Bbbk^m$, die *rechte Seite*, suchen wir alle Vektoren $x \in \Bbbk^n$, so dass $A \cdot x = b$. Das heißt, wir suchen die *Lösungsmenge*

$$L = \left\{ x \in \Bbbk^n \;\middle|\; A \cdot x = b \right\} .$$

Wenn wir die Gleichung $A \cdot x = b$ ausschreiben, erhalten wir tatsächlich ein System linearer Gleichungen, nämlich

$$(*) \qquad \begin{array}{ccccccc} a_{11} \cdot x_1 & + & \dots & + & a_{1n} \cdot x_n & = & b_1 , \\ \vdots & & & & \vdots & & \vdots \\ a_{m1} \cdot x_1 & + & \dots & + & a_{mn} \cdot x_n & = & b_m . \end{array}$$

Wir nennen das Gleichungssystem (*) *homogen,* wenn $b = 0$, und *inhomogen,* wenn $b \neq 0$. Das zu $A \cdot x = b$ gehörige homogene Gleichungssystem ist also $A \cdot x = 0$.

Etwas allgemeiner können wir eine lineare Abbildung $F\colon V \to W$ und eine „rechte Seite“ $w \in W$ betrachten, und nach der „Lösungsmenge“

$$L = \left\{ v \in V \;\middle|\; F(v) = w \right\} = F^{-1}(\{w\}) \,,$$

also dem Urbild von w unter F, fragen. Wenn V und W endlichdimensional sind, können wir Basen wählen und F als Matrix schreiben, und erhalten ein lineares Gleichungssystem vom obigen Typ.

3.20. Bemerkung. Lineare Gleichungssysteme treten zum Beispiel beim Lösen der folgenden Probleme auf.

(1) Betrachte $A \in M_{m,n}(\Bbbk)$, dann ist der Kern $\ker A$ von A gerade die Lösungsmenge des homogenen Gleichungssystems $A \cdot x = 0$.
(2) Sei A wie oben, dann liegt $b \in \Bbbk^m$ genau dann im Bild $\operatorname{im} A$ von A, wenn das Gleichungssystem $A \cdot x = b$ eine Lösung hat.
(3) Es sei $B \in M_n\Bbbk$ eine Basis des $\Bbbk^n$. Um die Koordinaten x eines Vektors $v \in \Bbbk^n$ bezüglich B zu bestimmen, müssen wir nach Bemerkung 2.74 das lineare Gleichungssystem $B \cdot x = v$ lösen. Für Orthonormalbasen geht es einfacher, siehe Proposition 2.82.
(4) Eine quadratische Matrix $A \in M_n(\Bbbk)$ ist genau dann invertierbar, wenn eine Matrix $B \in M_n(\Bbbk)$ mit $A \cdot B = E_n$ existiert (Übung). Um die Spalten $b_1, \ldots, b_n$ von B zu bestimmen, müssen wir die n Gleichungssysteme $A \cdot b_i = e_i$ lösen.
(5) Das Bestimmen von Schnittpunkten von Geraden und Ebenen im Euklidischen Raum führt oft auf lineare Gleichungssysteme. Seien etwa eine Gerade G und eine Ebene $E \subset \mathbb{R}^3$ gegeben durch

$$E = \left\{ \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} . r + \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} . s \;\middle|\; r, s \in \mathbb{R} \right\}$$

und

$$G = \left\{ \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} + \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix} . t \;\middle|\; t \in \mathbb{R} \right\} \,,$$

dann bestimmen wir $G \cap E$ durch Lösen des Gleichungssystems

$$\begin{aligned} 2 + r + s &= 3 + 2t \\ -r \quad &= 2 + \;\; t \\ -s &= 1 + \;\; t \end{aligned} \qquad \Longleftrightarrow \qquad \begin{aligned} r + s - 2t &= 1 \,, \\ -r \quad - \;\; t &= 2 \,, \\ -s - \;\; t &= 1 \,. \end{aligned}$$

Die einzige Lösung dieses Systems ist $r = -1$, $s = 0$, $t = -t$; sie führt auf den einzigen Schnittpunkt

$$\begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} - \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix} \,.$$

(6) In der Numerik approximiert man Funktionen, indem man ihre Werte nur an endlich vielen Stützstellen vorgibt. Anschließend nähert man Gleichungen mit zahlreichen unterschiedlichen Operationen (darunter

Multiplikation mit anderen Funktionen und Differentiation) durch lineare Gleichungssysteme in den endlich vielen gesuchten Funktionswerten an und erhält so lineare Gleichungssysteme mit sehr vielen Variablen und Gleichungen. In einer Simulation sind unter Umständen für jeden Zeitschritt mehrere solcher Gleichungssysteme zu lösen. Diese Gleichungssysteme zeichnen sich dadurch aus, dass in jeder Zeile und jeder Spalte der linken Seite A nur sehr wenige Einträge von 0 verschieden sind. Für diese Gleichungssysteme benötigt man schnelle, approximative Lösungsverfahren, die wir hier nicht besprechen werden.

Es folgen einfache, grundätzliche Überlegungen zum Lösungsverhalten linearer Gleichungssysteme.

3.21. Proposition. *Es sei $A \in M_{m,n}(\Bbbk)$ und $b \in \Bbbk^m$.*

(1) *Die Lösungsmenge des homogenen Gleichungssystems $A \cdot x = 0$ ist gerade* $\ker A$.
(2) *Das inhomogene Gleichungssystem $A \cdot x = b$ hat genau dann Lösungen, wenn $b \in \operatorname{im} A$.*
(3) *Es sei $A \cdot x_0 = b$, dann ist die Lösungsmenge des inhomogenen Gleichungssystems $A \cdot x = b$ der affine Unterraum*

$$\left\{ x \in \Bbbk^n \;\middle|\; A \cdot x = b \right\} = x_0 + \ker A \,.$$

Beweis. Die Aussagen (1) und (2) sind gerade die Punkte (1) und (2) aus Bemerkung 3.20. Zu (3) beachten wir, dass aus $A \cdot x_0 = b$ folgt, dass

$$A \cdot x = b \quad \Longleftrightarrow \quad A \cdot (x - x_0) = b - b = 0 \quad \Longleftrightarrow \quad x - x_0 \in \ker A \,. \qquad \square$$

Punkt (3) wird gern so umformuliert: Die *allgemeine Lösung* x des inhomogenen Gleichungssystems $A \cdot x + b$ ist die Summe aus einer *speziellen Lösung* x_0 des inhomogenen Gleichungssystems und der allgemeinen Lösung $v = x - x_0$ des zugehörigen homogenen Gleichungssystems $A \cdot v = 0$.

3.22. Proposition. *Es seien $A \in M_{m,n}(\Bbbk)$ und $b \in \Bbbk^m$. Die Lösungsmenge des linearen Gleichungssystems $A \cdot x = b$ verändert sich nicht, wenn man A und b von links mit der gleichen invertierbaren Matrix $B \in GL(m, \Bbbk)$ multipliziert.*

Beweis. Es sei $x \in \Bbbk^n$ mit $A \cdot x = b$, dann folgt

$$(B \cdot A) \cdot x = B \cdot (A \cdot x) = B \cdot b \,.$$

Gelte umgekehrt $(B \cdot A) \cdot x = B \cdot b$, und sei B^{-1} die Inverse von B, dann folgt

$$A \cdot x = B^{-1} \cdot (B \cdot A) \cdot x = B^{-1} \cdot B \cdot b = b \,.$$

Also haben das alte und das neue Gleichungssystem die gleichen Lösungen. $\square$

3.23. Bemerkung. Wir betrachten jetzt besonders einfache invertierbare Matrizen, die sogenannten *Elementarmatrizen.* Dazu seien $i, j \in \{1, \ldots, m\}$ mit $i \neq j$ und $k \in \Bbbk^\times = \Bbbk \setminus \{0\}$. Außerdem sei $A \in M_{m,n}(\Bbbk)$.

(1) Wir betrachten die Matrix

$$P_{ij} = \begin{array}{c} \\ \\ i \\ \\ \\ \\ j \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccccccc} & & & & i & & & & j \end{array} \\ \begin{pmatrix} 1 & 0 & & & \cdots & & & & 0 \\ 0 & \ddots & & & & & & & \\ & & 1 & & & & & & \\ & & & 0 & & & 1 & & \\ & & & & 1 & & & & \\ \vdots & & & & & \ddots & & & \vdots \\ & & & & & & 1 & & \\ & & & 1 & & & 0 & & \\ & & & & & & & 1 & \\ & & & & & & & \ddots & 0 \\ 0 & & & & \cdots & & & 0 & 1 \end{pmatrix} \end{array}.$$

Linksmultiplikation mit P_{ij} vertauscht die i-te und die j-te Zeile von A. Diese Matrix ist zu sich selbst invers, also $P_{ij}^{-1} = P_{ij}$.

(2) Als nächstes betrachten wir die Matrix

$$M_i(k) = \begin{array}{c} \\ \\ i \\ \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccccc} & & & & i & & \end{array} \\ \begin{pmatrix} 1 & 0 & & & \cdots & & 0 \\ 0 & \ddots & & & & & \\ & & 1 & & & & \\ \vdots & & & k & & & \vdots \\ & & & & 1 & & \\ & & & & & \ddots & 0 \\ 0 & & & \cdots & & 0 & 1 \end{pmatrix} \end{array}.$$

Linksmultiplikation mit $M_i(k)$ multipliziert die i-te Zeile von A mit k und lässt alle anderen Zeilen unverändert. Das Inverse dieser Matrix ist $M_i(k)^{-1} = M_i(k^{-1})$.

(3) Zu guter Letzt betrachten wir

$$E_{ij}(k) = \begin{array}{c} \\ i \\ \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccc} & & & j & \end{array} \\ \begin{pmatrix} 1 & 0 & & \cdots & 0 \\ 0 & \ddots & & k & \vdots \\ & & & & \\ \vdots & \ddots & & \ddots & 0 \\ 0 & \cdots & & 0 & 1 \end{pmatrix} \end{array}.$$

Linksmultiplikation mit $M_i(k)$ addiert das k-fache der j-ten Zeile von A zur i-ten Zeile. Das Inverse dieser Matrix ist $E_{ij}(-k)$.

Multiplikation mit einer der obigen Elementarmatrizen P_{ij}, $M_i(k)$ beziehungsweise $E_{ij}(k)$ heißt daher eine *elementare Zeilenumformung* vom Typ (1), (2) oder (3).

3.24. Definition. Eine Matrix $A \in M_{m,n}(\Bbbk)$ heißt *in Zeilenstufenform,* wenn es ganze Zahlen $0 \leq r \leq m$ und $1 \leq j_1 < \cdots < j_r \leq n$ gibt, so dass

(1) $a_{ij} = 0$ falls $i > r$ oder falls $i \leq r$ und $j < j_i$, und
(2) $a_{ij_i} = 1$ für alle $1 \leq i \leq r$.

Wir sagen, M sei *in strenger Zeilenstufenform,* wenn darüberhinaus

(3) $a_{ij_p} = 0$ für alle $1 \leq p \leq r$ und $i \neq p$.

Ein Gleichungssystem $A \cdot x = b$ heißt *in* (*strenger*) *Zeilenstufenform,* wenn die Matrix A in (strenger) Zeilenstufenform ist.

Eine Matrix $A = (a_{ij})_{i,j}$ in Zeilenstufenform hat also folgende Gestalt:

$$r \begin{pmatrix} 0 \dots 0 & \overset{j_1}{1} & a_{1,j_1+1} \dots & a_{1,j_2-1} & \overset{j_2}{*} & a_{1,j_2+1} \dots & a_{1,j_r-1} & \overset{j_r}{*} & a_{1,j_r-1} & \dots & a_{1,n} \\ 0 \dots & 0 & 1 & a_{2,j_2+1} \dots & a_{2,j_r-1} & * & a_{2,j_r+1} & \dots & a_{2,n} \\ \vdots & & & & & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & & & & & a_{r-1,j_r-1} & * & a_{r-1,j_r+1} & \dots & a_{r-1,n} \\ 0 & \dots & & & & & 0 & 1 & a_{r,j_r+1} & \dots & a_{r,n} \\ 0 & \dots & & & & & & & & & 0 \\ \vdots & & & & & & & & & & \vdots \\ 0 & \dots & & & & & & & & & 0 \end{pmatrix}.$$

Die „$*$“ sind beliebig, verschwinden aber, wenn A in *strenger* Zeilenstufenform ist. Die Zahlen r und $j_1, \dots, j_r$ sind durch A eindeutig bestimmt. Wir sehen in Proposition 3.26 unten, dass man bei einem Gleichungssystem in Zeilenstufenform die Lösunsmenge leicht ablesen kann.

3.25. Satz (Gauß-Verfahren)**.** *Jedes lineare Gleichungssystem lässt sich mit Hilfe elementarer Zeilenumformungen in (strenge) Zeilenstufenform bringen.*

Andere Namen sind *Gauß-Algorithmus* oder *Gauß-Elimination.*

Beweis. Das Gauß-Verfahren ist ein induktiver Algorithmus, bei man eine Reihe elementarer Zeilenumformungen auf die Matrix A und die rechte Seite b anwendet und so die Matrix A Spalte für Spalte in strenge Zeilenstufenform bringt.

Induktionsannahme. Es seien $r \geq 0$ und $1 \leq j_1 < \dots < j_r \leq n$ sowie q mit $j_r \leq q \leq n$ (beziehungsweise $q \geq 0$, falls $r = 0$) gegeben, so dass die Bedingungen (1) und (2) (beziehungsweise (1)–(3) für strenge Zeilenstufenform) in Definition 3.24 für alle $i \leq n$ und für alle $j \leq q$ gelten. Das heißt, die Matrix A ist bis einschließlich Spalte q bereits in strenger Zeilenstufenform.

Induktionsanfang. Wir beginnen mit $q = r = 0$. Dann sind die obigen Annahmen trivialerweise erfüllt.

Induktionsschritt. Falls $r = m$ oder $q = n$ gilt, sind wir fertig. Ansonsten setzen wir $j = q + 1 \leq n$ und unterscheiden zwei Fälle.

1. Fall: Falls es kein i mit $r < i \leq m$ und $a_{ij} \neq 0$ gibt, ist die Matrix bereits bis zur j-ten Spalte in strenger Zeilenstufenform. In diesem Fall erhöhen wir q um 1, so dass $q = j$, und führen den nächsten Induktionsschritt durch.

2. Fall: Ansonsten gibt es ein kleinstes $i > r$ mit $a_{ij} \neq 0$.

Schritt 1 („Tauschen“): Falls $i \neq r+1$, vertauschen wir die i-te und die $(r+1)$-te Zeile mit einer elementaren Zeilenumformung vom Typ (1). Anschließend erhöhen wir r um 1, so dass jetzt also $a_{rj} \neq 0$.

Schritt 2 („Normieren“): Falls $a_{rj} \neq 1$, multiplizieren wir die r-te Zeile mit a_{rj}^{-1}, so dass anschließend $a_{rj} = 1$, das ist eine elementare Zeilenumformung vom Typ (2). Jetzt setzen wir $j_r = j$, so dass jetzt $a_{rj_r} = 1$, das heißt, Punkt (2) in Definition 3.24 ist für $i = r$ erfüllt.

Schritt 3 („Ausräumen"): Schließlich subtrahieren wir von der i-ten Zeile das a_{ij_r}-fache der r-ten Zeile für alle $i > r$ (beziehungsweise für alle $i \neq r$ für die strenge Zeilenstufenform), das ist eine elementare Zeilenumformung vom Typ (3), so dass hinterher $a_{ij_r} = 0$ für alle $i > r$ (beziehunsweise für alle $i \neq r$). Wir erhöhen q um 1, so dass jetzt $q = j$, und haben nun auch Punkt (1) (und gegebenenfalls auch (3)) in Definition 3.24 für alle $j \leq q$ erfüllt. Anschließend wiederholen wir den Induktionsschritt.

Am Ende erhalten wir eine Matrix in Zeilenstufenform, beziehungsweise in strenger Zeilenstufenform, je nachdem, ob wir in Schritt 3 die gesamte Spalte oder nur unterhalb vom jeweiligen r ausgeräumt haben. □

Man beachte, dass wir in einem Schritt eine ganze Zeile durch a_{rj_r} dividieren mussten, um $a_{rj_r} = 1$ zu erreichen. Aus diesem Grund lässt sich das Gauß-Verfahren nicht auf Matrizen über Ringen anwenden, in denen nicht alle Elemente außer 0 invertierbar sind.

3.26. Proposition. *Sei $A \in M_{m,n}(\mathbb{k})$ eine Matrix in Zeilenstufenform, und sei $b \in \mathbb{k}^m$.*

(1) *Eine Basis des Bildes* $\operatorname{im} A = \mathbb{k}^r \times \{0\} \subset \mathbb{k}^m$ *von A besteht aus den Spalten $a_{j_i} = A(e_{j_i})$ für $i = 1, \ldots, r$, insbesondere ist* $\operatorname{rg} A = r$.

(2) *Das Gleichungssystem (*) ist genau dann lösbar, wenn $b_{r+1} = \cdots = b_m = 0$; in diesem Fall hat die Lösungsmenge die Gestalt*

$$\begin{aligned} &\left\{ x \in \mathbb{k}^n \;\middle|\; A \cdot x = b \right\} \\ &= \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{k}^n \;\middle|\; x_{j_i} = b_i - \sum_{j=j_i+1}^{n} a_{ij} x_j \text{ für alle } i = 1, \ldots, r \right\} , \end{aligned}$$

jede Lösung ist also eindeutig bestimmt durch die Angabe der Koordinaten x_j für alle $j \in \{1, \ldots, n\} \setminus \{j_1, \ldots, j_r\}$.

(3) *Es sei A in strenger Zeilenstufenform, und es sei $\{k_{r+1}, \ldots, k_n\} = \{1, \ldots, n\} \setminus \{j_1, \ldots, j_r\}$ eine Aufzählung der restlichen Spaltenindizes, dann erhalten wir eine Basis $(c_{r+1}, \ldots, c_n)$ von* $\ker A$ *aus Vektoren der Form*

$$c_\ell = e_{k_\ell} - \sum_{i=1}^{r} e_{j_i} \,.\, a_{ik_\ell} \in \ker A \subset \mathbb{k}^n \qquad \text{für } \ell = r+1, \ldots, n \,,$$

mit $c_{i\ell} \in \mathbb{k}$ für alle $i = 1, \ldots, r$.

Für die Basis von $\ker A$ in (2) benutzen wir die gleichen Buchstaben wir im Beweis des Rangsatzes 3.13.

Beweis. Zu Aussage (1) überlegen wir uns zunächst, dass $\operatorname{im} A \subset \mathbb{k}^r \times \{0\} \subset \mathbb{k}^n$, da alle Spalten von A in diesem Unterraum liegen.

Sei umgekehrt $b \in \mathbb{k}^r \times \{0\}$, dann hat die Lösungsmenge die in (2) angegebene Gestalt. Wenn wir x_j für $j \in \{1, \ldots, n\} \setminus \{j_1, \ldots, j_r\}$ beliebig vorgeben,

bestimmen die Zeilen $i = r, \ldots, 1$ in umgekehrter Reihenfolge die fehlenden Koordinaten $x_{j_r}, \ldots, x_{j_1}$ eindeutig. Daraus folgt (2) sowie $\operatorname{im} A = \mathbb{k}^r \times \{0\}$ und insbesondere $r = \operatorname{rg} A$, also gilt auch (1).

Zu (3) wählen wir $b = 0$ und bestimmen Elemente c_ℓ der Lösungsmenge $\ker A$, indem wir für $p = r+1, \ldots, n$ die Koordinaten $x_{k_p} = \delta_{\ell p}$ vorgeben. Wenn A in strenger Zeilenstufenform ist, ist die i-te Gleichung äquivalent zu

$$x_{j_i} = -\sum_{p=r+1}^{n} a_{ik_p} \,.\, x_{k_p} = -a_{ik_\ell} \,. \qquad \square$$

Wenn man das Gauß-Verfahren konkret anwendet, schreibt man gern die jeweilige linke Seite als Matrix ohne runde Klammern, macht rechts daneben einen senkrechten Strich, und schreibt die rechte Seite rechts neben diesen Strich. Dann führt man den obigen Algorithmus durch, wobei man sich nur an der linken Seite orientiert, aber alle Zeilenumformungen immer auf die linke und die rechte Seite simultan anwendet. Dabei reicht es, für jeden Induktionsschritt ein neues System aufzuschreiben. Unter Umständen kann es sinnvoll sein, auf der rechten Seite mehr als nur einen Vektor stehen zu haben, zum Beispiel, wenn man ein Gleichungssystem simultan für mehrere rechte Seiten zu lösen hat.

3.27. Bemerkung. Das Gauß-Verfahren kann benutzt werden, um viele verschiedene Probleme zu lösen. Einige davon haben wir in Bemerkung 3.20 bereits angeführt.

(1) Um das Gleichungssystem (*), also $A \cdot x = b$ zu lösen, bringen wir es zunächst mit dem Gauß-Verfahren in Zeilenstufenform. Nach Bemerkung 3.23 entsprechen elementare Zeilenumformungen gerade der Multiplikation mit invertierbaren Matrizen von links. Da wir alle Zeilenumformungen sowohl auf die linke als auch auf die rechte Seite des Gleichungssystems angewandt haben, ist das neue Gleichungssystem nach Proposition 3.22 zum alten äquivalent, und wir können die Lösungsmenge nach Proposition 3.26 (2) ablesen.

Zur Sicherheit sei daran erinnert, dass man ein Gleichungssystem löst, indem man die *gesamte* Lösungsmenge angibt (eventuell, indem man feststellt, dass diese leer ist), und nicht nur eine einzelnes Element der Lösungsmenge. Wenn die Lösungsmenge nicht leer ist, reicht es allerdings nach Proposition 3.21 (3), eine spezielle Lösung x_0 und den Unterraum $\ker A$ zu bestimmen, da die Lösungsmenge dann gerade $x_0 + \ker A$ ist.

(2) Es sei $A \in M_{m,n}(\mathbb{k})$, dann können wir Basen von $\ker A \subset \mathbb{k}^n$ und $\operatorname{im} A \subset \mathbb{k}^m$ bestimmen. Wir bringen dazu A mit dem Gauß-Verfahren in strenge Zeilenstufenform. Sei $B \in GL(m, \mathbb{k})$ das Produkt der elementaren Zeilenumformungen entsprechenden Elementarmatrizen, so dass $B \cdot A$ in strenger Zeilenstufenform ist. Mit Proposition 3.26 (3) bestimmen wir zunächst eine Basis von $\ker(B \cdot A) = \ker A$.

Seien r und $j_1, \ldots, j_r$ wie in Definition 3.24 zur Matrix $B \cdot A$, dann bilden die Vektoren $(B \cdot A)(e_{j_i})$ für $i = 1, \ldots, r$ eine Basis von $\operatorname{im}(B \cdot A)$

nach Proposition 3.26 (1). Da B einen Isomorphismus

$$B|_{\operatorname{im} A}\colon \operatorname{im} A \xrightarrow{\cong} \operatorname{im}(B \circ A)$$

induziert, erhalten wir als Basis von $\operatorname{im} A \subset \Bbbk^m$ gerade

$$\big(A(e_{j_1}), \dots, A(e_{j_r})\big) ,$$

insbesondere gilt $\operatorname{rg} A = \operatorname{rg}(B \cdot A) = r$, siehe auch Proposition 3.15 (1).

Übrigens können wir die Basis $(c_{r+1}, \dots, c_n)$ von $\ker A$ wie im Beweis des Rangsatzes 3.13 zu einer Basis $(c_1, \dots, c_n)$ von $\Bbbk^n$ mit $c_i = e_{j_i}$ für $i = 1, \dots, r$ ergänzen. Wenn wir wie dort fortfahren, erhalten wir ebenfalls die obige Basis $(A(e_{j_1}), \dots, A(e_{j_r}))$ von $\operatorname{im} A$.

(3) Es seien Vektoren $v_1, \dots, v_n \in \Bbbk^m$ gegeben. Wir möchten wissen, ob diese Vektoren linear unabhängig sind, und ob sie $\Bbbk^m$ erzeugen. Dazu schreiben wir die Vektoren als Spalten in eine Matrix A und bringen A in Zeilenstufenform. Dann bilden $(v_1, \dots, v_n)$ genau dann ein Erzeugendensystem, wenn $r = \operatorname{rg} A = m$ gilt.

Und sie sind linear unabhängig, wenn $A \cdot x = 0$ nur eine Lösung besitzt. Nach Proposition 3.26 (2) ist das genau dann der Fall, wenn $\{j_1, \dots, j_r\} = \{1, \dots, n\}$, das heißt, wenn $r = \operatorname{rg} A = n$ gilt.

(4) Um eine Matrix $A \in M_n(\Bbbk)$ zu invertieren, wenden wir das Gauß-Verfahren diesmal mit der rechten Seite E_n an, das heißt, wir lösen n lineare Gleichungssysteme mit der gleichen linken Seite simultan. Wenn wir während des Verfahrens nie eine Spalte überspringen (Fall 1 im Beweis tritt nicht ein) und A in strenge Zeilenstufenform bringen, dann gilt $j_i = i$ für alle $i = 1, \dots, n$. Also bleibt auf der linken Seite die Einheitsmatrix E_n stehen.

Rechts steht das Produkt B aller Elementarmatrizen, die wir im Laufe des Verfahrens angewendet haben, also

$$A \mid E_n \quad \rightsquigarrow \quad E_n \mid B .$$

Es gilt also $B \cdot A = E_n$. Da beide Matrizen quadratisch waren, ist A invertierbar, und B ist die inverse Matrix; dazu interpretiere A und B als lineare Abbildungen und wende eine Übungsaufgabe an.

Falls wir im Laufe des Gauß-Verfahrens eine Spalte überspringen, so dass $j_{i_0+1} > j_{i_0} + 1$ für ein i_0 (oder $j_1 > 1$ für $i_0 = 0$), folgt $i < j_i$ für alle $i > i_0$, insbesondere $r < j_r \leq n$, so dass $\operatorname{rg} A < n$ gilt und A daher nicht invertierbar sein kann. Das bedeutet, dass wir das Verfahren abbrechen können, sobald Fall 1 eintritt, und feststellen können, dass A nicht invertierbar ist.

(5) Für sehr große Matrizen ist das Gauß-Verfahren zu rechenaufwendig. Es gibt aber noch ein anderes Problem, sobald man nicht mit exakten Zahlen rechnet, sondern in jedem Zwischenschritt nach einer bestimmten Anzahl von Dual- oder Dezimalstellen rundet oder abschneidet: Sobald man zwei annähernd gleich große Zahlen mit kleinen prozentualen Fehlern voneinander abzieht, erhält man einen wesentlich größeren prozentualen Fehler im Ergebnis. Um dieses Problem so gut wie

möglich zu umgehen, kann man ein Verfahren anwenden, dass man Pivotisierung nennt. Dabei tauscht man in jedem Schritt 1 die Zeile $r+1$ mit derjenigen Zeile i, für die das Element a_{ij} in der gerade aktuellen Spalte betragsmäßig am größten ist.

3.28. Bemerkung. Die strenge Zeilenstufenform ist wieder eine Normalform. Diesmal betrachten wir als Objekte Matrizen $A \in M_{m,n}(\mathbb{k})$ und nennen zwei Objekte A, $A' \in M_{m,n}(\mathbb{k})$ „linksäquivalent“, wenn es eine invertierbare Matrix $B \in GL(m, \mathbb{k})$ gibt, so dass $A' = B \cdot A$. Mit dem Gauß-Verfahren 3.25 sehen wir, dass jede Matrix zu einer Matrix in strenger Zeilenstufenform linksäquivalent ist.

Mit ein bisschen zusätzlichem Aufwand kann man zeigen, dass zwei Matrizen in strenger Zeilenstufenform genau dann linksäquivalent sind, wenn sie gleich sind. Also gibt es in jeder Linksäquivalenzklasse genau eine Matrix in strenger Zeilenstufenform. Da es von diesen Matrizen offensichtlich sehr viele gibt, erhalten wir keine schöne vollständige Invariante für dieses Problem, außer der besagten Matrix in strenger Zeilenstufenform selbst.

KAPITEL 4

Determinanten

Wir wollen Endomorphismen von Vektorräumen beziehungsweise freien R-Moduln V verstehen, also lineare Abbildungen $F\colon V \to V$. Endomorphismen endlich erzeugter freier Moduln werden durch quadratische Matrizen $A \in M_n(R)$ dargestellt. In diesem Kapitel lernen wir eine wichtige Invariante quadratischer Matrizen kennen, die Determinante.

Über den reellen Zahlen hat die Determinante etwas mit Volumina von Parallelotopen zu tun, und etwas mit Orientierung. Über den meisten anderen Körpern und Ringen lassen sich diese Aspekte nicht voneinander trennen. Wir beginnen in Abschnitt 4.1 mit der Beschreibung von Volumina, benutzen die dort gewonnenen Erkenntnisse in Abschnitt 4.2 zur Definition der Determinante, und führen in Abschnitt 4.3 den Begriff der Orientierung ein.

Im ganzen Kapitel benötigen wir das Kommutativgesetz für die Multiplikation. Insbesondere wird R in diesem Kapitel immer einen kommutativen Ring mit Eins und $\Bbbk$ immer einen Körper bezeichnen. Warum wir das Kommutativgesetz brauchen, erklären wir in Bemerkung 4.5, und was ansonsten schiefgehen kann, sehen Sie in Beispiel 4.22.

4.1. Volumina und Determinantenfunktionen

In Bemerkung 1.69 (2) haben wir die Volumina von Parallelotopen im $\mathbb{R}^3$ ausgerechnet. Im $\mathbb{R}^n$ wollen wir entsprechend das n-dimensionale Volumen

$$\mathrm{vol}(v_1, \ldots, v_n)$$

eins von Vektoren $v_1, \ldots, v_n \in \mathbb{R}^n$ aufgespannten Parallelotops bestimmen. Wir möchten, dass dieser Volumenbegriff zwei Eigenschaften hat, nämlich *positive Homogenität* und *Scherungsinvarianz:* Für alle n-Tupel $(v_1, \ldots, v_n)$, alle i, $j \in \{1, \ldots, n\}$ mit $i \neq j$ und alle $k \in \mathbb{R}$ soll gelten

$$\mathrm{vol}(v_1, \ldots, v_{i-1}, v_i \,.\, k, v_{i+1}, \ldots, v_n) = \mathrm{vol}(v_1, \ldots, v_n) \cdot |k| \ ; \tag{1}$$

$$\mathrm{vol}(v_1, \ldots, v_{i-1}, v_i + v_j \,.\, k, v_{i+1}, \ldots, v_n) = \mathrm{vol}(v_1, \ldots, v_n) \ . \tag{2}$$

Bedingung (2) lässt sich mit dem Cavalierischen Prinzip begründen: die Querschnitte von beiden Parallelotopen mit affinen Unterräumen parallel zu $\langle v_1, \ldots, \widehat{v_i}, \ldots, v_n \rangle$ haben jeweils dasselbe Volumen, wenn man v_i um ein Vielfaches von v_j abändert. Da allgemeine Körper nicht angeordnet sind, ist

Bedingung (1) im allgemeinen nicht sinnvoll. Wir ersetzen sie daher durch eine Art Homogenität und erhalten ein „Volumen mit Vorzeichen“ mit

(1') $$\omega(v_1, \dots, v_{i-1}, v_i \,.\, k, v_{i+1}, \dots, v_n) = \omega(v_1, \dots, v_n) \cdot k \;.$$

Falls $\Bbbk = \mathbb{R}$ oder $\mathbb{Q}$ und ω die Bedingungen (1') und (2) erfüllt, erfüllt $\mathrm{vol} = |\omega|$ die Bedingungen (1) und (2) und liefert daher einen Volumen.

Soviel zur Motivation. Wir wollen jetzt Volumina mit Vorzeichen betrachten, und zwar zunächst über kommutativen Ringen R. Wir beginnen mit beliebigen R-Moduln M und Zahlen $k \in \mathbb{N}$.

4.1. Definition. Es sei M ein R-Modul, $k \in \mathbb{N}$, und $\alpha\colon M^k \to R$ eine Abbildung. Dann heißt α *multilinear,* wenn für alle $i \in \{1, \dots, k\}$ und alle $v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_k \in M$ die Abbildung

(1) $$M \to R \qquad \text{mit} \qquad w \longmapsto \alpha(v_1, \dots, v_{i-1}, w, v_{i+1}, \dots, v_k)$$

linear ist. Sie heißt *alternierend* oder auch *alternierende Form,* wenn für alle $i = 1, \dots, k-1$ gilt, dass

(2) $$\alpha(v_1, \dots, v_k) = 0 \qquad \text{falls } v_{i+1} = v_i \;.$$

Die Menge aller alternierenden multilinearen Abbildungen $\alpha\colon M^k \to R$ wird mit $\Lambda^k M^*$ bezeichnet. Falls V ein n-dimensionaler $\Bbbk$-Vektorraum ist, heißt eine alternierende multilineare Abbildung $\omega\colon V^n \to \Bbbk$ eine *Determinantenfunktion.*

Man beachte, dass wir für $k = 1$ gerade den dualen Modul $\Lambda^1 M^* = M^*$ erhalten. Für $k = 0$ setzt man sinnvollerweise $\Lambda^0 M^* = R$.

4.2. Beispiel. Wir betrachten das Spatprodukt $\mathbb{R}^3 \to \mathbb{R}$ mit $(x, y, z) \mapsto \langle x \times y, z\rangle$ aus Satz 1.68. Wegen Bemerkungen 1.52 (1) und 1.67 (1), (1') ist das Spatprodukt multilinear, und wegen Bemerkung 1.67 (2) und Satz 1.68 (1) ist es alternierend. Also ist das Spatprodukt eine Determinantenfunktion.

4.3. Proposition. *Es sei M ein R-Modul und $\alpha\colon M^k \to R$ multilinear. Dann sind die folgenden Aussagen äquivalent.*

(1) *Die Abbildung α ist alternierend,*
(2) *Es gilt $\alpha(v_1, \dots, v_k) = 0$, wenn $(v_1, \dots, v_k)$ linear abhängig sind.*

Die Aussagen (1) *und* (2) *implizieren die folgende Eigenschaft, die zu* (1) *und* (2) *über Körpern $R = \Bbbk$ der Charakteristik $\chi(\Bbbk) \neq 2$ äquivalent ist.*

(3) *Die Abbildung α ist* antisymmetrisch, *das heißt, für alle $(v_1, \dots, v_k) \in M^k$ und alle $i, j \in \{1, \dots, k\}$ mit $i < j$ gilt*

$$\alpha(v_1, \dots, v_{i-1}, v_j, v_{i+1}, \dots, v_{j-1}, v_i, v_{j+1}, \dots, v_k) = -\alpha(v_1, \dots, v_k) \;.$$

Beweis. Die Richtung „(2) $\Longrightarrow$ (1) ist klar, denn falls $v_{i+1} = v_i$, sind $(v_1, \dots, v_k)$ linear abhängig.

Zu „(1) $\Longrightarrow$ (3) betrachten wir zunächst den Fall $j = i + 1$. Dann folgt

$$\alpha(v_1, \dots, v_k) = \alpha(v_1, \dots, v_k) + \underbrace{\alpha(v_1, \dots, v_i, v_i, v_{i+2}, \dots, v_k)}_{=0}$$

$$\begin{aligned}
&= \alpha(v_1, \dots, v_i, v_i + v_{i+1}, v_{i+2}, \dots, v_k) \\
&\qquad - \underbrace{\alpha(v_1, \dots, v_{i-1}, v_i + v_{i+1}, v_i + v_{i+1}, v_{i+2}, \dots, v_k)}_{=0} \\
&= \alpha(v_1, \dots, v_{i-1}, -v_{i+1}, v_i + v_{i+1}, v_{i+2}, \dots, v_k) \\
&\qquad + \underbrace{\alpha(v_1, \dots, v_{i-1}, -v_{i+1}, -v_{i+1}, v_{i+2}, \dots, v_k)}_{=0} \\
&= -\alpha(v_1, \dots, v_{i-1}, v_{i+1}, v_i, v_{i+2}, \dots, v_k) \; .
\end{aligned}$$

Also ändert sich das Vorzeichen, wenn man zwei benachbarte Vektoren vertauscht. Der allgemeine Fall folgt durch Induktion über $p = j - i$, denn

$$\begin{aligned}
\alpha(v_1, \dots, v_k) &= -\alpha(v_1, \dots, v_{i-1}, v_{j-1}, v_{i+1}, \dots, v_{j-2}, v_i, v_j, v_{j+1}, \dots, v_k) \\
&= \quad \alpha(v_1, \dots, v_{i-1}, v_{j-1}, v_{i+1}, \dots, v_{j-2}, v_j, v_i, v_{j+1}, \dots, v_k) \\
&= -\alpha(v_1, \dots, v_{i-1}, v_j, v_{i+1}, \dots, v_{j-2}, v_{j-1}, v_i, v_{j+1}, \dots, v_k) \; .
\end{aligned}$$

Dabei haben wir nur Argumente im Abstand von weniger als p vertauscht.

Zu „(1) $\Longrightarrow$ (2)“ benutzen wir (3) und zeigen, dass aus (1) Scherungsinvarianz folgt. Für alle i, $j \in \{1, \dots, k\}$ mit $i \neq j$ und alle $r \in R$ gilt, dass

$$\begin{aligned}
\alpha(v_1, \dots, v_k) &= -\alpha(v_1, \dots, v_{i-1}, v_{j-1}, v_{i+1}, \dots, v_{j-2}, v_i, v_j, v_{j+1}, \dots, v_k) \\
&\qquad - \underbrace{\alpha(v_1, \dots, v_{i-1}, v_{j-1}, v_{i+1}, \dots, v_{j-2}, v_j, v_j, v_{j+1}, \dots, v_k)}_{=0} \cdot r \\
&= -\alpha(v_1, \dots, v_{i-1}, v_{j-1}, v_{i+1}, \dots, v_{j-2}, v_i + v_j \,.\, r, v_j, v_{j+1}, \dots, v_k) \\
&= \alpha(v_1, \dots, v_{i-1}, v_i + v_j \,.\, r, v_{i+1}, \dots, v_k) \; ,
\end{aligned}$$

insbesondere ist α scherungsinvariant. Seien jetzt die Vektoren $(v_1, \dots, v_k)$ linear abhängig. Nach Lemma 3.1 existiert ein $i \in \{1, \dots, k\}$, so dass v_i als Linearkombination der restlichen Vektoren dargestellt werden kann, also

$$v_i = \sum_{j \neq i} v_j \,.\, r_j$$

mit $r_j \in R$. Nur mit Hilfe der obigen Scherungsinvarianz folgt daraus

$$\begin{aligned}
\alpha(v_1, \dots, v_k) &= \alpha\left(v_1, \dots, v_{i-1}, \sum_{j \neq i} v_j \,.\, r_j, v_{i+1}, \dots, v_k\right) \\
&= \alpha(v_1, \dots, v_{i-1}, 0, v_{i+1}, \dots, v_k) = 0 \; .
\end{aligned}$$

Schließlich sei $R = \Bbbk$ ein Körper der Charakteristik $\chi(\Bbbk) \neq 2$, und es gelte $v_i = v_j$ für i, $j \in \{1, \dots, k\}$ mit $i < j$. Aus (3) folgt

$$\begin{aligned}
\alpha(v_1, \dots, v_k) &= \frac{1}{2}\, \alpha(v_1, \dots, v_k) \\
&\qquad - \frac{1}{2}\, \alpha(v_1, \dots, v_{i-1}, v_j, v_{i+1}, \dots, v_{j-1}, v_i, v_{j+1}, \dots, v_k) = 0 \; . \quad \square
\end{aligned}$$

4.4. Bemerkung. Wir haben in der Motivation von einem „Volumen mit Vorzeichen“ Homogenität (1') und Scherungsinvarianz gefordert. Multilineare Abbildungen sind insbesondere homogen, und im obigen Beweis zu „(1) $\Longrightarrow$ (2)“

haben wir gesehen, dass alternierende multilineare Abbildungen auch scherungsinvariant sind.

Umgekehrt sei V jetzt ein n-dimensionaler $\Bbbk$-Vektorraum und $\omega\colon V^n \to \Bbbk$ sei homogen und scherungsinvariant. Wir haben im Schritt „(1) $\Longrightarrow$ (2)“ gesehen, dass aus Scherungsinvarianz folgt, dass $\omega(v_1, \dots, v_n) = 0$, wenn $(v_1, \dots, v_n)$ linear abhängig sind.

Wir wollen jetzt zeigen, dass

$$\omega(u + w, v_2, \dots, v_n) = \omega(u, v_2, \dots, v_n) + \omega(w, v_2, \dots, v_n) \ ,$$

dann ist $\omega(v_1, \dots, v_n)$ linear in v_1. Die Linearität in den anderen Argumenten folgt genauso. Wir unterscheiden zwei Fälle: wenn $(v_2, \dots, v_n)$ linear abhängig sind, reduziert sich die obige Gleichung zu $0 = 0 + 0$.

Wir dürfen also annehmen, dass $(v_2, \dots, v_n)$ linear unabhängig sind, und ergänzen zu einer Basis $(v_1, \dots, v_n)$. Dann existieren k_j, $\ell_j \in \Bbbk$, so dass

$$u = \sum_j v_j \,.\, k_j \qquad \text{und} \qquad w = \sum_j v_j \,.\, \ell_j \ .$$

Aus Scherungsinvarianz und Homogenität folgt

$$\begin{aligned}
\omega(u + w, v_2, \dots, v_n) &= \omega\left(\sum_j v_j \,.\, (k_j + \ell_j), v_2, \dots, v_n\right) \\
&= \omega(v_1 \,.\, (k_1 + \ell_1), v_2, \dots, v_n) \\
&= \omega(v_1, v_2, \dots, v_n) \cdot k_1 + \omega(v_1, v_2, \dots, v_n) \cdot \ell_1 \\
&= \omega\left(\sum_j v_j \,.\, k_j, v_2, \dots, v_n\right) + \omega\left(\sum_j v_j \,.\, \ell_j, v_2, \dots, v_n\right) \\
&= \omega(u, v_2, \dots, v_n) + \omega(w, v_2, \dots, v_n) \ .
\end{aligned}$$

Also entsprechen Determinantenfunktionen genau unseren „Volumina mit Vorzeichen.“

4.5. Bemerkung. Wir überlegen uns leicht, dass die Summe zweier Determinantenfunktionen und auch ein skalares Vielfaches einer Determinantenfunktion wieder eine solche ist. Also ist $\Lambda^n M^*$ ein R-Modul. An dieser Stelle braucht man Kommutativität von R, siehe dazu die Bemerkung vor Definition 2.41. Aber man braucht Kommutativität von R bereits, um überhaupt multilineare Abbildungen mit zwei oder mehr Argumenten zu bekommen, wie die folgende Rechnung zeigt:

$$\begin{aligned}
\alpha(v_1, \dots, v_k) \cdot r \cdot s = \alpha(v_1 \,.\, r, v_2, \dots, v_k) \cdot s &= \alpha(v_1 \,.\, r, v_2 \,.\, s, v_3, \dots, v_k) \\
&= \alpha(v_1, v_2 \,.\, s, v_3, \dots, v_k) \cdot r = \alpha(v_1, \dots, v_k) \cdot s \cdot r \ .
\end{aligned}$$

Dass es überhaupt verschiedene Determinantenfunktionen auf demselben Modul oder Vektorraum gibt, sollte uns nicht erstaunen; schließlich kann man auch das Volumen im „uns umgebenden $\mathbb{R}^3$“ verschieden messen — etwa in Litern, Kubikmetern, flüssigen Unzen, Fässern, etc.

Wir wollen jetzt für alle Ringe R (kommutativ, mit Eins) ein spezielles Element $\omega_n \in \Lambda^n(R^n)^*$, die *Standard-Determinantenfunktion,* durch Induktion über $n \in \mathbb{N}$ konstruieren. Für $n = 0$ setzen wir $\omega_0() = 1 \in R$ und sind fertig.

Sei ω_{n-1} bereits konstruiert. Wir fassen Vektoren $x \in R^n$ durch Weglassen der letzten Koordinate als Vektoren $x' \in R^{n-1}$ auf, und nennen die letzte Koordinate $\varepsilon_n(x)$. Wir definieren ω_n rekursiv durch

$$(*) \qquad \omega_n(x_1, \ldots, x_n) = \sum_{i=1}^{n} (-1)^{i+n}\, \varepsilon_n(x_i)\, \omega_{n-1}(x'_1, \ldots, \widehat{x'_i}, \ldots, x'_n) \in R\ ,$$

wobei ein Dach über einem Eintrag wie zu Beginn von Abschnitt 3.1 gerade „Weglassen“ bedeutet. Diese Konstruktion liefert zugleich ein erstes Verfahren zur Berechnung von ω_n, die Laplace-Entwicklung, siehe Satz 4.12 unten.

4.6. Proposition. *Es sei R ein kommutativer Ring mit Eins, dann ist die oben konstruierte Abbildung $\omega_n \colon R^n \to R$ alternierend, multilinear, und erfüllt*

$$\omega_n(e_1, \ldots, e_n) = 1\ .$$

Beweis. Wir beweisen die Aussage wieder durch Induktion über n. Für $n = 1$ ist die Behauptung klar.

Sei die Proposition für ω_{n-1} bereits bewiesen. Linearität von ω_n an der i-ten Stelle folgt für den i-ten Summand in (*) aus der Linearität von ε_n, für die restlichen Summanden aus der Multilinearität von ω_{n-1}.

Sei jetzt $x_{i+1} = x_i$ für ein $i \in \{1, \ldots, n-1\}$. Dann sind der i-te und der $(i+1)$-te Summand in (*) bis auf das Vorzeichen gleich und heben sich weg, bei allen anderen Summanden werden zwei gleiche Vektoren nebeneinander in ω_{n-1} eingesetzt, was nach Induktionsvoraussetzung 0 ergibt.

Außerdem ist $\varepsilon_n(e_i) = 0$ für $i < n$, und die Vektoren e'_i für $i < n$ sind gerade die Standardbasisvektoren des R^n. Also gilt

$$\omega_n(e_1, \ldots, e_n) = (-1)^{n+n}\, \varepsilon_n(e_n)\, \omega_{n-1}(e'_1, \ldots, e'_{n-1}) = 1\ . \qquad \square$$

Als nächstes überlegen wir uns, dass der Raum $\Lambda^n V^*$ genau eindimensional ist.

4.7. Proposition. *Es sei R ein kommutativer Ring mit Eins, $r \in R$ und M ein freier R-Modul mit Basis $B = (b_1, \ldots, b_n)$. Dann existiert genau eine Determinantenfunktion $\omega \in \Lambda^n M^*$ mit*

$$\omega(e_1, \ldots, e_n) = r\ .$$

Sei ω_B die obige Determinantenfunktion zu $r = 1$, dann ist $\Lambda^b M^*$ ein freier R-Modul mit Basis (ω_B).

Beweis. Zur Eindeutigkeit bestimmen wir den Wert von $\omega(v_1, \ldots, v_n)$ für Modulelemente

$$v_j = \sum_{i=1}^{n} b_i\, .\, a_{ij} \in R^n\ .$$

Als erstes schließen wir aus Multilinearität, dass

$$\begin{aligned}\omega(v_1,\dots,v_n) &= \omega\Big(\sum_{i=1}^n b_i \,.\, a_{i1},\dots,\sum_{i=1}^n b_i \,.\, a_{in}\Big)\\ &= \sum_{i_1=1}^n \cdots \sum_{i_n=1}^n \omega(b_{i_1},\dots,b_{i_n})\cdot a_{i_1 1}\cdots a_{i_n n}\ .\end{aligned}$$

Als nächstes dürfen wir wegen 4.3 (2) wir alle Summanden weglassen, bei denen $i_j = i_k$ für $j \neq k$, und erhalten

$$\omega(v_1,\dots,v_n) = \sum_{\substack{i_1,\dots,i_n\in\{1,\dots,n\}\\ \{i_1,\dots,i_n\}=\{1,\dots,n\}}} \omega\big(b_{i_1},\dots,b_{i_n}\big)\cdot a_{i_1,1}\cdots a_{i_n,n}\ .$$

Schließlich geht $\omega\big(b_{i_1},\dots,b_{i_n}\big)$ nach Proposition 4.11 unten aus $\omega(b_1,\dots,b_n)$ hervor, indem man p-mal einzelne Argumente vertauscht, wobei die Zahl $p = p(i_1,\dots,i_n)$ vom Tupel $(i_1,\dots,i_n)$ abhängt. Wegen Proposition 4.3 (3) gilt

$$\omega\big(b_{i_1},\dots,b_{1_n}\big) = (-1)^p\cdot\omega(b_1,\dots,b_n) = (-1)^p\, r\ .$$

Also ist ω eindeutig bestimmt durch

$$\omega(v_1,\dots,v_n) = \sum_{\substack{i_1,\dots,i_n\in\{1,\dots,n\}\\ \{i_1,\dots,i_n\}=\{1,\dots,n\}}} (-1)^{p(i_1,\dots,i_n)}\, r\cdot a_{i_1,1}\cdots a_{i_n,n}\ .$$

Es sei $B\colon R^n \to M$ die Basisabbildung, siehe Bemerkung 2.74, und es sei $v_j = B(a_j)$ mit $a_j = (a_{ij})_i \in R^n$. Wir definieren zunächst eine alternierende multilineare Abbildung ω_B mit

$$\omega_B(v_1,\dots,v_n) = \omega_n(a_1,\dots,a_n)\ , \qquad \text{so dass} \qquad \omega_B(b_1,\dots,b_n) = 1\ .$$

Nach Proposition 4.6 ist ω_n multilinear und alternierend, also auch ω_B. Wir erhalten die gesuchte Form ω als

$$\omega = \omega_B\cdot r = \omega_B\,.\,\omega(b_1,\dots,b_n)\ .$$

Aufgrund der obigen Eindeutigkeitsaussage sind alle $\omega \in \Lambda^n M^*$ von dieser Gestalt, also bildet (ω_B) eine Basis. □

Der obige Beweis liefert uns eine zweite Berechnungsmethode der Standard-Determinantenfunktion ω_n, die sogenannte Leibniz-Formel, siehe Satz 4.13 unten.

4.2. Die Determinante

Ausgehend von den Überlegungen im letzten Kapitel führen wir jetzt Determinanten von Endomorphismen und quadratischen Matrizen ein. Während Determinantenfunktionen dazu dienen, Volumina von Parallelotopen in einem Vektorraum zu beschreiben, misst die Determinante, um welchen Faktor ein Endomorphismus das Volumen einzelner Parallelotope vergrößert oder verkleinert.

4.8. Bemerkung. Es seien M, N Moduln über R und $F\colon M \to N$ linear, dann definieren wir für alle k eine Abbildung $F^*\colon \Lambda^k N^* \to \Lambda^k M^*$ durch

$$(F^*(\alpha))(v_1, \dots, v_k) = \alpha\big(F(v_1), \dots, F(v_k)\big) \tag{1}$$

für alle $\alpha \in \Lambda^k N^*$ und alle $v_1, \dots, v_k$. Die rechte Seite ist sinnvoll, da wir α auf k Elemente $F(v_1), \dots, F(v_k)$ von N anwenden, und entsprechend erhalten wir eine Abbildung $F^*(\alpha)\colon M^k \to R$. Man nennt $F^*(\alpha)$ auch die mit F *zurückgeholte Form.*

Wir zeigen, dass $F^*(\alpha)$ im ersten Argument linear ist; für die anderen Argumente zeigt man Linearität genauso. Es seien x, y und $v_2, \dots, v_k \in M$ und r, $s \in R$, dann folgt

$$\begin{aligned}
&(F^*(\alpha))(x \,.\, r + y \,.\, s, v_2, \dots, v_k) \\
&\qquad = \alpha\big(F(x \,.\, r + y \,.\, s), F(v_2), \dots, F(v_k)\big) \\
&\qquad = \alpha\big(F(x) \,.\, r + F(y) \,.\, s, F(v_2), \dots, F(v_k)\big) \\
&\qquad = \alpha\big(F(x), F(v_2), \dots, F(v_k)\big) \cdot r + \alpha\big(F(y), F(v_2), \dots, F(v_k)\big) \cdot s \\
&\qquad = (F^*(\alpha))(x, v_2, \dots, v_k) \cdot r + (F^*(\alpha))(y, v_2, \dots, v_k) \cdot s \,.
\end{aligned}$$

Also ist $F^*(\alpha)$ multlinear.

Und $F^*(\alpha)$ ist auch alternierend, denn

$$(F^*(\alpha))(v_1, \dots, v_i, v_i, \dots, v_k) = \alpha\big(F(v_1), \dots, F(v_i), F(v_i), \dots, F(v_k)\big) = 0 \,.$$

Es folgt $F^*(\alpha) \in \Lambda^k M^*$ wie behauptet.

In Bemerkung 4.5 haben wir uns überlegt, dass $\Lambda^k M^*$ und $\Lambda^k N^*$ Moduln über R sind. Die Abbildung $F^*\colon \Lambda^k N^* \to \Lambda^k M^*$ ist linear, denn für alle α, $\beta \in \Lambda^k N^*$, alle r, $s \in R$ und alle $v_1, \dots, v_k \in M$ gilt

$$\begin{aligned}
&\big(F^*(\alpha \,.\, r + \beta \,.\, s)\big)(v_1, \dots, v_k) \\
&\qquad = (\alpha \,.\, r + \beta \,.\, s)\big(F(v_1), \dots, F(v_k)\big) \\
&\qquad = \alpha\big(F(v_1), \dots, F(v_k)\big) \cdot r + \beta\big(F(v_1), \dots, F(v_k)\big) \cdot s \\
&\qquad = \big(F^*(\alpha) \,.\, r + F^*(\beta) \,.\, s\big)(v_1, \dots, v_k) \,.
\end{aligned} \tag{2}$$

Schließlich seien $F\colon M \to N$ und $G\colon L \to M$ lineare Abbildungen, dann gilt $(F \circ G)^* = G^* \circ F^*\colon \Lambda^k N^* \to \Lambda^k L^*$, denn

$$\begin{aligned}
\big((F \circ G)^*(\alpha)\big)(\ell_1, \dots, \ell_k) &= \alpha\big(F(G(\ell_1)), \dots, F(G(\ell_k))\big) \\
&= (F^*(\alpha))\big(G(\ell_1), \dots, G(\ell_k)\big) = \big(G^*(F^*(\alpha))\big)(\ell_1, \dots, \ell_k) \,.
\end{aligned} \tag{3}$$

Es sei M ein freier R-Modul mit Basis $(b_1, \dots, b_n)$. In Proposition 4.7 haben wir gesehen, dass $\Lambda^n V^n$ ein eindimensionaler Vektorraum ist, erzeugt von dem Element ω_B mit $\omega_B(b_1, \dots, b_n) = 1$. Sei jetzt $F \in \mathrm{End}_R(M)$, dann ist $F^* \in \mathrm{End}_R(\Lambda^n M^*)$ nach der obigen Bemerkung, aber $\mathrm{End}_R(\Lambda^n M^*) \cong \mathrm{End}_R(R) = R$,

da $\Lambda^n V^* \cong R$. Also existiert zu jedem $F \in \operatorname{End} M$ ein Skalar $a = \det F \in R$, so dass

$$F^*\omega = \omega \,.\, a \qquad \text{für alle } \omega \in \Lambda^n M^* \,.$$

Um a zu bestimmen, wählen wir eine Basis $(b_1, \ldots, b_n)$, definieren ω_B wie in Proposition 4.7, und überlegen uns, dass

$$\begin{aligned}\omega_B\big(F(b_1), \ldots, F(b_n)\big) &= (F^*(\omega_B))(b, \ldots, b_n) \\ &= (\omega_B \,.\, a)(b, \ldots, b_n) = (\omega_B)(b, \ldots, b_n) \cdot a = a \,.\end{aligned}$$

Im Spezialfall $M = R^n$ mit der Standardbasis sind die Vektoren $F(e_1)$, …, $F(e_n)$ nach Folgerung 2.75 genau die Spalten der Abbildungsmatrix $A \in M_n(R)$ von F, und ω_B ist gerade die Standarddeterminantenfunktion ω_n aus Proposition 4.6. Das motiviert die folgende Definition.

4.9. Definition. Es sei R ein kommutativer Ring mit Eins, M ein freier R-Modul mit einer n-elementigen Basis, wobei $n \geq 1$, und $F \in \operatorname{End}_R(M)$ ein Endomorphismus. Dann ist die *Determinante* von F der eindeutige Skalar $\det F \in R$, so dass

$$F^*\omega = \omega \,.\, \det F \qquad \text{für alle } \omega \in \Lambda^n M^* \,. \tag{1}$$

Wir definieren die *Determinante* einer Matrix $A \in M_n(R)$ mit den Spalten $a_1, \ldots, a_n \in R^n$ durch

$$\det A = \omega_n(a_1, \ldots, a_n) \,. \tag{2}$$

Im Falle $n = 0$ folgt $\det() = 1$, da $\omega_0() = 1$. In Gleichung (1) haben wir für jeden Endomorphismus $F \in \operatorname{End}_R M$ die Determinante definiert, ohne eine Basis fixiert und F als Matrix geschrieben zu haben; diese Definition ist also *basisunabhängig.* Wenn wir eine Basis B wählen und A die Abbildungsmatrix von F bezüglich der Basis B (sowohl vom Definitions- als auch vom Wertebereich) darstellen, ist die Determinante von A durch (2) definiert. Unsere obige Vorüberlegung besagt, dass

$$\det A = \det F \,.$$

Auf diese Weise hängen (1) und (2) zusammen.

Wir wollen jetzt verschiedene Berechnungsverfahren für Determinanten angeben. Zunächst erinnern wir uns an die Automorphismengruppe $\operatorname{Aut}(M)$ einer Menge aus Beispiel 2.5.

4.10. Definition. Es sei $n \in \mathbb{N}$. Die *symmetrische Gruppe S_n in n Elementen* ist definiert als $S_n = \operatorname{Aut}(\{1, \ldots, n\})$, ihre Elemente $S_n \ni \sigma\colon \{1, \ldots, n\} \to \{1, \ldots, n\}$ heißen *Permutationen.*

Es sei R ein kommutativer Ring mit Eins. Einer Permutation $\sigma \in S_n$ ordnen wir die *Permutationsmatrix* $P_\sigma = (\delta_{i,\sigma(j)})_{i,j} \in M_n(R)$ und das *Vorzeichen* oder auch *Signum*

$$\operatorname{sign}(\sigma) = \det(P_\sigma) = \det\big((\delta_{i,\sigma(j)})_{i,j}\big) \,.$$

Unter einer *Transposition* verstehen wir eine Permutation $\tau \in S_n$, die nur zwei Elemente i und j mit $1 \leq i < j \leq n$ vertauscht, also

$$\tau(k) = \begin{cases} j & \text{falls } k = i, \\ i & \text{falls } k = j, \text{ und} \\ k & \text{sonst.} \end{cases}$$

Die Permutationsmatrix einer Transposition ist gerade die Elementarmatrix $P_{ij} = P_{\tau_{ij}}$ aus Bemerkung 3.23 (1).

4.11. Proposition. *Jede Permutation $\sigma \in S_n$ kann als Produkt $\sigma = \tau_1 \circ \cdots \circ \tau_k$ von Transpositionen $\tau_1, \ldots, \tau_k \in S_n$ geschrieben werden, und es gilt*

$$\text{(1)} \qquad \operatorname{sign}(\sigma) = (-1)^k \, .$$

Für $\rho, \sigma \in S_n$ gilt

$$\text{(2)} \qquad \operatorname{sign}(\rho \circ \sigma) = \operatorname{sign}(\rho) \cdot \operatorname{sign}(\sigma) \qquad \textit{und} \qquad \operatorname{sign}(\sigma^{-1}) = \operatorname{sign}(\sigma) \, .$$

Dabei fassen wir die Identität als „leeres Produkt“ mit $k = 0$ auf. Nach (1) ist das Vorzeichen einer Permutation stets 1 oder -1, unabhängig vom Ring R. Allerding könnte $1 = -1$ in R gelten (Beispiel: $R = \mathbb{Z}/2\mathbb{Z}$); in diesem Fall verliefert das Vorzeichen seine Information. Der Beweis unten benutzt keine Determinanten, um Permutationen als Produkte von Transpositionen darzustellen, so dass wir im Beweis von Proposition 4.7 keinen Zirkelschluss erhalten.

Beweis. Wir beweisen die erste Aussage durch Induktion über n. Für $n = 1$ gibt es nur eine Permutation, die Identität, mit

$$\operatorname{sign}(\mathrm{id}_{\{1\}}) = \det(E_1) = 1 \, .$$

Sei die Aussage für alle $\sigma' \in S_{n-1}$ bewiesen, und sei $\sigma \in S_n$. Falls $\sigma(n) = n$, sei $\sigma' = \sigma|_{\{1,\ldots,n-1\}} \in S_{n-1}$. Da σ' ein Produkt von Transpositionen aus S_{n-1}, ist σ das Produkt von Transpositionen aus S_n, die jeweils die gleichen Elemente vertauschen. Falls $\sigma(n) \neq n$, sei τ die Transposition, die $\sigma(n)$ und n vertauscht, so dass

$$(\tau \circ \sigma)(n) = n \, .$$

Nach dem obigen Argument ist $\tau \circ \sigma$ ein Produkt von Transpositionen $\tau_1 \circ \cdots \circ \tau_k$. Da $\tau = \tau^{-1}$, folgt

$$\sigma = \tau \circ \tau_1 \circ \cdots \circ \tau_k \, .$$

Sei $\sigma = \tau_1 \circ \cdots \circ \tau_k \in S_n$, dann geht P_σ aus der Einheitsmatrix hervor, indem man nacheinander k-mal je zwei Spalten vertauscht. Aus Proposition 4.3 (3) folgt (1), denn

$$\operatorname{sign}(\sigma) = \det(P_\sigma) = (-1)^k \, .$$

Zu (2) stellen wir ρ und σ als Produkte von j und k Transpositionen dar, dann erhalten wir eine Darstellung von $\rho \circ \sigma$ als Produkt von $j + k$ Transpositionen, und die erste Behauptung folgt. Die letzte ergibt sich dann aus

$$\operatorname{sign}(\sigma) \cdot \operatorname{sign}(\sigma^{-1}) = \operatorname{sign}(\sigma \cdot \sigma^{-1}) = \operatorname{sign}(\mathrm{id}) = 1 \, . \qquad \square$$

Sei $A = (a_{ij})_{i,j} \in M_n(R)$ eine Matrix, dann bezeichnen wir die Matrix A ohne die i-te Zeile und die j-te Spalte mit

$$A_{ij} = \begin{pmatrix} a_{11} & \dots & a_{1,j-1} & a_{1,j+1} & \dots & a_{1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{i-1,1} & \dots & a_{i-1,j-1} & a_{i-1,j+1} & \dots & a_{i-1,n} \\ a_{i+1,1} & \dots & a_{i+1,j-1} & a_{i+1,j+1} & \dots & a_{i+1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{n1} & \dots & a_{n,j-1} & a_{n,j+1} & \dots & a_{nn} \end{pmatrix} \in M_{n-1}(R) \, .$$

Es folgen zwei Sätze zur Berechnung von Determinanten.

4.12. Satz (Laplace-Entwicklung)**.** *Es sei $A \in M_n(R)$ mit $n \geq 1$.* Entwicklung nach der i-ten Zeile. *Für alle $i \in \{1, \dots, n\}$ gilt*

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \cdot \det(A_{ij}) \, . \tag{1}$$

Entwicklung nach der j-ten Spalte. *Für alle $j \in \{1, \dots, n\}$ gilt*

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \cdot \det(A_{ij}) \, . \tag{2}$$

Beweis. Wir betrachten die durch die rechte Seite von Formel (1) induktiv definierte Abbildung $\omega \colon M_n(R) \to R$ und zeigen wie im Beweis von Proposition 4.6, dass sie multilinear und alterniered in den Spalten von A ist. Aufgrund der Eindeutigkeitsaussage in Proposition 4.7 und Definition 4.9 reicht es zu zeigen, dass die rechte Seite für die Einheitsmatrix den Wert 1 annimmt, um die Behauptung (1) zu beweisen.

Es sei $n \geq 1$ und $i \in \{1, \dots, n\}$, und $\omega(A)$ bezeichne die rechte Seite von (1). Linearität von ω an der k-ten Stelle folgt für den k-ten Summand, da a_{ik} linear von $a_k \in R^n$ abhängt. Für die restlichen Summanden folgt sie, da $\det A_{ij}$ multilinear in den Spalten von A_{ij} ist.

Sei jetzt $a_{k+1} = a_k$ für ein $k \in \{1, \dots, n-1\}$. Dann sind der k-te und der $(k+1)$-te Summand in (1) bis auf das Vorzeichen gleich und heben sich weg; bei allen anderen Summanden stimmen zwei benachbarte Spalten von A_{ij} überein, so dass $\det(A_{ij}) = 0$. Also ist ω multilinear und alternierend.

Für die Einheitsmatrix erhalten wir

$$\omega(E_n) = \sum_{j=1}^{n} (-1)^{i+j} \, \delta_{ij} \cdot \det\big((E_n)_{ij}\big) = \det(E_{n-1}) = 1 \, ,$$

da nur der Summand mit $i = j$ beiträgt, und da nach Streichen der i-ten Spalte und Zeile aus der Einheitsmatrix E_n die Einheitsmatrix E_{n-1} wird. Damit ist (1) bewiesen.

Wir beweisen (2), indem wir die Transponierte A^t in (1) einsetzen. In Folgerung 4.15 unten zeigen wir, dass $\det A^t = \det A$ ohne Benutzung der Laplace-Entwicklung, so dass dann (2) aus (1) folgt. □

4.13. Satz (Leibniz-Formel)**.** *Für jede Matrix $A \in M_n(R)$ mit $n \geq 1$ gilt*

$$\det A = \sum_{\rho \in S(n)} \operatorname{sign}(\sigma) \cdot \prod_{j=1}^{n} a_{\rho(j),j} = \sum_{\sigma \in S(n)} \operatorname{sign}(\sigma) \cdot \prod_{i=1}^{n} a_{i,\sigma(i)} \ .$$

Beweis. Wir gehen vor wie im Beweis von Proposition 4.7 und erhalten

$$\begin{aligned} \det A = \omega_n(a_1, \ldots, a_n) &= \sum_{i_1=1}^{n} \cdots \sum_{i_n=1}^{n} \omega_n(e_{i_1}, \ldots, e_{i_n}) \cdot a_{i_1 1} \cdots a_{i_n n} \\ &= \sum_{\rho \in S_n} \omega_n(e_{\rho(1)}, \ldots, e_{\rho(n)}) \prod_{j=1}^{n} a_{\rho(j),j} = \sum_{\rho \in S_n} \det\big((\delta_{i\rho(j)})_{i,j}\big) \prod_{j=1}^{n} a_{\rho(j),j} \\ &= \sum_{\rho \in S_n} \operatorname{sign}(\rho) \prod_{j=1}^{n} a_{\rho(j),j} \ . \end{aligned}$$

Dabei haben wir alle Tupel $(i_1, \ldots, i_n)$ mit gleichen Einträgen aussortiert und die verbleibenden injektiven (und daher bijektiven) Abbildungen $j \mapsto i_j$ als Permutationen $\rho \in S_n$ aufgefasst.

Es sei schließlich $\sigma = \rho^{-1}$. Nach Proposition 4.11 (2) gilt $\operatorname{sign}(\sigma) = \operatorname{sign}(\rho)$. Indem wir über $i = \rho(j)$ summieren, erhalten wir

$$\det A = \sum_{\rho \in S_n} \operatorname{sign}(\rho) \prod_{j=1}^{n} a_{\rho(j),j} = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)} \ . \qquad \square$$

4.14. Bemerkung. Permutationen $\sigma \in S_n$ werden oft als $2 \times n$-Matrix

$$\sigma = \begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \ldots & \sigma(n) \end{pmatrix}$$

geschrieben.

Für $n = 2$ gibt es genau zwei Permutationen

$$\mathrm{id} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \qquad \text{und} \qquad \tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \ .$$

Da τ eine Transposition ist, gilt $\operatorname{sign}(\tau) = -1$, und es folgt die einfache Formel

$$\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = a_{1,\mathrm{id}(1)} \cdot a_{2,\mathrm{id}(2)} - a_{1,\tau(1)} \cdot a_{2,\tau(2)} = a_{11}\, a_{22} - a_{12}\, a_{21} \ .$$

Für $n = 3$ gibt es schon sechs Permutationen

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

wobei die erste Reihe Vorzeichen 1 und die zweite Reihe Vorzeichen -1 hat. Hiermit erhalten wir für 3×3-Matrizen die *Sarrussche Regel:*

$$\det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \begin{array}{ccccc} a_{11} & a_{12} & a_{13} & a_{11} & a_{12} \\ \searrow & & \searrow & \searrow & \cdot\cdot\searrow \\ a_{21} & a_{22} & a_{23} & a_{21} & a_{22} \\ \cdot\cdot\searrow & & \searrow & \searrow & \searrow \\ a_{31} & a_{32} & a_{33} & a_{31} & a_{32} \end{array}$$

$$= a_{11}\, a_{22}\, a_{33} + a_{12}\, a_{23}\, a_{31} + a_{13}\, a_{21}\, a_{32} - a_{11}\, a_{23}\, a_{32} - a_{12}\, a_{21}\, a_{33} - a_{13}\, a_{22}\, a_{31} \ .$$

Hierbei werden die Elemente entlang der drei durchgezogenen Linien jeweils aufmultipliziert und zusammenaddiert, und die Elemente entlang der unterbrochenen Linien werden ebenfalls aufmultipliziert und danach subtrahiert.

Für $n = 4$ gibt es bereits $4! = 24$ Permutationen; zuviele, um die Leibniz-Formel durch ein einprägsames Rechenschema darzustellen.

Zur Berechnung größerer Determinanten ist die Leibniz-Formel nicht zu empfehlen (Übung). Sie erlaubt aber einige interessante Schlussfolgerungen.

4.15. Folgerung. *Es sei R ein kommutativer Ring mit Eins und $A \in M_n(R)$.*

(1) *Es gilt* $\det(A^t) = \det A$.
(2) *Die Determinante* $\det A$ *ist multilinear und alternierend in den Zeilen der Matrix A.*
(3) *Die Determinante* $\det A$ *verschwindet, wenn die Zeilen von A linear abhängig sind.*
(4) *Die Determinante* $\det A$ *ändert sich nicht, wenn man ein Vielfaches einer Zeile zu einer anderen dazuaddiert.*
(5) *Die Determinante* $\det A$ *wechselt das Vorzeichen, wenn man zwei Zeilen vertauscht.*

Beweis. Aussage (1) ergibt sich durch Vergleich der Leibniz-Formeln aus Satz 4.13 für A und A^t, denn

$$\det(A^t) = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \cdot \prod_{i=1}^{n} a_{\sigma(i),i} = \det(A) \ .$$

Jetzt folgen (2)–(5) für A jeweils aus Definition 4.1, Proposition 4.3 und Bemerkung 4.4, angewandt auf die Matrix A^t. □

4.16. Definition. Eine Matrix $A = (a_{ij})_{i,j} \in M_n(\mathbb{k})$ heißt *in oberer* (*unterer*) *Dreiecksgestalt,* oder kurz *obere* (*untere*) *Dreiecksmatrix,* wenn $a_{ij} = 0$ für alle i, $j \in \{1, \ldots, n\}$ mit $i > j$ ($i < j$). Eine Matrix heißt in *strikter* oberer/unterer Dreiecksgestalt, wenn zusätzlich $a_{ii} = 0$ für alle $i \in \{1, \ldots, n\}$.

Somit ist die linke Matrix unten eine obere Dreiecksmatrix, und die rechte sogar in strikter Dreiecksgestalt:

$$\begin{pmatrix} a_{11} & & \dots & a_{1n} \\ 0 & a_{22} & & \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & a_{nn} \end{pmatrix}, \qquad \begin{pmatrix} 0 & a_{12} & \dots & a_{1n} \\ \vdots & \ddots & \ddots & \vdots \\ & & & a_{n-1,n} \\ 0 & & \dots & 0 \end{pmatrix}.$$

4.17. Folgerung. *Es sei R ein kommutativer Ring mit Eins.*

(1) *Seien $A \in M_k(R)$, $B \in M_{k,\ell}(R)$, $C \in M_{\ell,k}(R)$ und $D \in M_{\ell,\ell}(R)$. Dann gilt*

$$\det \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} = \det(A) \cdot \det(D) = \det \begin{pmatrix} A & 0 \\ C & D \end{pmatrix}$$

und $$\det \begin{pmatrix} B & A \\ D & 0 \end{pmatrix} = (-1)^{k\ell} \det(A) \cdot \det(D) = \det \begin{pmatrix} 0 & A \\ D & C \end{pmatrix}.$$

(2) *Es sei A eine obere oder untere Dreiecksmatrix, dann gilt*

$$\det(A) = \prod_{i=1}^{n} a_{ii}\,.$$

Beweis. Die symmetrische Gruppe $S_{k+\ell}$ enthält eine Teilmenge

$$\begin{aligned} U &= \left\{ \sigma \in S_{k+\ell} \;\middle|\; \sigma(i) \le k \text{ für } i \le k \text{ und } \sigma(i) > k \text{ für } i > k \right\} \\ &= \mathrm{Aut}(\{1, \dots, k\}) \times \mathrm{Aut}(\{k+1, \dots, k+\ell\}) \cong S_k \times S_\ell\,. \end{aligned}$$

Für $\pi \in S_k$ und $\rho \in S_\ell$ sei $\sigma = (\pi, \rho) \in U$ gegeben durch

$$\sigma(i) = (\pi, \rho)(i) = \begin{cases} \pi(i) & \text{falls } i \le k, \text{ und} \\ \rho(j) + k & \text{falls } i = k + j > k. \end{cases}$$

Schreibt man π und ρ als Produkt von Transpositionen, dann erhält man σ als Produkt all dieser Transpositionen, wobei jede zu ρ Transposition, die eigentlich i und $j \le \ell$ vertauscht, durch eine Transposition ersetzt, die stattdessen $k+i$ und $k+j$ vertauscht. Es folgt

$$\mathrm{sign}(\pi, \rho) = \mathrm{sign}(\pi) \cdot \mathrm{sign}(\rho)\,.$$

Wir bezeichnen die gesamte Matrix mit $M = (m_{ij}) \in M_{k+\ell}(R)$. Wir beweisen die erste Gleichung in (1), das heißt, wir nehmen an, dass $m_{ij} = 0$, falls $j \le k < i$. Sei nun $\sigma \in S_{k+\ell} \setminus U$, dann gibt es entweder ein $i > k$ mit $\sigma(i) \le k$ und in dem zugehörigen Summand der Leibniz-Formel taucht das Element $m_{i,\sigma(i)} = 0$ auf; oder es gibt ein $j \le k$ mit $\sigma(j) > k$, aber in diesem Fall muss es auch ein i wie oben geben, da σ bijektiv ist. Mit dieser und den vorangegangenen Überlegungen lässt sich die Leibniz-Formel aus 4.13 vereinfachen

zu

$$\begin{aligned}\det\begin{pmatrix} A & B \\ 0 & D \end{pmatrix} &= \sum_{\sigma\in U} \operatorname{sign}(\sigma) \prod_{i=1}^{k+\ell} m_{i,\sigma(i)} \\ &= \sum_{\pi\in S_k}\sum_{\rho\in S_\ell} \operatorname{sign}(\pi)\,\operatorname{sign}(\rho) \prod_{i=1}^{k} m_{i,\sigma(i)} \prod_{j=1}^{\ell} m_{j+k,\rho(j)+k} \\ &= \sum_{\pi\in S_k} \operatorname{sign}(\pi) \prod_{i=1}^{k} a_{i,\sigma(i)} \cdot \sum_{\rho\in S_\ell} \operatorname{sign}(\rho) \prod_{j=1}^{\ell} d_{j,\rho(j)} = \det A \cdot \det D\ .\end{aligned}$$

Genauso zeigt man die zweite Gleichung in der ersten Zeile von (1). Für die zweite Zeile vertauscht man erst jede der k hinteren Spalten mit jeder der ℓ vorderen, bis die Matrizen wieder die gleiche Gestalt wie in der ersten Zeile haben. Die $k \cdot \ell$ Vertauschungen ergeben den zusätzlichen Faktor $(-1)^{k\ell}$.

Wir beweisen (2) für obere Dreiecksmatrizen durch Induktion. Für $n = 1$ ist die Aussage klar. Wenn wir sie für $n-1$ bereits bewiesen haben, schreiben wir A als Blockmatrix

$$A = \det\begin{pmatrix} A' & b \\ 0 & a_{nn} \end{pmatrix}\ ,$$

dabei ist $A' \in M_{n-1}(R)$ wieder eine obere Dreiecksmatrix und $b \in R^{n-1}$. Aus (1) folgt, dass

$$\det A = \det\begin{pmatrix} A' & b \\ 0 & a_{nn} \end{pmatrix} = \det A' \cdot a_{nn} = \prod_{i=1}^{n} a_{ii}\ . \qquad \square$$

4.18. Bemerkung. In Folgerung 4.15 haben wir gesehen, wie sich die Determinante unter Zeilenumformungen verhält, also können wir Determinanten jetzt auch mit dem Gauß-Verfahren aus Satz 3.25 berechnen. Wegen Folgerung 4.17 müssen wir unsere Matrix nicht auf strenge Zeilenstufenform bringen; es reicht obere Dreiecksgestalt. In den Übungen sehen Sie, dass das Gauß-Verfahren weniger Rechenaufwand verursacht als Leibniz-Formel und Laplace-Entwicklung, es sei denn, die Matrix enthielte viele Nullen. Hauptnachteil des Gauß-Verfahrens: es funktioniert nur über Körpern.

Wir modifizieren das im Beweis von Satz 3.25 beschriebene Verfahren, angewandt auf eine Matrix A, wie folgt. Wir beginnen mit einem Vorfaktor $a_0 = 1$ und erhalten nach dem r-ten Schritt

$$\det A = \cdots = a_r \cdot \det \begin{pmatrix} 1 & a_{12} & & \cdots & & a_{1,n} \\ 0 & \ddots & \ddots & & & \vdots \\ & \ddots & 1 & a_{r,r+1} & \cdots & a_{r,n} \\ \vdots & & 0 & a_{r+1,r+1} & \cdots & a_{r+1,n} \\ & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & a_{n,r+1} & \cdots & a_{n,n} \end{pmatrix} \begin{matrix} \\ \\ \leftarrow r \\ \\ \\ \\ \end{matrix}$$

$$= a_r \cdot \det \begin{pmatrix} a_{r+1,r+1} & \cdots & a_{r+1,n} \\ \vdots & & \vdots \\ a_{n,r+1} & \cdots & a_{n,n} \end{pmatrix}$$

Hierbei haben wir Folgerung 4.17 (1) und (2) ausgenutzt und geschlossen, dass nur der untere rechte Block einen Beitrag leistet. Sie müssen also bei einer größeren Matrix gegen Ende des Verfahrens nicht mehr die ganze Matrix mitschleppen.

Falls wir im Laufe des Verfahrens eine Spalte überspringen („1. Fall“ im Beweis von Satz 3.25) ist am Ende des Verfahrens die letzte Zeile 0, folgt $\det A$ aus Folgerung 4.15 (3), und wir können das Gauß-Verfahren an dieser Stelle abbrechen. Genauso sind wir beim Invertieren in Bemerkung 3.27 (4) verfahren.

Ansonsten ändern wir dann, wenn wir im ersten Schritt tauschen müssen, das Vorzeichen der Vorfaktors wegen Folgerung 4.15 (5). Beim Normieren multiplizieren wir den Vorfaktor mit a_{rr} und erhalten unser neues a_r wegen Folgerung 4.15 (2). Anschließend räumen wir unterhalb der aktuellen Zeile aus, wobei sich der Vorfaktor wegen Folgerung 4.15 (4) nicht ändert.

Am Schluss des Verfahrens erhalten wir einen Vorfaktor a_n, multipliziert mit der Determinante einer oberen Dreicksmatrix mit Einsen auf der Diagonalen (also $a_{11} = \cdots = a_{nn} = 1$). Nach Folgerung 4.17 ist diese Determinante 1, also ist a_n die Determinante der ursprünglichen Matrix.

Unsere Definition der Determinante auf dem Umweg über das Zurückziehen von Determinantenfunktionen hat Vorteile: sie ist basisunabhängig und erlaubt es uns, relativ einfach die Multiplikativität der Determinante zu verstehen.

4.19. Satz. *Sei V ein freier R-Modul mit einer n-elementigen Basis, und es seien F, $G \in \operatorname{End} V$, dann gilt*

$$\det(F \circ G) = \det F \cdot \det G \,, \tag{1}$$

d.h., die Determinante ist multiplikativ. *Insbesondere ist* $\det\colon \operatorname{Aut} V \to R^\times$ *ein Gruppen-Homomorphismus. Für Matrizen A, $B \in M_n(R)$ gilt entsprechend*

$$\det(A \cdot B) = \det A \cdot \det B \,. \tag{2}$$

Beweis. Die Multiplikativität von det über einem Körper $\Bbbk$ folgt direkt aus der Kompositionsregel in Bemerkung 4.8 (3), denn für alle $\omega \in \Lambda^n V^*$ gilt

$$\omega \,.\, \det(F \circ G) = (F \circ G)^* \omega = G^* \circ F^* \omega = F^* \omega \,.\, \det G = \omega \,.\, \det G \cdot \det F \,.$$

Indem wir $\omega = \omega_n \neq 0$ wählen, folgt (1). Sei $F \in \operatorname{Aut} V$, dann ist F invertierbar nach Definition 2.41, also existiert eine Umkehrabbildung F^{-1} mit

$$\det F \cdot \det F^{-1} = \det(F \circ F^{-1}) = \det(\mathrm{id}_V) = 1 \,.$$

Insbesondere folgt $\det F \in \Bbbk^\times = \Bbbk \setminus \{0\}$ mit $(\det F)^{-1} = \det(F^{-1})$, und außerdem ist $\det\colon \operatorname{Aut} V \to \Bbbk^\times$ ein Gruppenhomomorphismus.

Wir erhalten (2) als Spezialfall für $M = R^n$, da $\operatorname{End}_R M = M_n(R)$. □

In der folgenden Definition verwenden wir die Matrizen A_{ij} aus der Lagrange-Entwicklung, siehe Satz 4.12.

4.20. Definition. Es sei $A \in M_n(R)$. Die *Adjunkte* von A ist definiert als

$$\operatorname{adj} A = \big((-1)^{i+j} \det(A_{ji})\big)_{i,j} \in M_n(R) \; .$$

Trotz der ähnlichen Namen hat die Adjunkte nichts mit der adjungierten Matrix aus Definition 2.80 zu tun. Die nächste Folgerung ergibt sich aus dem Laplaceschen Entwicklungssatz.

4.21. Folgerung (Cramersche Regeln)**.** *Es sei R ein kommutativer Ring mit Eins. Eine Matrix $A \in M_n(R)$ ist genau dann invertierbar, wenn*

$$\det A \in R^\times = \big\{\, r \in R \;\big|\; \textit{es gibt ein } s \in R \textit{ mit } rs = 1 \,\big\} \; ,$$

und in diesem Fall gilt

$$A^{-1} = (\det A)^{-1} \operatorname{adj} A \; . \tag{1}$$

Wenn $\det A \in R^\times$*, ist das Gleichungssystem $A \cdot x = b$ für alle $b \in R^n$ eindeutig lösbar mit*

$$x_i = \frac{\det A_i}{\det A} \; , \qquad \textit{wobei } A_i = (a_1, \ldots, a_{i-1}, b, a_{i+1}, \ldots, a_n) \in M_n(R) \; . \tag{2}$$

Beweis. Sei $A'_{ij} \in M_n(\Bbbk)$ diejenige Matrix, die wir erhalten, indem wir in A die i-te Spalte durch eine Kopie der j-ten ersetzen. Außerdem sei $\operatorname{adj} A = (c_{ij})_{i,j}$. Wir berechnen

$$\begin{aligned} \operatorname{adj} A \cdot A &= \left(\sum_{k=1}^{n} c_{ik} a_{kj} \right)_{i,j} = \left(\sum_{k=1}^{n} (-1)^{i+k} \det(A_{ki}) \cdot a_{kj} \right)_{i,j} \\ &= (\det A'_{ij})_{i,j} = \det A \cdot E_n \; . \end{aligned}$$

Im letzten Schritt haben wir zum einen ausgenutzt, dass A'_{ij} zwei gleiche Spalten hat und daher $\det A'_{ij} = 0$, falls $i \neq j$. Zum anderen ist $A'_{ii} = A$ für alle i, und die obige Formel folgt aus der Laplace-Entwicklung nach Satz 4.12 (2).

Wenn $A \in M_n(R)$ in R invertierbar ist, folgt $\det A \cdot \det A^{-1} = 1$ aus Satz 4.19 (2), also ist $\det A$ in R invertierbar. Umgekehrt, wenn $\det A$ in R invertierbar ist, existiert nach obiger Rechnung eine Inverse A^{-1} wie in (1).

Zu (2) multiplizieren wir b mit der Inversen A^{-1} aus (1) und erhalten mit der Laplace-Entwicklung nach der i-ten Spalte insbesondere

$$x_i = \det A^{-1} \, (\operatorname{adj} A \cdot b)_i = \frac{1}{\det A} \sum_{j=1}^{n} (-1)^{i+j} \det(A_{ji}) \cdot b_j = \frac{\det A_j}{\det A} \; . \qquad \square$$

4.22. Beispiel. Das Inverse einer 2×2-Matrix ist nach der 1. Cramerschen Regel gerade

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \; .$$

Bereits für $n \geq 3$ empfiehlt es sich jedoch nicht mehr, Matrizen über Körpern mit der Cramerschen Regel zu invertieren. Das Gauß-Verfahren aus Bemerkung 3.27 (4) ist schneller. Nur über Ringen funktioniert das Gauß-Verfahren in der Regel nicht.

Anhand der obigen Formel sieht man ein Problem mit Determinanten über Schiefkörpern: die quaternionische Matrix $A = \left(\begin{smallmatrix} 1+i & 1+j \\ 1-j & 1-i \end{smallmatrix}\right)$ ist invertierbar (Übung), aber es gilt

$$ad - bc = (1+i)(1-i) - (1+j)(1-j) = 2 - 2 = 0 \,.$$

4.23. Bemerkung. Mit Hilfe von Determinantenfunktionen können wir (ähnlich wie in Folgerung 3.5 über Schiefkörpern) zeigen, dass alle Basen von endlich erzeugten freien R-Moduln die gleiche Länge haben.

Seien nämlich $B = (b_1, \ldots, b_m)$ und $C = (c_1, \ldots, c_n)$ Basen, und sei $A \in M_{m,n}(R)$ die Basiswechselmatrix wie in Proposition 2.77, so dass

$$c_j = \sum_{i=1}^{m} b_i \,.\, a_{ij} \qquad \text{für alle } j \in \{1, \ldots, n\} \,.$$

Wir konstruieren ω_C wie in Proposition 4.7, dann gilt

$$1 = \omega_C(c_1, \ldots, c_n) = \sum_{i_1=1}^{m} \cdots \sum_{i_n=1}^{m} \omega_C(b_{i_1}, \ldots, b_{i_n}) \cdot a_{i_1 1} \cdots a_{i_n n}$$

Wäre $m < n$, so würde auf der rechten Seite mindestens ein Index mehr als einmal vorkommen, also $i_j = i_k$ für $j \neq k$, und die gesamte rechte Seite wäre 0 wegen Proposition 4.3 (2). Da das nicht sein kann, folgt $m \geq n$. Indem wir die Rollen von B und C vertauschen, erhalten wir auch $n \geq m$, und somit schließlich $n = m$.

Also ist die Zahl der Basiselemente eines freien R-Moduls M mit einer endlichen Basis eine Invariante des Moduls M, der *Rang* $\operatorname{rg} M \in \mathbb{N}$ von M. Im Falle eines Vektorraums ist der Rang gerade die Dimension. Für freie R-Moduln mit endlicher Basis bis auf Isomorphie ist der Rang wieder eine vollständige Invariante , das heißt, je zwei freie R-Moduln vom gleichen Rang sind isomorph, und die zugehörige Normalform ist wieder der Modul R^n der Spaltenvektoren.

Als letztes wollen wir die Ableitung der Determinante berechnen.

4.24. Definition. Es sei $A \in M_n(R)$, dann definieren wir die *Spur* von A durch

$$\operatorname{tr} A = \sum_{i=1}^{n} a_{ii} \in R \,.$$

4.25. Folgerung. *Es sei $\Bbbk = \mathbb{R}$ oder $\mathbb{C}$ und $A\colon (a,b) \to M_n(\Bbbk)$ eine differenzierbare Abbildung, dann gilt*

$$(\det A)' = \operatorname{tr}(A' \cdot \operatorname{adj} A) = \det A \cdot \operatorname{tr}(A' \cdot A^{-1}) \,.$$

Der letzte Ausdruck ist wegen der Cramerschen Regel 4.21 (1) offensichtlich nur sinnvoll, wenn $\det A \neq 0$.

BEWEIS. Es sei $t \in (a,b)$. Wir setzen $A = A(t)$ und $B = A'(t)$. Mit Hilfe der Leibniz-Formel aus Satz 4.13 sehen wir, dass die Determinante eine Summe von Produkten ist, die aus jeder Spalte genau einen Matrixeintrag enthalten. Nach der Produktregel müssen wir in jedem Produkt jeden einzelnen Faktor einmal ableiten und mit den anderen Faktoren zusammenmultiplizieren. Sei wieder $\operatorname{adj} A = (c_{ij})_{i,j}$, dann gilt

$$\begin{aligned}(\det A)'(t) &= \sum_{j=1}^{n} \det((a_1, \ldots, a_{j-1}, b_j, a_{j+1}, \ldots, a_n)) \\ &= \sum_{i,j=1}^{n} (-1)^{i+j} b_{ij} \cdot \det(A_{ij}) = \sum_{i,j=1}^{n} b_{ij}\, c_{ji} = \operatorname{tr}(B \cdot \operatorname{adj} A)\,.\end{aligned}$$

Dabei haben in der zweiten Zeile nach der j-ten Spalte entwickelt und dann die Definition der Adjunkten ausgenutzt. Mit der Cramerschen Regel 4.21 (1) folgt auch die zweite Behauptung. □

4.3. Orientierung reeller Vektorräume

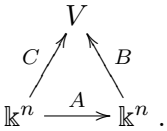
Eine einfache Folgerung aus Satz 4.19 ist die Möglichkeit, endlich erzeugte Vektorräume zu „orientieren“. Wir lassen nur Körper $\Bbbk \subset \mathbb{R}$ zu, damit wir vom „Vorzeichen“ eines Elements von $\Bbbk$ sprechen können.

4.26. Definition. Sei $\Bbbk \subset \mathbb{R}$ ein Körper, und sei V ein n-dimensionaler $\Bbbk$-Vektorraum. Seien $(x_1, \ldots, x_n)$ und $(y_1, \ldots, y_n)$ zwei Basen von V mit $y_j = \sum_{i=1}^{n} a_{ij} x_i$. Dann heißen die Basen *gleich orientiert,* wenn die Basiswechselmatrix $A = (a_{ij})_{i,j} \in \operatorname{End}(\Bbbk^n)$ positive Determinante hat.

4.27. Folgerung. *Sei V ein $\Bbbk$-Vektorraum der Dimension $n \geq 1$. Der Begriff „gleich orientiert“ definiert eine Äquivalenzrelation mit zwei Äquivalenzklassen auf der Menge aller Basen von V.*

Sei $0 \neq \omega \in \Lambda^n V^*$ eine Determinantenfunktion, dann bestehen diese Äquivalenzklassen aus allen Basen $(b_1, \ldots, b_n)$ für die $\omega(b_1, \ldots, b_n) > 0$ beziehungsweise $\omega(b_1, \ldots, b_n) < 0$ gilt.

BEWEIS. Es seien B, C Basen von V. Wir betrachten den Basiswechsel



Da Basiswechsel nach Proposition 2.77 invertierbar sind, hat A ein Inverses $A^{-1} \in \operatorname{End}(\Bbbk^n)$. Also folgt $\det A \neq 0$.

Wenn wir $\omega \in \Lambda^n V^* \neq 0$, dann folgt

$$\omega(c_1, \ldots, c_n) = (A^*\omega)(b_1, \ldots, b_n) = \det A \cdot \omega(b_1, \ldots, b_n)\,.$$

Also sind die Basen B und C genau dann gleich orientiert, wenn $\omega(b_1, \ldots, b_n)$ und $\omega(c_1, \ldots, c_n)$ das gleiche Vorzeichen haben. Da „hat das gleiche Vorzeichen

wie“ eine Äquivalenzrelation auf $\Bbbk^\times = \Bbbk \setminus \{0\} \subset \mathbb{R}^\times$ definiert, erhalten wir die gesuchte Äquivalenzrelation auf der Menge aller Basen.

Da es nur zwei mögliche Vorzeichen gibt, finden wir höchstens zwei Äquivalenzklassen. Dass es zwei gibt, sieht man daran, dass $(-b_1, b_2, \ldots, b_n)$ und $(b_1, \ldots, b_n)$ verschieden orientiert sind. □

4.28. Definition. Sei $\Bbbk \subset \mathbb{R}$ ein Körper. Eine *Orientierung* eines endlich erzeugten $\Bbbk$-Vektorraums V ist eine Äquivalenzklasse gleich orientierter Basen. Sei $\omega \neq 0$ eine Determinantenfunktion, die genau auf dieser Äquivalenzklasse positiv ist, dann heißt ω *positiv* bezüglich der gegebenen Orientierung, und umgekehrt heißt obige Orientierung *durch* ω *induziert.*

Ein Automorphismus $F \in \operatorname{Aut} V$ heißt *orientierungserhaltend* (*orientierungsumkehrend*), wenn $\det F > 0$ ($\det F < 0$).

Aus dem obigen Beweis folgt, dass die Begriffe „orientierungserhaltend“ und „orientierungsumkehrend“ nicht von der Wahl einer Orientierung auf V abhängen.

4.29. Beispiel. Auf dem Vektorraum $\mathbb{R}^n$ definieren wir die *Standard-Orientierung* so, dass die Standard-Basis $e_1, \ldots, e_n$ positiv orientiert ist. Für die Standard-Determinantenfunktion gilt

$$\omega_n(e_1, \ldots, e_n) = 1 > 0 \,,$$

also ist sie positiv bezüglich der Standard-Orientierung.

In Bemerkung 1.69 haben wir eine geometrische Interpretation des Kreuz- und des Spatproduktes gegeben. Nur das Vorzeichen hatten wir nicht klären können. Mit Hilfe der Sarrusschen Regel können wir nachrechnen, dass

$$\omega_3(u, v, w) = \langle u \times v, w \rangle$$

gilt. Also ist das Spatprodukt nach 1.69 (2) die (eindeutige) positive Determinantenfunktion, deren Absolutbetrag das Volumen von Parallelotopen angibt. Da

$$\omega_3(u, v, u \times v) = \|u \times v\|^2 \geq 0$$

gilt, ist das Kreuzprodukt $u \times v$ nach 1.69 (1) der (eindeutige) Vektor im $\mathbb{R}^3$, der senkrecht auf u und v steht, dessen Länge den Flächeninhalt des von u und v aufgespannten Parallelogramms angibt, und der (falls u und v nicht linear abhängig sind) mit u und v eine positiv orientierte Basis des $\mathbb{R}^3$ bildet.

4.30. Bemerkung. In den Übungen haben Sie die Gruppe $O(n)$ der linearen Isometrien des $\mathbb{R}^n$ kennengelernt, das heißt, der linearen Abbildungen, die das Standardskalarprodukt $\langle \cdot, \cdot \rangle$ aus Definition 1.51 erhalten. Für alle $A \in O(n)$ gilt $\det A \in \{\pm 1\}$, da

$$O(n) = \left\{ A \in M_n(\mathbb{R}) \;\middle|\; A^t \cdot A = E_n \right\} ,$$

siehe auch Proposition 2.82. Außerdem haben wir die Untergruppe $SO(n)$ der Elemente $A \in O(n)$ mit $\det A = 1$ definiert, das ist also die Untergruppe der orientierungserhaltenden Isometrien.

Genauso haben wir die Untergruppe $SL(n,\mathbb{R}) \subset GL(n,\mathbb{R})$ der Elemente mit Determinante 1 kennengelernt. Wir betrachten zunächst die Gruppe

$$GL(n,\mathbb{R})^+ = \left\{ A \in GL(n,\mathbb{R}) \;\middle|\; \det A > 0 \right\} \subset GL(n,\mathbb{R})$$

der orientierungserhaltenden Automorphismen. Als nächstes gibt es auch eine Untergruppe

$$\left\{ A \in GL(n,\mathbb{R}) \;\middle|\; |\det A| = 1 \right\} \subset GL(n,\mathbb{R})$$

der *volumenerhaltenden Automorphismen.* Dabei erinnern wir uns daran, dass das Volumen durch den Absolutbetrag einer Determinantenfunktion gemessen wird, siehe dazu den Beginn von Abschnitt 4.1. Der Durchschnitt der beiden obigen Untergruppen ist genau $SL(n,\mathbb{R})$, somit ist $SL(n,\mathbb{R})$ die Gruppe der orientierungs- und volumenerhaltenden Automorphismen des $\mathbb{R}^n$. Wie bereits am Anfang von Abschnitt 4.1 gesagt, ist über anderen Körpern wie $\mathbb{C}$ oder $\mathbb{Z}/p\mathbb{Z}$ nicht möglich, Volumina „ohne Vorzeichen“ zu erklären. Aus dem gleichen Grund ist von den obigen Untergruppen der $GL(n,\Bbbk)$ nur $SL(n,\Bbbk)$ für alle $\Bbbk$ sinnvoll definiert.

Notation

Stichwortverzeichnis