

Lineare Algebra — WS 2025/26

Sebastian Goette

Inhaltsverzeichnis

Einleitung	1
Kapitel 1. Zahlen	3
1.1. Mengen und Abbildungen	3
1.2. Natürliche Zahlen	10
1.3. Ganze und Rationale Zahlen	14
1.4. Etwas Euklidische Geometrie	21
1.5. Komplexe Zahlen und die Geometrie der Ebene	24
1.6. Geometrie des Raumes und Quaternionen	29
1.7. Zusammenfassung	36
Kapitel 2. Vektorräume und Moduln	37
2.1. Gruppen, Ringe, Körper	37
2.2. Moduln, Vektorräume und lineare Abbildungen	47
2.3. Unterräume und Quotienten	54
2.4. Linearkombinationen, Basen und Koordinaten	62
2.5. Matrizen	69
2.6. Unendliche Indexmengen	75
2.7. Zusammenfassung	78
Kapitel 3. Vektorräume über Körpern und Schiefkörpern	79
3.1. Basen	79
3.2. Dimension und Rang	82
3.3. Lineare Gleichungssysteme	88
3.4. Die Methode der kleinsten Quadrate	96
3.5. Zusammenfassung	100
Kapitel 4. Determinanten	101
4.1. Volumina und Determinantenfunktionen	101
4.2. Die Determinante	108
4.3. Orientierung reeller Vektorräume	117
4.4. Zusammenfassung	119
Notation	121
Stichwortverzeichnis	123

Einleitung

Die Lineare Algebra ist die Lehre von Vektorräumen und linearen Abbildungen. In der Schule haben Sie bereits Vektorrechnung in der Ebene und im Raum kennengelernt; dieser Stoff wird hier ausgebaut. In vielen weiterführenden Vorlesungen werden Ihnen 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 Einführung, 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 beschreiben wir die Euklidische Geometrie der Ebene \mathbb{R}^2 und des Raumes \mathbb{R}^3 mit Hilfe der komplexen Zahlen beziehungsweise der Quaternionen.

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. Allgemeiner lernen wir, wie man Elemente in freien Moduln über einem gegebenen Ring durch Koordinaten und lineare Abbildungen zwischen solchen Moduln durch Matrizen beschreibt.

In jedem Kapitel ab dem zweiten werden wir nur die Grundannahmen machen, die wir für den jeweiligen Stoff benötigen. Beispielsweise müssen wir in Kapitel 2 nicht dividieren und auch die Faktoren in Produkten nicht vertauschen, so dass wir statt über Körpern auch über nichtkommutativen Ringen arbeiten können. Wir werden aber immer nur dann allgemeinere Objekte als Vektorräume über Körpern betrachten, wenn das ohne zusätzlichen technischen Aufwand möglich ist. Aus diesem Grund ist das vorliegende Skript auch nicht schwerer zu verstehen als andere Skripten zur linearen Algebra.

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 $M = \{a_1, \dots, a_n\}$ 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

$$\emptyset = \{ \}, \quad \{ \emptyset \}, \quad \{ \{ \emptyset \}, \emptyset \} \quad \text{usw.} \dots,$$

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 . \square

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 .

1.9. BEMERKUNG. Angenommen, wir wollen zeigen, dass zwei Mengen M und N gemäß Definition 1.2 gleich sind. Dazu werden wir oft erst $M \subset N$ und dann $N \subset M$ beweisen; aus beiden Aussagen zusammen folgt $M = N$.

Es sei \emptyset die leere Menge aus Beispiel 1.4. Gilt dann $\emptyset = \{\emptyset\}$?

- Da \emptyset nach Konstruktion keine Elemente enthält, liegt jedes Element von \emptyset in $\{\emptyset\}$. Also gilt $\emptyset \subset \{\emptyset\}$.
- Die Menge $\{\emptyset\}$ enthält das Element \emptyset , aber $\emptyset \notin \emptyset$, denn \emptyset enthält ja gar keine Elemente. Also gilt $\{\emptyset\} \not\subset \emptyset$.

Und somit gilt $\emptyset \neq \{\emptyset\}$.

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.

1.10. 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 $y \in N$.

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.

1.11. BEMERKUNG. Die Notation (x, y) bezeichnet ein (geordnetes) *Paar*, allgemeiner bezeichnet (x_1, \dots, 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

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

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

1.13. BEISPIEL. Sei $M = \{1, 2\}$, dann gilt

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

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.

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

BEWEIS. Noch ein indirekter 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. \square

1.15. DEFINITION. Es seien M und N Mengen. Eine *Abbildung* $F: M \rightarrow N$ (lies „ F von M nach N “) ordnet jedem Element $x \in M$ ein Element $F(x) \in N$ zu.

Formal betrachten wir Teilmengen $X \subset M \times N$. Wir fordern, dass zu jedem $x \in M$ genau ein $y \in N$ mit $(x, y) \in X$ existiert, und setzen $F(x) = y$. Also ist X der *Graph* $\Gamma(F) = \{(x, F(x)) \mid x \in M\}$ von F .

1.16. DEFINITION. Es sei $F: M \rightarrow N$ eine Abbildung. Dann heißt M der *Definitionsbereich* von M und N der *Wertebereich*. Die Menge aller Abbildungen von M nach N wird mit $\text{Abb}(M, N)$ 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.

1.17. DEFINITION. Es sei $F: M \rightarrow N$ eine Abbildung. Dann heißt die Teilmenge

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

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 $F^{-1}(\{y\})$.

1.18. DEFINITION. Eine Abbildung $F: M \rightarrow N$ 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.

1.19. BEISPIEL. (1) Für alle Mengen M ist die Abbildung $\text{id}_M: M \rightarrow M$ mit $\text{id}_M(x) = x$ definiert. Sie heißt die *Identität* und ist stets bijektiv.

- (2) Die Abbildung $F: \mathbb{R} \rightarrow \mathbb{R}$ mit $F(x) = x^2$ ist weder injektiv noch surjektiv, denn

$$F(-2) = F(2) = 4 \quad \text{und} \quad -1 \notin \text{im}(F).$$

- (3) Die Abbildung $F: \mathbb{N} \rightarrow \mathbb{N}$ mit $F(x) = x^2$ ist injektiv. Die Abbildung $G: \mathbb{N} \rightarrow \{x^2 \mid x \in \mathbb{N}\}$ 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.

1.20. DEFINITION. Seien L, M, N Mengen und $F: M \rightarrow N$, $G: L \rightarrow M$ Abbildungen. Die *Verkettung* $F \circ G: L \rightarrow N$ (lies „ F nach G “) ist die durch

$$(F \circ G)(x) = F(G(x))$$

definierte Abbildung.

1.21. BEMERKUNG. Die Buchstaben in „ $F \circ G$ “ scheinen „falsch herum“ zu stehen, denn die Abbildungen verlaufen von links nach rechts geschrieben so:

$$\begin{array}{ccccc} L & \xrightarrow{G} & M & \xrightarrow{F} & N \\ x & \mapsto & G(x) & \longrightarrow & F(G(x)) . \end{array}$$

Aber in „ $(F \circ G)(x) = F(G(x))$ “ stimmt die Reihenfolge wieder. Beispielsweise seien $F, G: \mathbb{R} \rightarrow \mathbb{R}$ definiert durch

$$F(x) = x^2 \quad \text{und} \quad G(x) = x + 1 ,$$

dann ist

$$(F \circ G)(x) = (x + 1)^2 \quad \text{und} \quad (G \circ F)(x) = x^2 + 1 .$$

Insbesondere gilt $G \circ F \neq F \circ G$.

1.22. BEMERKUNG. Sei $F: M \rightarrow N$ eine Abbildung, und sei $U \subset M$ eine Teilmenge. Die Abbildung $G: U \rightarrow M$ mit $G(x) = x$ für alle $x \in U$ heißt *Inklusion*. Sie ist stets injektiv. Die Verkettung

$$F|_U = F \circ G: U \rightarrow N$$

(lies „ F eingeschränkt auf U “) heißt *Einschränkung* von F auf U .

1.23. SATZ. Seien L, M, N Mengen und $F, F': M \rightarrow N$, $G, G': L \rightarrow M$ 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 $F = F'$. □

1.24. SATZ. Sei $F: M \rightarrow N$ bijektiv. Dann existiert genau eine Abbildung $G: N \rightarrow M$ mit $G \circ F = \text{id}_M$ und $F \circ G = \text{id}_N$.

1.25. DEFINITION. Die Abbildung G aus Satz 1.24 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 1.24. Wir müssen zeigen, dass G *existiert*, und dass G *eindeutig* ist.

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

$$X = \{ (y, x) \in N \times M \mid (x, y) \in \Gamma(F) \} ,$$

das ist eine Menge, da M, N Mengen sind und $(x, y) \in \Gamma(F)$ eine wohldefinierte Eigenschaft ist. 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 nach Definition 1.15 der Graph einer Funktion $G: N \rightarrow M$.

Für alle $x \in M$ ist $(F(x), x) \in X = \Gamma(G)$, also $G(F(x)) = x$, und somit $G \circ F = \text{id}_M$. 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 $F \circ G = \text{id}_N$. Also existiert eine Umkehrfunktion, nämlich G . \square

1.26. DEFINITION. Zwei Mengen M und N heißen *gleichmächtig*, wenn es eine bijektive Abbildung $F: M \rightarrow N$ gibt.

1.27. 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, siehe Definition 1.42. Allerdings sollte eine Relation immer auf einer Menge definiert sein, und die Menge aller Mengen gibt es nach Folgerung 1.14 nicht.

1.28. BEISPIEL. (1) Die Mengen $M = \{1, 2, 3\}$ und $N = \{4, 7, 15\}$ sind gleichmächtig. Definiere z.B. $F: M \rightarrow N$ 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 $F: \mathbb{N} \rightarrow M$ 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 $\mathcal{N}f(n) = n+1$. Schließlich wollen wir, dass die natürlichen Zahlen eine Menge bilden, die sonst keine weiteren Objekte enthält.

1.29. ANNAHME (Peano-Axiome). *Wir nehmen an, dass es eine Menge \mathbb{N} mit einem ausgezeichneten Element $0 \in \mathbb{N}$ und einer Abbildung $\mathcal{N}f: \mathbb{N} \rightarrow \mathbb{N}$ gibt, die die folgenden Peano-Axiome erfüllt:*

- (P1) *Die Nachfolger-Abbildung ist bijektiv als Abbildung $\mathcal{N}f: \mathbb{N} \rightarrow \mathbb{N} \setminus \{0\}$.*
 (P2) *Prinzip der vollständigen Induktion. Sei $M \subset \mathbb{N}$ mit $0 \in M$, so dass für alle $m \in M$ auch $\mathcal{N}f(m) \in M$ gilt, dann ist bereits $M = \mathbb{N}$.*

Axiom (P1) besagt, dass jede Zahl genau einen Nachfolger hat, und jede Zahl außer 0 selbst Nachfolger genau einer anderen Zahl ist. Axiom (P2) besagt, dass die Menge \mathbb{N} die “kleinste” Menge ist, die (P1) 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 $0, 1, 2, \dots$ enthält, aber keine weiteren Elemente. Übrigens gibt es Autoren, für die 0 nicht zu \mathbb{N} gehört. Zur Sicherheit können Sie beide Versionen mit \mathbb{N}_0 und $\mathbb{N}_>$ bezeichnen.

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

$$\mathcal{N}f(\underline{n}) = \underline{n+1} = \{\underline{0}, \dots, \underline{n}\} = \underline{n} \cup \{\underline{n}\}.$$

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

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.

1.31. 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*.

1.32. 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 1.27 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 $F: \underline{n} \rightarrow M$ bijektiv, dann schreibe

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

Ist M umgekehrt als $\{x_1, \dots, x_n\}$ 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. Wir schreiben aber „ $\#M < \infty$ “, wenn M endlich ist.

1.33. DEFINITION. Es seien $m, n \in \mathbb{N}$, dann gilt $m \leq n$ 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.

1.34. BEMERKUNG. Aus Bemerkung 1.30 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 $(x, y) \in R$.

1.35. 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 (O1)–(O4) heißen auch *Ordnungsaxiome*.

1.36. BEISPIEL. (1) Sei M eine Menge, dann definiert „ \subset “ eine Halbordnung auf der Potenzmenge $\mathcal{P}(M)$, denn für alle $A, B, C \subset M$ gilt

$$\begin{aligned} A &\subset A, \\ A \subset B \text{ und } B \subset A &\implies A = B, \\ A \subset B \text{ und } B \subset C &\implies A \subset C. \end{aligned}$$

- (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. Nach Bemerkung 1.30 gilt $\underline{\mathbb{N}} \subset \mathcal{P}(\underline{\mathbb{N}})$, und nach Definition 1.33 entspricht „ \leq “ der Einschränkung von „ \subset “ auf $\underline{\mathbb{N}}$. Wegen (1) ist „ \subset “ eine Halbordnung auf $\underline{\mathbb{N}}$, also ist „ \leq “ eine Halbordnung auf \mathbb{N} . Zu zeigen wäre noch, dass für alle $m, n \in \mathbb{N}$ gilt

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

- (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 1.29 (P2) führt uns zur Beweismethode durch vollständige Induktion. Wir benötigen sie bald zum Rechnen.

1.37. SATZ (Vollständige 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 (P2) folgt dann $M = \mathbb{N}$. Nach Definition von M gilt $A(n)$ also für alle $n \in \mathbb{N}$. \square

Eine andere Art der vollständigen Induktion funktioniert so: Wenn gilt

- (1) $A(0)$ ist wahr, und
- (2) aus $A(0) \wedge \dots \wedge A(n)$ 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

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

induktiv mit Satz 1.37 beweist.

Wir haben in Bemerkung 1.30 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 $F(0), \dots, F(n)$ bestimmt.

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

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

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

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

BEISPIEL. Zwei einfache Rechnungen:

$$3 + 2 = 3 + \mathcal{N}f(1) = \mathcal{N}f(3 + 1) = \mathcal{N}f(3 + \mathcal{N}f(0)) = \mathcal{N}f(\mathcal{N}f(3)) = \mathcal{N}f(4) = 5,$$

$$3 \cdot 2 = 3 \cdot \mathcal{N}f(1) = 3 \cdot 1 + 3 = 3 \cdot \mathcal{N}f(0) + 3 = 3 \cdot 0 + 3 + 3 = 0 + 3 + 3 = 6.$$

1.39. 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 $\#\text{Abb}(N, M) = \#M^{\#N}$.

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 1.26 und 1.31 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 $F: \underline{n+1} = \underline{n} \dot{\cup} \{\underline{n}\} \rightarrow N$. Setze

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

so dass $\#N' = n$. Nach Induktionsvoraussetzung gilt $\#(M \dot{\cup} N') = m + n$, also existiert eine bijektive Abbildung $G': \underline{m+n} \rightarrow M \dot{\cup} N'$. Wir definieren $G: \underline{(m+n)+1} \rightarrow M \dot{\cup} N$ 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 1.38 (1) folgt

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

1.40. BEMERKUNG. Die Grundrechenarten hätten wir auch über die Eigenschaften (1)–(3) definieren können. Außerdem folgt aus (1), dass $m \leq \ell$ 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 $+: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ als Abbildung auf, dann bedeutet $(\ell + m) + n$ gerade $+(+(\ell, m), n)$, $\ell + (m + n)$ bedeutet $+(\ell, +(m, n))$.

1.41. 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

$$\ell + n = m + n \quad \implies \quad \ell = m$$

$$\ell \cdot n = m \cdot n \quad \implies \quad \ell = m \text{ oder } n = 0.$$

BEWEIS. Die Aussagen (2) folgen leicht aus Definition 1.38. Alle anderen lassen sich durch vollständige Induktion beweisen. Der Beweis von (5) ist Übung. \square

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.

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

$$(\text{Ä1}) \quad xRx \quad (\text{Reflexivität}),$$

$$(\text{Ä2}) \quad xRy \implies yRx \quad (\text{Symmetrie}),$$

$$(\text{Ä3}) \quad xRy \text{ und } yRz \implies xRz \quad (\text{Transitivität}).$$

Im Unterschied zu Halbordnungen (Definition 1.35) 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 1.12.

1.43. DEFINITION. Es sei R eine Äquivalenzrelation auf M . Für alle $x \in M$ definieren wir die (R -) Äquivalenzklasse $[x]$ von x als

$$[x] = \{ y \in M \mid xRy \} .$$

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

$$M/R = \{ [x] \mid x \in M \} \subset \mathcal{P}(M) ,$$

und alle Elemente $y \in [x]$ heißen *Repräsentanten* von $[x] \in M/R$. Die Abbildung $p: M \rightarrow M/R$ 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 $p: M \rightarrow M/=$ ist bijektiv mit $x \mapsto \{x\}$. Allerdings gilt strenggenommen nicht $M = M/=$, zum Beispiel ist

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

Sei M eine beliebige Menge. Nach Bemerkung 1.27 definiert Gleichmächtigkeit eine Äquivalenzrelation R auf der Potenzmenge $\mathcal{P}(M)$.

1.44. 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 $p: M \rightarrow M/R$ ist surjektiv, und es gilt $p(x) = p(y)$ genau dann, wenn xRy gilt.*
- (3) *Es sei $F: M \rightarrow N$ eine Abbildung. Dann existiert genau dann eine Abbildung $\bar{F}: M/R \rightarrow N$ 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:

$$\begin{array}{ccc} M & \xrightarrow{F} & N \\ p \downarrow & \nearrow \bar{F} & \\ M/R & & \end{array}$$

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 „ \implies “. Sei also $\bar{F}: M/R \rightarrow N$ 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 „ \impliedby “ 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 1.23 (7) aus der Surjektivität von p . \square

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

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

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 $m, n \in \mathbb{N}$.

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

- (1) $(m - n) = (p - q) \in \mathbb{Z} \iff m + q = n + p \in \mathbb{N} ,$
- (2) $(m - n) + (p - q) = (m + p) - (n + q) ,$
- (3) $-(m - n) = n - m ,$
- (4) $(m - n) \cdot (p - q) = (m \cdot p + n \cdot q) - (m \cdot q + n \cdot p) ,$
- (5) $(m - n) \leq (p - q) \iff m + q \leq n + p .$

Für eine Menge M und $n \in \mathbb{N}$ bezeichne M^n das n -fache kartesische Produkt von M mit sich selbst, etwa $M^2 = M \times M$. Anstelle von $m - n \in \mathbb{Z}$ betrachten wir das Paar $(m, n) \in \mathbb{N}^2$. Gemäß Bemerkung 1.45 (1) definieren wir eine Relation \sim auf der Menge \mathbb{N}^2 durch

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

Außerdem definieren wir Addition, Negatives, Multiplikation und eine Relation \leq gemäß Bemerkung 1.45 (2)–(5) durch

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

1.46. 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

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

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

$$\text{und } -(m, n) \sim -(p, q).$$

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

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

BEWEIS. Zu (1): „ \sim “ ist reflexiv und symmetrisch nach Konstruktion und dem Kommutativgesetz 1.41 (3). Zur Transitivität benutzen wir zusätzlich die Kürzungsregel 1.41 (5):

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

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

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

Wir zeigen als nächstes $(m, n) \cdot (r, s) \sim (p, q) \cdot (r, s)$ mit der Rechnung

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

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 1.40 ein $k \in \mathbb{N}$ mit

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

Wir definieren also \mathbb{Z} als Quotienten

$$\mathbb{Z} = \mathbb{N}^2 / \sim = \{ [(m, n)] \mid (m, n) \in \mathbb{N}^2 \}.$$

Proposition 1.46 garantiert wegen der universellen Eigenschaft aus 1.44 (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 $p: \mathbb{N}^2 \rightarrow \mathbb{Z}$ die Quotientenabbildung. Wir halten zunächst das Paar $(r, s) \in \mathbb{N}^2$ fest und betrachten die Abbildung $F = p \circ (\cdot + (r, s))$ wie im folgenden Diagramm:

$$\begin{array}{ccc} \mathbb{N}^2 & \xrightarrow{\cdot + (r, s)} & \mathbb{N}^2 \\ p \downarrow & \searrow F & \downarrow p \\ \mathbb{Z} & \xrightarrow{\bar{F}} & \mathbb{Z} \end{array}$$

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 $G = [(m, n)] + \cdot: \mathbb{N}^2 \rightarrow \mathbb{Z}$ wie im folgenden Diagramm:

$$\begin{array}{ccc} \mathbb{N}^2 & & \\ p \downarrow & \searrow [(m, n)] + \cdot & \\ \mathbb{Z} & \xrightarrow{\quad} & \mathbb{Z} \end{array}$$

Wir setzen das zu einem größeren Diagramm zusammen

$$\begin{array}{ccc} \mathbb{N}^2 \times \mathbb{N}^2 & \xrightarrow{+} & \mathbb{N}^2 \\ p \times \text{id}_{\mathbb{N}^2} \downarrow & & \downarrow p \\ \mathbb{Z} \times \mathbb{N}^2 & \xrightarrow{+} & \mathbb{Z} \\ \text{id}_{\mathbb{Z}} \times p \downarrow & & \downarrow \\ \mathbb{Z} \times \mathbb{Z} & \xrightarrow{+} & \mathbb{Z} \end{array}$$

dabei bleibt im oberen Parallelogramm das zweite Argument in \mathbb{N}^2 unverändert, und im unteren das erste Argument, jetzt aber in \mathbb{Z} . Also dürfen wir zwei ganze Zahlen addieren. Mit den analogen Diagrammen erhalten wir auch die Multiplikation.

1.47. DEFINITION. Die Menge $\mathbb{Z} = \mathbb{N}^2 / \sim$ heißt Menge der *ganzen Zahlen*.

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

1.48. 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

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

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:

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

BEWEIS. Das meiste folgt direkt aus Satz 1.41 und den obigen Definitionen. Die neue Gleichung

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

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

$$\begin{aligned} (p, q) \approx (r, s) &\iff p \cdot s = q \cdot r && \left(\iff \frac{p}{q} = \frac{r}{s} \right), \\ (p, q) + (r, s) &= (ps + qr, qs) && \left(\text{da } \frac{p}{q} + \frac{r}{s} = \frac{ps + qr}{qs} \right), \\ (p, q) \cdot (r, s) &= (pr, qs) && \left(\text{da } \frac{p}{q} \cdot \frac{r}{s} = \frac{pr}{qs} \right), \\ -(p, q) &= (-p, q) && \left(\text{da } -\frac{p}{q} = \frac{-p}{q} \right), \\ (p, q) \leq (r, s) &\iff p \cdot s \leq q \cdot r && \left(\iff \frac{p}{q} \leq \frac{r}{s}, \text{ da } q, s > 0 \right). \end{aligned}$$

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 $\mathbb{Z} \times (\mathbb{N} \setminus \{0\})$.

1.49. PROPOSITION. (1) Die Relation „ \approx “ ist eine Äquivalenzrelation.

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

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

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

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

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

(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 1.46, wir lassen den Beweis daher aus, ein Teil ist Übung. \square

1.50. DEFINITION. Der Quotient $\mathbb{Z} \times (\mathbb{N} \setminus \{0\}) / \approx$ 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 1.49 (2), dass wir mit Brüchen so rechnen dürfen, wie wir es aus der Schule kennen. Proposition 1.49 (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} .

1.51. 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 1.41 und 1.48, 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

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

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

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

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

Alle anderen Aussagen lassen sich ähnlich beweisen. \square

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 $0,99\dots = 1$. Andere Konstruktionen benutzen (Äquivalenzklassen von) Cauchy-Folgen oder Dedekindsche Schnitte, jeweils in \mathbb{Q} . Die reellen Zahlen haben folgende Eigenschaften.

- (1) Die reellen Zahlen bilden einen *angeordneten Körper*, das heißt, es gelten alle Rechenregeln aus Satz 1.51.
- (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, es ist der größte Körper, für den (1) und (2) gelten. Genauer: wenn es einen anderen Körper \mathbb{k} gibt, der (1) und (2) erfüllt, dann ist \mathbb{k} zu einem Teilkörper von \mathbb{R} isomorph. Noch genauer: es existiert eine eindeutige Abbildung $f: \mathbb{k} \rightarrow \mathbb{R}$, so dass für alle x, y gilt, dass $f(x + y) = f(x) + f(y)$, $f(xy) = f(x) \cdot f(y)$, $f(1) = 1$ und $f(x) \leq f(y)$ genau dann, wenn $x \leq y$, und diese Abbildung ist injektiv.
- (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 eine Möglichkeit, Vollständigkeit zu definieren, ohne analytische Begriffe zu verwenden.

In der Schule haben Sie Vektorrechnung möglicherweise wie folgt kennengelernt (meist mit $n = 2$ oder $n = 3$). Es sei

$$\mathbb{R}^n = \underbrace{\mathbb{R} \times \dots \times \mathbb{R}}_{n \text{ Faktoren}} = \{ x = (x_1, \dots, x_n) \mid x_1, \dots, x_n \in \mathbb{R} \},$$

dann definiert man eine Vektoraddition $\mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}^n$, eine skalare Multiplikation $\mathbb{R} \times \mathbb{R}^n \rightarrow \mathbb{R}^n$ für $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_n) \in \mathbb{R}^n$ und $a \in \mathbb{R}$ und

einen Nullvektor 0 durch

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

Übrigens werden wir in dieser Vorlesung nicht zwischen Orts- und Richtungsvektoren unterscheiden — ein n -Tupel kann immer beides bedeuten.

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 $\cos: [0, \pi] \rightarrow [-1, 1]$ mit Umkehrfunktion $\arccos: [-1, 1] \rightarrow [0, \pi]$. Hierbei messen wir Winkel grundsätzlich in Bogenmaß. Insbesondere gilt

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

1.52. DEFINITION. Wir definieren das *Standard-Skalarprodukt* auf \mathbb{R}^n als Abbildung $\langle \cdot, \cdot \rangle: \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}$ für Vektoren x und $y \in \mathbb{R}^n$ durch

$$(1) \quad \langle x, y \rangle = x_1 y_1 + \dots + x_n y_n.$$

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

$$(2) \quad \|x\| = \sqrt{\langle x, x \rangle} = \sqrt{x_1^2 + \dots + x_n^2}.$$

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

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

Wir sammeln einige wichtige Eigenschaften und Rechenregeln.

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

$$\begin{aligned}(1) \quad & \langle ax + by, z \rangle = a \langle x, z \rangle + b \langle y, z \rangle; \\(2) \quad & \langle x, y \rangle = \langle y, x \rangle; \\(3) \quad & \langle x, x \rangle \geq 0 \quad \text{und} \quad \langle x, x \rangle = 0 \iff x = 0.\end{aligned}$$

All das rechnet man leicht nach; für (3) nutzen wir aus, dass $x_1^2, \dots, x_n^2 \geq 0$. 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* $|\cdot|: \mathbb{R} \rightarrow \mathbb{R}$, 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 $|r| = \sqrt{r^2}$.

1.54. 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 gilt $\|x\| = 0$ und

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

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

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

aufgrund von Bemerkung 1.53 (3) also auch zu

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

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

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. \square

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.

1.55. BEMERKUNG. Aus der Cauchy-Schwarz-Ungleichung 1.54 folgt

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

also ist der Arcuscosinus in Definition 1.52 (3) erklärt und der Winkel wohldefiniert. Umgekehrt gilt also

$$(1) \quad \langle x, y \rangle = \|x\| \|y\| \cos \angle(x, y).$$

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:

$$(2) \quad \|x - y\|^2 = \|x\|^2 - 2\langle x, y \rangle + \|y\|^2 = \|x\|^2 + \|y\|^2 - 2\|x\| \|y\| \cos \angle(x, y).$$

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:

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

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

Um das rigoros zu machen, betrachten wir eine komplexe Zahl als Paar aus zwei reellen Zahlen, und definieren Addition und Multiplikation wie oben.

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

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

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

für alle $a, b, c, d \in \mathbb{R}$.

1.57. 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 1.56 nachrechnen. Beispielsweise gilt

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

Wir sehen, dass die Abbildung $\mathbb{R} \rightarrow \mathbb{C}$ mit $a \mapsto (a, 0)$ verträglich mit $+$ und \cdot ist, und 0 und $1 \in \mathbb{R}$ auf $0_{\mathbb{C}}$ und $1_{\mathbb{C}}$ 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

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

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.

1.58. BEMERKUNG. Auf \mathbb{C} gibt es keine Ordnung „ \leq “, die zu Satz 1.51 (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:

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

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

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

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

1.60. DEFINITION. Die Abbildung $\mathbb{C} \rightarrow \mathbb{C}$ mit $z \mapsto \bar{z} = \operatorname{Re}(z) - \operatorname{Im}(z) \cdot i$ heißt *komplexe Konjugation*, \bar{z} heißt das (*komplex*) *Konjugierte* von z .

1.61. BEMERKUNG. Die komplexe Konjugation ist verträglich mit allen Rechenoperationen, das heißt, es gilt

$$\begin{aligned} \bar{z} + \bar{w} &= \overline{z + w}, & \bar{z} \cdot \bar{w} &= \overline{z \cdot w}, \\ \overline{-z} &= -\bar{z}, & \overline{z^{-1}} &= \bar{z}^{-1}, \\ \overline{0} &= 0, & \overline{1} &= 1, \end{aligned}$$

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 1.57 gelten und eine Zahl i mit $i^2 = -1$ existiert. Aber i ist dadurch nicht eindeutig bestimmt, denn offensichtlich 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.

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

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

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.

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

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

1.64. 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 1.52 (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 1.54, 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 Hilfe 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, der zugehörige Punkt in $\mathbb{C} = \mathbb{R}^2$ liegt also auf dem Einheitskreis

$$S^1 = \{ w \in \mathbb{C} \mid |w| = 1 \}.$$

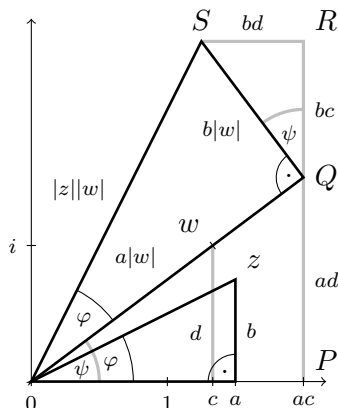
und beschreibt die Richtung von z . Es sei $\varphi \in [0, 2\pi)$ der Winkel zwischen der reellen Achse (x -Achse) und $\frac{z}{|z|}$ entgegen dem Uhrzeigersinn, dann folgt

$$\frac{z}{|z|} = \cos \varphi + i \sin \varphi \quad \text{und} \quad z = |z| (\cos \varphi + i \sin \varphi).$$

Später lernen Sie, dass $\cos \varphi + i \sin \varphi = e^{i\varphi}$. Man nennt $z = r e^{i\varphi}$ mit $r = |z|$ auch die *Polardarstellung* der Zahl $z \neq 0$. Der Winkel φ heißt auch das *Argument* von z , geschrieben $\varphi = \arg(z)$. Das Argument von 0 ist nicht definiert.

1.65. LEMMA (Geometrische Interpretation der komplexen Multiplikation). *Es sei $z \in \mathbb{C} \setminus \{0\}$, dann entspricht die Multiplikation mit z einer Streckung um den Faktor $|z|$ gefolgt von einer Drehung um den Winkel $\varphi = \arg(z)$ gegen den Uhrzeigersinn.*

BEWEIS. Wir beweisen die Aussage durch Ähnlichkeitsüberlegungen in der Ebene. Dazu sei $z = a + bi \neq 0$ gegeben und $w = c + di \neq 0$ ein beliebiger Punkt. Wir betrachten das folgende Bild.



Wir strecken das Dreieck $\Delta 0cw$ um den Faktor $a = \operatorname{Re}(z)$ und erhalten das Dreieck $\Delta 0PQ$. Anschließend strecken wir $\Delta 0cw$ um den Faktor $b = \operatorname{Im}(z)$, drehen um einen rechten Winkel gegen den Uhrzeigersinn, und verschieben, so dass wir das Dreieck ΔQRS erhalten. Dann hat der Punkt S die Koordinaten $ac - bd$ und $ad + bc$, folglich ist S der gesuchte Punkt zw .

Nach Konstruktion liegen die Punkte P , Q und R auf einer Geraden. Da sich die drei Winkel bei Q zu π ergänzen, hat das Dreieck $\Delta 0QS$ bei Q einen rechten Winkel. Die beiden Katheten haben die Längen $a|w|$ beziehungsweise $b|w|$, folglich ist $\Delta 0QS$ ähnlich zum Dreieck $\Delta 0az$ mit Streckfaktor $|w|$. Insbesondere hat es bei 0 den Winkel $\varphi = \arg(z)$.

Wir sehen also, dass der Punkt $S = zw$ einen um den Faktor $|z|$ größeren Absolutbetrag (d.h., Abstand zum Nullpunkt) hat als w , und ein um $\varphi = \arg(z)$ größeres Argument als w . Der Punkt $w = 0$ hingegen bleibt unter Multiplikation mit z unverändert. \square

Wir können also komplexe Zahlen in Polardarstellung multiplizieren durch

$$r e^{i\varphi} \cdot s e^{i\psi} = rs e^{i(\varphi+\psi)} .$$

Wir können auch Wurzeln ziehen (wobei wir uns auf das Vorzeichen einigen müssen):

$$\sqrt{r e^{i\varphi}} = \pm \sqrt{r} e^{i\frac{\varphi}{2}} .$$

Andererseits lassen sich komplexe Zahlen in Polardarstellung nicht so leicht addieren.

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

$$(-\pi, \pi] = \{ x \in \mathbb{R} \mid -\pi < x \leq \pi \}$$

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

In Definition 1.52 (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 der Arcus Cosinus sich nach unserer Definition für Winkel in $[0, \pi]$ entscheidet.

1.66. BEMERKUNG. Unter einer *Isometrie* verstehen wir eine abstandserhaltende Abbildung f . Eine Isometrie $f: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ der Ebene muss für alle $x, y \in \mathbb{R}^2$ also

$$\|f(x) - f(y)\| = \|x - y\|$$

erfüllen. Aufgrund des Cosinussatzes 1.55 (2) erhält f auch (unorientierte) Winkel, für alle $x, y, z \in \mathbb{R}^2$ gilt also

$$\angle f(x)f(y)f(z) = \angle (f(x) - f(y), f(z) - f(y)) = \angle (x - y, z - y) = \angle xyz .$$

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 $F: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ mit Hilfe komplexer Zahlen schreiben als

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

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

1.6. Geometrie des Raumes und Quaternionen

Wir geben einen kurzen Abriss der Euklidischen Geometrie des Raumes, insbesondere 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.

1.67. DEFINITION. Das *Kreuzprodukt* (*Vektorprodukt*) auf dem \mathbb{R}^3 ist eine Abbildung $\times: \mathbb{R}^3 \times \mathbb{R}^3 \rightarrow \mathbb{R}^3$ 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 kartesische Produkt von Mengen ($\mathbb{R}^3 \times \mathbb{R}^3$) aus Definition 1.10 (5) als auch das Kreuzprodukt von Vektoren bezeichnet. Missverständnisse wird es deswegen voraussichtlich nicht geben.

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

- (1) $(au + bv) \times w = a(u \times w) + b(v \times w),$
- (2) $u \times v = -v \times u.$

All dies folgt unmittelbar aus Definition 1.67. 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

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

1.69. SATZ. Für alle $u, v, w, t \in \mathbb{R}^3$ gilt

- (1) $\langle u \times v, w \rangle = \langle v \times w, u \rangle = \langle w \times u, v \rangle,$
- (2) $(u \times v) \times w = \langle u, w \rangle \cdot v - \langle v, w \rangle \cdot u = w \times (v \times u),$
- (3) $0 = (u \times v) \times w + (v \times w) \times u + (w \times u) \times v,$
- (4) $\langle u \times v, w \times t \rangle = \langle u, w \rangle \langle v, t \rangle - \langle u, t \rangle \langle v, w \rangle$

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

$$\langle u \times v, w \rangle = u_2 v_3 w_1 - u_3 v_2 w_1 + u_3 v_1 w_2 - u_1 v_3 w_2 + u_1 v_2 w_3 - u_2 v_1 w_3,$$

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:

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

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:

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

1.70. BEMERKUNG. Wir geben eine geometrische Interpretation.

(1) Satz 1.69 (4) und Bemerkung 1.55 (1) implizieren, dass

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

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 1.68 (2) und Satz 1.69 (1) folgt

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

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 4.28 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

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

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 1.56 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} .

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

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

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

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

1.72. SATZ. In \mathbb{H} gelten Assoziativ- und Kommutativgesetz für die Addition. Die Multiplikation ist assoziativ aber nicht kommutativ. Es gilt das Distributivgesetz

$$(1) \quad p \cdot (q + r) = p \cdot q + p \cdot r$$

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

$$(2) \quad -(a, u) = (-a, -u)$$

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

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

Für ein Quaternion $p = (a, u)$ gilt

$$(4) \quad p \cdot q = q \cdot p$$

für alle $q \in \mathbb{H}$ genau dann, wenn $p \in \mathbb{R}$, das heißt, wenn $u = 0$.

Für die Quaternionen-Konjugation gilt

$$(5) \quad \overline{p + q} = \bar{p} + \bar{q}, \quad \overline{-p} = -\bar{p},$$

$$(6) \quad \overline{p \cdot q} = \bar{q} \cdot \bar{p}, \quad \overline{p^{-1}} = \bar{p}^{-1}$$

für alle $p, q \in \mathbb{H}$, und für $p = (a, u) \in \mathbb{H}$ gilt

$$(7) \quad \bar{p} \cdot p = a^2 + \|u\|^2 = p \cdot \bar{p}.$$

Die Quaternionen-Konjugation ist ein *Anti-Automorphismus*, das heißt, sie respektiert alle Verknüpfungen bis auf die Multiplikation, bei der sie die Reihenfolge der Faktoren vertauscht. Daher können wir aus (1) und (6) auch Distributivität im ersten Faktor folgern.

Anstelle von p/q schreiben wir sicherheitshalber pq^{-1} , was ja nicht das gleiche wie $q^{-1}p$ sein muss. Wir erlauben Brüche von Quaternionen nur, wenn der Nenner reell ist.

BEWEIS. Die Rechenregeln für die Addition sind leicht zu überprüfen. Das Distributivgesetz (1) folgt aus den Bemerkungen 1.53 (1) und 1.68 (1):

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

Das Assoziativgesetz für die Multiplikation folgt aus Satz 1.69 (1) und (2). 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) für ein Quaternion (a, u) . Aus der Symmetrie des Skalarproduktes und der Antisymmetrie des Kreuzproduktes folgt

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

Wir setzen für v die drei Einheitsvektoren e_1, e_2, e_3 ein und erhalten $u_1 = u_2 = u_3 = 0$ aus Definition 1.71. Also gilt $u = 0$, das heißt $(a, u) \in \mathbb{R}$.

Es gilt

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

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

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

Im Beweis sieht man, dass das Kreuzprodukt wichtig ist für das Assoziativgesetz der Multiplikation.

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

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

Wegen Satz 1.72 (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.

1.74. 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:

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

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 $1_{\mathbb{H}} = (1, 0)$ können wir jetzt alle Quaternionen miteinander multiplizieren. Wir sehen, dass alle Einträge außerhalb der Diagonalen vom Kreuzprodukt in der Definition der Multiplikation in 1.71 herrühren.

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

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

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

1.75. 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 $w \in \mathbb{R}^3 \subset \mathbb{H}$ ist $qw\bar{q}$ wieder imaginär. Die Abbildung $F_q: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ 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 1.72 (1) und (4), das heißt, sie bildet Summen auf Summen ab und ist mit Streckungen verträglich. 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 1.54 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

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

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

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

Cosinus und Sinus des doppelten Winkels berechnen sich als

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

Wenn wir $\|w\| = 1$ annehmen, dann folgt aus Bemerkung 1.70, dass die Vektoren v , w und $v \times w$ aufeinander senkrecht stehen, und dass auch

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

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

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

Wenn wir in der obigen Rechnung w durch $v \times w$ ersetzen, wird $v \times w$ wegen der Graßmann-Identität zu $v \times (v \times w) = -w$. Wir sehen jetzt, dass auch $v \times w$ in der zu v senkrechten Ebene um den Winkel 2φ gedreht wird. Wegen Linearität gilt das also für den gesamten \mathbb{R}^3 . \square

Man beachte, dass φ und $\varphi + \pi$ die gleiche Drehung beschreiben, da 2π ja einer vollen Umdrehung entspricht. Zu einer Drehung gehören also genau zwei Quaternionen q und $-q$; dieses Phänomen nennt man „Spin“. Es hat sowohl in der Mathematik als auch in der Physik eine Bedeutung.

Die Drehrichtung ergibt sich aus einer „Rechte-Faust-Regel“. Sei $0 < \varphi < \pi$, so dass wir um $2\varphi \in (0, 2\pi)$ drehen. Zeigt der Daumen der rechten Hand in die Richtung von $\operatorname{Im} q = v \sin \varphi$, dann erfolgt die Drehung in Richtung der gekrümmten Finger. Ist q rein imaginär, also beispielsweise $\varphi = \frac{\pi}{2}$, dann wird um $\pi = 180^\circ$ gedreht, so dass es auf die Drehrichtung nicht mehr ankommt.

Wir haben gesehen, dass Quaternionenmultiplikation nicht kommutativ ist. Im Allgemeinen erschwert das den Umgang mit \mathbb{H} . Aber Satz 1.75 funktioniert gerade, weil \mathbb{H} nicht kommutativ ist. Wäre \mathbb{H} kommutativ, dann wäre auch $qw\bar{q} = q\bar{q}w = |q|^2 w = w$ wegen $|q| = 1$, und F_q wäre einfach die Identität.

1.76. 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 Richtung 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 1.66 können wir also jede Isometrie schreiben als

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

Dabei sind $u \in \operatorname{Im} \mathbb{H}$ und $q \in \mathbb{H}$ mit $|q| = 1$ durch F fast eindeutig festgelegt — man kann nach wie vor q durch $-q$ ersetzen.

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:

$$(F \circ G)(w) = u + q(v + rw\bar{r})\bar{q} = (u + qv\bar{q}) + qr w \overline{q\bar{r}}.$$

- Anhand der obigen Formel kann man u und q leicht bestimmen, wenn man Drehachse und -winkel kennt. Umgekehrt kann man Drehachse und -winkel ablesen, wenn u und q bekannt sind.

Aufgrunddessen lassen sich Quaternionen in der Praxis einsetzen, zum Beispiel in der Robotersteuerung und in der dreidimensionalen Bildverarbeitung.

1.77. BEMERKUNG. Analog zu den Bemerkungen 1.66 und 1.76 können wir auch alle Isometrien des \mathbb{R}^4 beschreiben durch

$$F(w) = v + pw\bar{q} \quad \text{oder} \quad F(w) = v + p\bar{w}\bar{q}.$$

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 Tripel (v, p, q)

durch das Tripel $(v, -p, -q)$ ersetzen. Es gibt also auch hier einen „Spin“. Der Zusammenhang zwischen dem Paar (p, q) und der Gestalt der Isometrie ist nicht so einfach zu erklären wie in Satz 1.75 und Bemerkung 1.76.

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

1.7. Zusammenfassung

In diesem Kapitel haben wir noch einmal den Aufbau des Zahlensystems Revue passieren lassen — von der Mengenlehre als Grundlage der natürlichen Zahlen bis hin zu komplexen Zahlen und Quaternionen. Gleichzeitig haben wir gesehen, dass Euklidische Geometrie — in ihrer analytischen Ausprägung als Vektorgeometrie — zumindest in kleineren Dimensionen — eng mit Erweiterungen der reellen Zahlen verknüpft ist.

In der folgenden Tabelle gehen wir die Zahlbereiche noch einmal durch. Ganz links steht jeweils der Zahlbereich. Direkt daneben geben wir ein „Modell“ an, das heißt, eine Konstruktion des jeweiligen Zahlbereichs aus „bekanntem“ Objekten. Es folgen in Spalte 3 die entscheidenden Neuerungen, und in der letzten Spalte Stichworte zu wichtigen Konzepten.

\mathbb{N}	$\underline{\mathbb{N}}$		Rekursive Definitionen, vollständige Induktion
\mathbb{Z}	$\mathbb{N} \times \mathbb{N} / \sim$	–	„Differenzrechnung“
\mathbb{Q}	$\mathbb{Z} \times (\mathbb{N} \setminus \{0\}) / \approx$	/	Bruchrechnung
\mathbb{R}	???		Vollständigkeit
\mathbb{C}	\mathbb{R}^2	i	Fundamentalsatz der Algebra, ebene Geometrie
\mathbb{H}	$\mathbb{R} \times \mathbb{R}^3$	j, k	Nichtkommutativ, Geometrie des Raumes

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.

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 $*$: $G \times G \rightarrow G$, 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. Dazu ersetzen wir „ $*$ “ durch eine bekannte Operation, hier „ $+$ “.

- (1) Die ganzen Zahlen \mathbb{Z} bilden eine abelsche Gruppe $(\mathbb{Z}, +)$, genannt die *unendliche zyklische Gruppe*, siehe auch Satz 1.48.
- (2) Sei $\mathbb{k} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ oder \mathbb{H} . Dann ist $(\mathbb{k}, +)$ eine abelsche Gruppe, die sogenannte *additive Gruppe* von \mathbb{k} , siehe dazu die Sätze 1.51, 1.57 und 1.72, sowie Punkt (1) am Anfang von Abschnitt 1.4.
- (3) Die natürlichen Zahlen \mathbb{N} bilden keine Gruppe, denn es fehlen die inversen Elemente.

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 Proposition.

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*

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

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

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 aus (G2') insbesondere

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

Umgekehrt gelte $g * f = g$ für alle $g \in G$, dann folgt aus (G2) 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

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

2.4. BEMERKUNG. Wir erinnern uns an die Verkettung „ \circ “ von Abbildungen aus Definition 1.20, an die Identität id_M aus Beispiel 1.19 (1) und an die Umkehrabbildungen aus Satz 1.24.

- (1) Es seien
- K, L, M, N
- Mengen und
- $F: M \rightarrow N, G: L \rightarrow M$
- und
- $H: K \rightarrow L$
- 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
- $F: M \rightarrow N$
- gilt
- $\text{id}_N \circ F = F = F \circ \text{id}_M$
- , denn für alle
- $m \in M$
- gilt
- $(\text{id}_N \circ F)(m) = \text{id}_N(F(m)) = F(m) = F(\text{id}_M(m)) = (F \circ \text{id}_M)(m)$
- .

- (3) Es sei
- F
- bijektiv. Dann existiert eine Umkehrabbildung
- S
- nach Satz 1.24, und es gilt

$$S \circ F = \text{id}_M \quad \text{und} \quad F \circ S = \text{id}_N .$$

Diese Beziehungen sehen fast so aus wie die Gruppenaxiome (G1)–(G3). Man sollte aber beachten, dass die Abbildungen $F, G, H, \text{id}_M, \text{id}_N$ 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 $F \in \text{Abb}(M, N), \text{id}_M \in \text{Abb}(M, M)$, und so weiter.

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

$$\text{Aut}(M) = \{ F: M \rightarrow M \mid F \text{ ist bijektiv} \} .$$

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

- (1) Seien F und G bijektiv, dann ist $F \circ G$ bijektiv nach Satz 1.23 (3). Also ist die Verknüpfung „ \circ “ auf $\text{Aut}(M)$ wohldefiniert.
- (2) Es gilt das Assoziativgesetz (G1) nach Bemerkung 2.4 (1).
- (3) Die Identität id_M aus Beispiel 1.19 (1) ist bijektiv. Nach Bemerkung 2.4 (2) ist id_M das neutrale Element in $(\text{Aut}(M), \circ)$.

- (4) Das Inverse zu $F \in \text{Aut}(M)$ ist die Umkehrabbildung G aus Satz 1.24. Aus Satz 1.23 (4) und (5) folgt, dass G wieder bijektiv ist, und das Axiom (G3) folgt aus Bemerkung 2.4 (3).

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

2.6. DEFINITION. Ein *Ring* $(R, +, \cdot)$ besteht aus einer Menge R mit einer *Addition* $+: R \times R \rightarrow R$ und einer *Multiplikation* $\cdot: R \times R \rightarrow R$, so dass $(R, +)$ eine abelsche Gruppe bildet, und so dass für alle $r, s, t \in R$ die folgenden Ringaxiome gelten:

$$\begin{aligned} \text{(R1)} \quad & (r \cdot s) \cdot t = r \cdot (s \cdot t) && \text{(Assoziativgesetz),} \\ \text{(R2)} \quad & \begin{cases} r \cdot (s + t) = r \cdot s + r \cdot t \\ (r + s) \cdot t = r \cdot t + s \cdot t \end{cases} && \text{(Distributivgesetze).} \end{aligned}$$

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

$$\text{(R3)} \quad 1_R \cdot r = r \cdot 1_R = r \quad \text{(Einsselement).}$$

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

$$\text{(R4)} \quad r \cdot s = s \cdot r \quad \text{(Kommutativgesetz).}$$

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, daher brauchen wir beide Gleichungen in (R2) und (R3). Wir haben auch keine Links- oder Rechtskürzungsregeln für die Multiplikation, da uns die multiplikativen Inversen fehlen.

Die Gruppe $(R, +)$ heißt die additive Gruppe des Rings $(R, +, \cdot)$. Ihr neutrales Element heißt *Nullelement* (*Null*) und 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 kommutativen Ring mit Eins, siehe Satz 1.48.
- (2) Sei $\mathbb{k} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ oder \mathbb{H} . Dann ist $(\mathbb{k}, +, \cdot)$ ein Ring mit Eins; siehe dazu die Sätze 1.51, 1.57 und 1.72, 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*

$$(1) \quad 0_R \cdot r = r \cdot 0_R = 0_R,$$

$$(2) \quad r \cdot (-s) = (-r) \cdot s = -r \cdot s.$$

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 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

$$r = 1_R \cdot r = 0_R \cdot r = 0_R. \quad \square$$

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 „ $\equiv \text{ mod } n$ “ auf \mathbb{Z} durch

$$a \equiv b \pmod{n} \quad \iff \quad \text{es gibt } k \in \mathbb{Z} \text{ mit } a - b = kn,$$

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

Wir wollen zeigen, dass es sich um eine Äquivalenzrelation handelt. Die Relation ist 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

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

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

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

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 $\mathbb{Z}/n\mathbb{Z}$ wohldefinierte Rechenoperationen definieren. Es sei etwa $a - b = kn$ und $c - d = \ell n$, dann folgt

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

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

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

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 wir $0_{\mathbb{Z}/n\mathbb{Z}} = [0]$ 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

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

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 Null 0_K , in dem für alle $k \in K \setminus \{0_K\}$ ein $k^{-1} \in K$ existiert, so dass für alle $k \in K \setminus \{0_K\}$ die folgenden Körperaxiome gelten:

$$\begin{aligned}(\text{K1}) \quad k^{-1} \cdot k &= 1_K && (\text{multiplikatives linksinverses Element}), \\ (\text{K2}) \quad 1_K &\neq 0_K && (\text{Nichttrivialität}).\end{aligned}$$

Ein Schiefkörper heißt *Körper*, wenn die Multiplikation 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 1.51, 1.57 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 1.72.
- (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 $+, \cdot : K \times K \rightarrow K$ und Elementen $0_K, 1_K \in K$ bildet genau dann einen Schiefkörper $(K, +, \cdot)$ mit Nullelement 0_K und Einselement 1_K , wenn*

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

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

BEWEIS. \implies : Sei $(K, +, \cdot)$ ein Schiefkörper, 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

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

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

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

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).

\impliedby : Wenn (1)–(3) erfüllt sind, gelten zunächst einmal (G1)–(G3) und (R2) wegen (1) und (3). Außerdem folgt $0_K \cdot k = 0_K = k \cdot 0_K$ für alle $k \in K$ mit dem gleichen Beweis wie für Proposition 2.8 (1). Es gilt $1_K \cdot a = a = a \cdot 1_K$ für alle $a \in K$ nach der obigen Überlegung, falls $a = 0$, und nach (G2) und (G2') aus Proposition 2.3 für $(K \setminus \{0_K\}, \cdot)$, falls $a \neq 0_K$. Also gilt (R3).

Aus (R3) und dem Axiom (G2) folgt für $(K \setminus \{0_K\}, \cdot)$ mit den Distributivgesetzen, dass

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

Die Kürzungsregeln in $(K, +)$ 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 , siehe oben.

Das Axiom (K1) ist gerade (G3) für $(K \setminus \{0_K\}, \cdot)$, und (K2) folgt, da $1_K \in K \setminus \{0_K\}$. Also ist $(K, +, \cdot)$ ein Schiefkörper. \square

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. Aus (G3') folgt für $k \in K^\times$ auch, dass $k \cdot k^{-1} = 1_K$.

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 1.41 (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 $1_K \cdot a = a \cdot 1_K = a$ 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 $b = 1_K$;
- (5) *Eindeutigkeit des Inversen*: aus $a \cdot b = 1_K$ oder $b \cdot a = 1_K$ für $a, b \in K$ folgen $a, b \in K^\times$ 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

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

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

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

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:

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

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

- (1) Aus dem ersten Peano-Axiom 1.29 (P1) 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 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. Wir nennen eine Zahl $p \in \mathbb{Z}$ mit $p > 1$ eine Primzahl, wenn für alle $a, b \in \mathbb{N}$ aus $p \mid ab$ folgt, dass $p \mid a$ oder $p \mid b$. Hieraus folgt, dass p keine Teiler außer 1 und sich selbst hat. 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

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

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. \square

2.17. BEISPIEL. Der Ring $\mathbb{Z}/n\mathbb{Z}$ aus Beispiel 2.9 kann also nur ein Körper sein, wenn n 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 $[a] \in \mathbb{Z}/p\mathbb{Z} \setminus \{[0]\}$ hat genau p verschiedene Vielfache in $\mathbb{Z}/p\mathbb{Z}$, denn sonst gäbe es $[b], [c] \in \mathbb{Z}/p\mathbb{Z}$ 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 $F: \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$ mit $F([b]) = [a][b]$ injektiv, und daher auch surjektiv (Übung), somit existiert $[b] \in \mathbb{Z}/p\mathbb{Z}$ mit $[a][b] = [1]$, das heißt, $[a]$ hat ein multiplikatives Inverses. Es gibt also *endliche Körper*, das heißt, Körper mit endlich vielen Elementen.

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

$$(1) \quad a_{i-1} = b_{i+1}a_i + a_{i+1} \quad \text{für alle } 1 \leq i \leq i_0 .$$

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 $d_{i_0-1}, \dots, d_1, d_0 \in \mathbb{Z}$ so, dass

$$(2) \quad d_{i-1} = d_{i+1} - d_i b_{i+1} \quad \text{für } i_0 \geq i \geq 1 .$$

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 $a_{i_0} = \text{ggT}(a_0, a_1)$.

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, \dots, 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}, \dots, a_1 und a_0 teilt. Also ist $a_{i_0} = \text{ggT}(a_0, a_1)$.

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

$$(3) \quad a_{i_0} = d_{i+1}a_i + d_i a_{i+1} .$$

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. \square

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 der Charakteristik p mit unendlich vielen Elementen.

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

2.2. Moduln, Vektorräume und lineare Abbildungen

Gruppen, Ringe und Körper begegnen uns oft dadurch, dass sie auf anderen Strukturen “wirken”. Uns interessiert hier zunächst der Fall von Ring- und Körperwirkungen; Gruppenwirkungen lernen wir später auch noch kennen.

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

- (M1) $m \cdot (r \cdot s) = (m \cdot r) \cdot s$ (*Verträglichkeit der Multiplikation*),
 (M2) $m \cdot (r + s) = m \cdot r + m \cdot s$ (*Erstes Distributivgesetz*),
 (M3) $(m + n) \cdot r = m \cdot r + n \cdot r$ (*Zweites Distributivgesetz*).

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

- (M4) $m \cdot 1 = m$ (*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 $\cdot : R \times M \rightarrow M$. In diesem Fall dreht sich in (M1)–(M4) jeweils die Reihenfolge der Faktoren um, beispielsweise würde (M1) zu

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

Auf der anderen Seite folgt Kommutativität der Addition bei einem unitären R -Modul aus den restlichen Axiomen wie in Proposition 2.12.

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

- (1) $(M, +, \cdot) = (R, +, \cdot)$ ist ein Rechts- R -Modul, wobei “+” und “ \cdot ” die gleichen Verknüpfungen sind wie in R , aufgefasst als $+: M \times M \rightarrow M$ und $\cdot : M \times R \rightarrow M$. 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 $(\{0\}, +, \cdot)$ mit $0 \cdot r = 0$ für alle $r \in R$. Er heißt der *Nullmodul*.
- (3) Jede abelsche Gruppe A wird zu einem Rechts R -Modul mit $a \cdot r = 0_A$ 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 $(M, +, \cdot)$ ein $(R, +, \cdot)$ -Rechtsmodul. Dann gilt für alle $m \in M$ und $r \in R$, dass*

- (1) $0_M \cdot r = m \cdot 0_R = 0_M$,
- (2) $m \cdot (-s) = (-m) \cdot s = -m \cdot s$.

Analoge Aussagen gelten für Linksmoduln.

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

Wir nennen 0_M das *Nullelement* oder die *Null*, bei Vektorräumen auch den *Nullvektor* von M .

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

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

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 bei 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.

In den Abschnitten 1.4–1.6 haben wir uns viel mit linearen Abbildungen eines Vektorraums in sich beschäftigt. Dieser Begriff ist bereits sinnvoll für Abbildungen zwischen Moduln.

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

- (L1) $F(\ell + m) = F(\ell) + F(m)$ (*Additivität*),
- (L2) $F(m \cdot r) = F(m) \cdot r$ (*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 $\text{Hom}_R(M, N)$ bezeichnet. Analog definieren wir *Links- R -Modulhomomorphismen*. Die Menge aller Links- R -Modulhomomorphismen von A nach B wird mit ${}_R\text{Hom}(M, N)$ bezeichnet.

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 $\text{Hom}(M, N)$ oder $\text{Hom}_R(M, N)$ für die Menge aller linearer Abbildungen.

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

$$(1) \quad F(0_M) = F(0_M \cdot 0_R) = F(0_M) \cdot 0_R = 0_N .$$

Außerdem sind lineare Abbildungen verträglich mit Linearkombinationen: Seien $m, n \in R$ und $r, s \in R$, dann gilt

$$(2) \quad F(m \cdot r + n \cdot s) = F(m \cdot r) + F(n \cdot s) = F(m) \cdot r + F(n) \cdot s .$$

2.26. 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 1.66, sowie Drehungen um Achsen durch den Nullpunkt, die Punktspiegelung am Ursprung, sowie Spiegelungen an Ebenen durch den Nullpunkte im \mathbb{R}^3 , siehe Bemerkung 1.76.
- (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 1.61 gilt

$$\overline{z + w} = \bar{z} + \bar{w} \quad \text{und} \quad \overline{z \cdot w} = \bar{z} \cdot \bar{w} .$$

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

- (3) Sei $M = R$ ein unitärer Rechts- R -Modul wie in Beispiel 2.21 (1), so dass $m \cdot r = mr$ für $m, r \in R$. Es sei $f: M \rightarrow M$ rechts R -linear und $p = f(1)$. dann folgt

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

also wird f durch Linksmultiplikation mit $p = f(1)$ gegeben. Umgekehrt ist Linksmultiplikation mit einem beliebigen $r \in R$ eine rechts- R -lineare Abbildung, denn für alle $m, n, s \in R$ gilt

$$r \cdot (m + n) = r \cdot m + r \cdot n \quad \text{und} \quad r \cdot (m \cdot s) = (r \cdot m) \cdot s .$$

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

$$(1) \quad f(x) = f(x_0) + f'(x_0) \cdot (x - x_0) + o(x - x_0) ,$$

dabei ist der zweite Term linear in $x - x_0$, und der Rest $o(x - x_0)$ geht für $x \rightarrow x_0$ 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“ $f(x_0) + f'(x_0) \cdot (x - x_0)$ (die in unserem Sinne im Allgemeinen nicht linear, sondern Summe einer konstanten und einer linearen Abbildung ist) ablesen: wenn $f'(x_0) \neq 0$ ist, ist x_0 keine lokale Extremstelle von f , und f besitzt nahe x_0 sogar eine differenzierbare Umkehrfunktion.

Außerdem rechnet man in der Analysis nach, dass Ableiten selbst eine lineare Abbildung ist, beispielsweise vom Vektorraum der differenzierbaren Funktionen auf einem Intervall I in den Raum aller Funktionen auf I , denn für differenzierbare Funktionen f und g und beliebige reelle Zahlen $r \in \mathbb{R}$ gilt

$$(f + g)' = f' + g' \quad \text{und} \quad (rf)' = r f' .$$

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

2.28. BEISPIEL. Es sei M, N Rechts- R -Moduln. Dann sind die folgenden Abbildungen immer R -linear:

(1) Die Identität aus Beispiel 1.19 (1), denn

$$\begin{aligned} \text{id}_M(\ell + m) &= \ell + m = \text{id}_M(\ell) + \text{id}_M(m) , \\ \text{und} \quad \text{id}_M(m \cdot r) &= m \cdot r = \text{id}_M(m) \cdot r . \end{aligned}$$

(2) Die Nullabbildung $0: M \rightarrow N$ mit $0(m) = 0_N$ für alle $m \in M$, denn

$$\begin{aligned} 0(\ell + m) &= 0_N = 0_N + 0_N = 0(\ell) + 0(m) , \\ \text{und} \quad 0(m \cdot r) &= 0_N = 0_N \cdot r = 0(m) \cdot r . \end{aligned}$$

2.29. PROPOSITION. *Die Hintereinanderausführung von linearen Abbildungen ist linear. Die Umkehrabbildung einer bijektiven linearen Abbildung ist linear. Die Summe linearer Abbildungen ist linear. Das Vielfache einer linearen Abbildung ist linear, wenn R kommutativ ist.*

BEWEIS. Seien L, M und N Rechts- R -Moduln, und seien $F: M \rightarrow N$ und $G: L \rightarrow M$ R -linear. Dann folgt aus der Linearität von F und G für

alle $\ell, m \in L$ und alle $r \in R$, dass

$$\begin{aligned}(F \circ G)(\ell + m) &= F(G(\ell + m)) = F(G(\ell) + G(m)) \\ &= F(G(\ell)) + F(G(m)) = (F \circ G)(\ell) + (F \circ G)(m), \\ \text{und } (F \circ G)(\ell \cdot r) &= F(G(\ell \cdot r)) = F(G(\ell) \cdot r) \\ &= F(G(\ell)) \cdot r = (F \circ G)(\ell) \cdot r.\end{aligned}$$

Also ist auch $F \circ G$ linear.

Sei jetzt $F: M \rightarrow N$ eine bijektive lineare Abbildung und $G: N \rightarrow M$ ihre Umkehrabbildung, siehe Satz 1.24. Es seien $p, q \in N$ beliebig und $\ell = G(p)$, $m = G(q) \in M$, so dass $F(\ell) = p$ und $F(m) = q$. Außerdem sei $r \in R$. Aus der Linearität von F folgt

$$\begin{aligned}G(p + q) &= G(F(\ell) + F(m)) = G(F(\ell + m)) = \ell + m = G(p) + G(q), \\ \text{und } G(q \cdot r) &= G(F(m) \cdot r) = G(F(m \cdot r)) = m \cdot r = G(q) \cdot r.\end{aligned}$$

Also ist die Umkehrabbildung G linear.

Seien jetzt $F, G: M \rightarrow N$ linear, dann ist auch $F + G$ linear, denn für alle $\ell, m \in M$ und alle $r \in R$ gilt

$$\begin{aligned}(F + G)(\ell + m) &= F(\ell + m) + G(\ell + m) = F(\ell) + F(m) + G(\ell) + G(m) \\ &= (F + G)(\ell) + (F + G)(m), \\ (F + G)(m \cdot r) &= F(m \cdot r) + G(m \cdot r) = F(m) \cdot r + G(m) \cdot r \\ &= (F + G)(m) \cdot r.\end{aligned}$$

Sei schließlich $F: M \rightarrow N$ linear, $m \in M$ und $r, s \in R$. Dann gilt

$$\begin{aligned}(F \cdot r)(m \cdot s) &= F(m \cdot s) \cdot r = F(m) \cdot s \cdot r = F(m) \cdot (sr), \\ (F \cdot r)(m) \cdot s &= F(m) \cdot r \cdot s = F(m) \cdot (rs).\end{aligned}$$

□

Achtung: wenn R nicht kommutativ ist, zeigt die obige Rechnung, dass $F \cdot r$ nicht automatisch linear sein muss.

2.30. DEFINITION. Es seien M, N Rechts- R -Moduln. Bijektive lineare Abbildungen $F: M \rightarrow N$ heißen (*Rechts- R -*) *Modulisomorphismen*. Lineare Abbildungen $F: M \rightarrow M$ 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 $\text{Iso}_R(M, N) \subset \text{Hom}_R(M, N)$ bezeichnet, die Menge aller Modul- oder Vektorraumendo- oder -automorphismen von M mit $\text{End}_R(M)$ beziehungsweise $\text{Aut}_R M \subset \text{End}_R M$. Analoge Bezeichnungen ${}_R \text{Iso}(M, N)$, ${}_R \text{End } M$ und ${}_R \text{Aut } M$ führen wir für Links- R -Moduln oder -Vektorräume ein.

Bei Aut_R und End_R lässt man gelegentlich die Klammern weg, es ist also $\text{End}_R M = \text{End}_R(M)$. 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.

2.31. FOLGERUNG (aus Proposition 2.29). *Es sei R ein Ring, und M und N seien Rechts- R -Moduln.*

- (1) *Die Automorphismen von M bilden eine Gruppe $(\text{Aut}_R M, \circ)$, die Automorphismengruppe von M .*
- (2) *Die Endomorphismen von M bilden einen Ring $(\text{End}_R M, +, \circ)$ mit Eins id_M , den Endomorphismenring von M .*
- (3) *Der Modul M ist ein Links- $\text{End}_R M$ -Modul, die skalare Multiplikation wirkt für alle $F \in \text{End}_R M$ und alle $m \in M$ durch $F \cdot m = F(m) \in M$.*
- (4) *Die Homomorphismen $\text{Hom}_R(M, N)$ bilden einen unitären Rechts- $\text{End}_R M$ -Modul, und einen unitären Links- $\text{End}_R N$ -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 2.29, genauso wie die Umkehrabbildung eines Automorphismus. Nach Beispiel 2.28 (1) ist auch die Identität ein Automorphismus. Die Gruppenaxiome ergeben sich wieder aus Bemerkung 2.4 (1)–(3).

Die Addition auf $\text{End}_R(M)$ in (2) ist die gleiche wie in Proposition 2.29, insbesondere ist die Summe zweier Endomorphismen wieder ein Endomorphismus, und das neutrale Element ist die Nullabbildung aus Beispiel 2.28 (2). Man überprüft leicht die Axiome (G1)–(G4). Aus Bemerkung 2.4 (1) und (2) folgen (R1), (R3). Als nächstes seien $F, G, H \in \text{End}_R(M)$, 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 $(\text{End}_R M, +, \circ)$ einen Ring mit Eins $1_{\text{End}_R M} = \text{id}_M$.

Wir lassen den Beweis von (3) und (4) als Übung. □

Es sei R ein Ring mit Eins. Wir betrachten $\text{Hom}_R(M, R)$ als Spezialfall von (4), mit $N = R$ als unitärem Rechts- R -Modul. In Beispiel 2.26 (3) haben wir gesehen, dass $\text{End}_R R = R$, wobei $r \in R = \text{End}_R R$ durch Multiplikation von links wirkt. Also ist $\text{Hom}_R(M, R)$ ein Links- R -Modul mit $(r \cdot f)(m) = r \cdot f(m) \in R$. Wir überprüfen (M1): für $f \in \text{Hom}_R(M, R)$, m in M und $r, s \in R$ gilt

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

Umgekehrt ist ${}_R \text{Hom}(M, R)$ ein Rechts- R -Modul mit $(f \cdot r)(m) = f(m) \cdot r \in R$.

2.32. DEFINITION. Sei M ein Rechts- R -Modul, dann ist $M^* = \text{Hom}_R(M, R)$ 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 .

2.3. Unterräume und Quotienten

In diesem Abschnitt lernen wir, wie man aus gegebenen Moduln neue konstruieren kann. Der Einfachheit halber werden wir ab jetzt meistens nur noch über Ringe mit Eins und unitäre Moduln sprechen.

2.33. DEFINITION. Es sei R ein Ring mit Eins, M ein unitärer Rechts- R -Modul und $U \subset M$ eine Teilmenge. Dann heißt U ein (*Rechts- R -*) *Unterm modul*, falls für alle $u, v \in U$ und alle $r \in R$ die folgenden Untermodulaxiome gelten:

- (U1) $0_M \in U$ (*Neutrales Element*),
- (U2) $u + v \in U$, (*abgeschlossen unter Addition*),
- (U3) $u \cdot r \in U$ (*abgeschlossen unter skalarer Multiplikation*).

Analog definieren wir Links- R -Unterm oduln 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 $0_M = u \cdot 0_R \in U$ aus (U3) und Proposition 2.22. Außerdem ist mit $u \in U$ stets auch

$$-u = u \cdot (-1) \in U.$$

Falls R keine Eins besitzt oder M nicht unitär ist, muss man in (U2) zusätzlich $-u \in U$ fordern.

2.34. 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 .

2.35. BEMERKUNG. Jeder Untermodul U eines unitären Rechts- R -Moduls $(M, +, \cdot)$ ist selbst ein unitärer Rechts- R -Modul. Zunächst einmal existiert ein Nullelement 0_M und die Verknüpfungen $+: U \times U \rightarrow U$, $-: U \rightarrow U$ und $\cdot: U \times R \rightarrow U$ sind wohldefiniert dank (U1)–(U3). Da die Axiome (G1)–(G4) und (M1)–(M4) 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 $U \rightarrow M$ aus Bemerkung 1.22 ist linear, da (L1) und (L2) offensichtlich gelten.

Auf völlig analoge Weise kann man *Untergruppen* und *Unterringe* definieren. Entscheidend ist, dass eine Teilmenge der ursprünglichen Struktur mit der

Einschränkung der vorgegebenen Verknüpfungen wieder alle Gruppen- beziehungsweise Ringaxiome erfüllt. Beispielsweise sollte ein Unterring $U \subset R$ das Element 0_R enthalten, und die Summe, das Produkt und das additive Inverse von Elementen von U sollten wieder in U liegen. Bei Körpern bevorzugt man aus sprachlichen Gründen den Begriff *Teilkörper*.

2.36. DEFINITION. Es seien M und N Rechts- R -Moduln, und es sei $F: M \rightarrow N$ rechts- R -linear. Dann definieren wir den *Kern* $\ker F$ durch

$$\ker F = F^{-1}(\{0_N\}) = \{ m \in M \mid F(m) = 0 \} .$$

Wir erinnern uns auch an das Bild im F , siehe Definition 1.16.

2.37. PROPOSITION. *Es seien M und N Rechts- R -Moduln, und $F: M \rightarrow N$ 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 $\text{im } F$ ist ein Untermodul von N , und F ist genau dann surjektiv, wenn $\text{im } F = N$.*

Die letzte Aussage in (2) ist klar nach Definition 1.18.

BEWEIS. Die Untermodulaxiome für der Kern folgen aus der Linearität von F , denn für alle $m, n \in M$ und alle $r \in R$ gilt

$$\begin{aligned} F(0_M) &= 0_N , \\ F(m) = F(n) = 0_N &\implies F(m+n) = F(m) + F(n) = 0 , \\ F(m) = 0_N &\implies F(m \cdot r) = F(m) \cdot r = 0 \end{aligned}$$

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 $\text{im } F \subset N$ folgen wieder aus der Linearität von F : für alle $m, n \in N$, $p, q \in N$ und $r \in R$ gilt

$$\begin{aligned} 0_N &= F(0_M) , \\ p = F(m) , \quad q = F(n) &\implies p + q = F(m + n) , \\ p = F(m) &\implies p \cdot r = F(p \cdot r) . \quad \square \end{aligned}$$

Wir wollen nun Quotientenmoduln in Analogie zu Beispiel 2.9 konstruieren. Dazu sei $(M, +, \cdot)$ 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

$$m \sim n \iff n - m \in U .$$

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

$$\begin{aligned} m - m = 0 \in U, \quad n - m \in U &\implies m - n = -(n - m) \in U, \\ \text{sowie } m - \ell \in U \text{ und } n - m \in U &\implies n - \ell = (n - m) + (m - \ell) \in U. \end{aligned}$$

2.38. 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. Es sei $p: M \rightarrow M/\sim$ die Quotientenabbildung, siehe Definition 1.43.

2.39. PROPOSITION. *Es sei $(M, +, \cdot)$ ein unitärer Rechts- R -Modul und $U \subset M$ ein Untermodul. Dann induzieren „ $+$ “ und „ \cdot “ Verknüpfungen*

$$+ : M/U \times M/U \rightarrow M/U \quad \text{und} \quad \cdot : M/U \times R \rightarrow M/U,$$

und $(M/U, +, \cdot)$ ist ein unitärer Rechts- R -Modul. Außerdem ist die Quotientenabbildung $p: M \rightarrow M/U$ rechts- R -linear.

BEWEIS. Wir gehen vor wie in Beispiel 2.9. Seien $m, n, p, q \in M$ mit $[m] = [n]$ und $[p] = [q] \in M/U$, also $n - m \in U$ und $q - p \in U$, und $r \in R$, dann folgt

$$\begin{aligned} (n + q) - (m + p) &= (n - m) + (q - p) && \in U, \\ (n \cdot r) - (m \cdot r) &= (n - m) \cdot r && \in U \\ \text{und } (-n) - (-m) &= -(n - m) && \in U, \end{aligned}$$

also sind Addition und skalare Multiplikation auf M/U wohldefiniert durch

$$[m] + [p] = [m + p], \quad -[m] = [-m] \quad \text{und} \quad [m] \cdot r = [m \cdot r].$$

Wir setzen $0_{M/U} = [0_M]$. Jetzt können wir (G1)–(G4), (M1)–(M4) auf die entsprechenden Axiome in M zurückführen. Beispielsweise gilt (M1), denn

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

Schließlich zur Linearität der Quotientenabbildung: für alle $m, n \in M$ und $r, s \in R$ gilt

$$p(m \cdot r + n \cdot s) = [m \cdot r + n \cdot s] = [m] \cdot r + [n] \cdot s = p(m) \cdot r + p(n) \cdot s. \quad \square$$

2.40. BEISPIEL. Wir betrachten $M = \mathbb{Z}$ als \mathbb{Z} -Modul und

$$U = n\mathbb{Z} = \{an \mid a \in \mathbb{Z}\} = \{\dots, -n, 0, n, \dots\}.$$

Dann ist U ein Untermodul, und der Quotient $M/U = \mathbb{Z}/n\mathbb{Z}$ entspricht als abelsche Gruppe dem Ring aus Beispiel 2.9. Wir dürfen $\mathbb{Z}/n\mathbb{Z}$ also auch als \mathbb{Z} -Modul auffassen.

2.41. BEMERKUNG. In Bemerkung 2.35 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 eine Gruppe

beziehungsweise ein Ring, wenn U gewisse zusätzliche Bedingungen erfüllt (siehe Übungen). Körper und Schiefkörper haben keine Quotienten.

Der folgende Satz entspricht Proposition 1.44 (3).

2.42. PROPOSITION (Universelle Eigenschaft des Quotienten). *Es seien M und N Rechts- R -Moduln, es sei $U \subset M$ ein Untermodul mit Quotientenabbildung $p: M \rightarrow M/U$, und es sei $F: M \rightarrow N$ eine rechts- R -lineare Abbildung. Dann existiert genau dann eine Abbildung $\bar{F}: M/U \rightarrow N$ mit $F = \bar{F} \circ p$, wenn $U \subset \ker F$. In diesem Fall ist \bar{F} eindeutig bestimmt und rechts- R -linear. Es gilt*

$$\operatorname{im} \bar{F} = \operatorname{im} F \quad \text{und} \quad \ker \bar{F} = \ker F/U .$$

Es gilt $U \subset \ker F$ genau dann, wenn $F|_U = 0$. In diesem Fall erhalten wir folgendes Diagramm:

$$\begin{array}{ccccc} U & \xrightarrow{\iota} & M & \xrightarrow{p} & M/U \\ & \searrow & \downarrow F & \exists! \nearrow & \\ & 0 & N & \bar{F} & \end{array}$$

BEWEIS. Zu „ \implies “ nehmen wir an, dass \bar{F} existiert. Für alle $u \in U$ gilt $[u] = 0_{M/U}$, somit

$$F(u) = \bar{F}([u]) = \bar{F}(0_{M/U}) = F(0_M) = 0_N ,$$

es folgt $U \subset \ker F$.

Zu „ \impliedby “ nehmen wir an, dass $U \subset \ker F$. Seien $m, n \in M$ mit $[m] = [n] \in M/U$, dann folgt

$$m - n \in U \subset \ker F \implies F(m) - F(n) = F(m - n) = 0_N ,$$

also gilt $F(m) = F(n)$, und $\bar{F}([m]) = F(m)$ ist wohldefiniert.

Die Eindeutigkeit von \bar{F} folgt aus Proposition 1.44 (3). Außerdem ist \bar{F} linear, denn

$$\begin{aligned} \bar{F}([m] + [n]) &= F(m + n) = F(m) + F(n) = \bar{F}([m]) + \bar{F}([n]) , \\ \bar{F}([m] \cdot r) &= F(m \cdot r) = F(m) \cdot r = \bar{F}([m]) \cdot r \end{aligned}$$

für alle $m, n \in M$ und alle $r \in R$.

Wir sehen leicht, dass $\operatorname{im} \bar{F} = \operatorname{im} F$. Es gilt $[m] \in \ker \bar{F} \subset M/U$ genau dann, wenn $m \in \ker F$, somit folgt

$$\ker \bar{F} = \ker F/U . \quad \square$$

2.43. FOLGERUNG (Homomorphiesatz). *Es seien M und N Rechts- R -Moduln und $F: M \rightarrow N$ linear. Dann induziert F einen Isomorphismus*

$$\bar{F}: M/\ker F \rightarrow \operatorname{im} F .$$

BEWEIS. Wir wenden Proposition 2.42 an mit $U = \ker F$. Da $\text{im } \bar{F} = \text{im } F$ gilt, dürfen wir \bar{F} als Abbildung mit Bildbereich $\text{im } F$ auffassen. Dann ist \bar{F} linear. Da $\ker \bar{F} = \ker F / \ker F = \{[0_M]\}$, ist \bar{F} injektiv nach Proposition 2.37 (1). Außerdem ist \bar{F} surjektiv, da $\text{im } \bar{F} = \text{im } F$. Also ist \bar{F} ein Isomorphismus. \square

Wir können also jede lineare Abbildung $F: M \rightarrow N$ wie folgt zerlegen:

$$\begin{array}{ccc} M & \xrightarrow{F} & N \\ & \searrow p & \nearrow \iota \\ & M/\ker F & \xrightarrow[\cong]{\bar{F}} \text{im } F \end{array}$$

Dabei ist p die Quotientenabbildung und ι die Inklusion. Die Abbildung \bar{F} ist eindeutig dadurch bestimmt, dass das Diagramm kommutiert. Um F zu verstehen, bieten sich die folgenden Schritte an.

- (1) Bestimme $\ker F$ als Untermodul von M .
- (2) Bestimme $\text{im } F$ als Untermodul von N .
- (3) Bestimme den Isomorphismus $\bar{F}: M/\ker F \rightarrow \text{im } F$.

2.44. 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 $F: \mathbb{R}^3 \rightarrow U$ so, dass $F(x)$ gerade dieser Schnittpunkt ist.

Mit anderen Worten schreiben wir $x = u + v$ mit $u \in U$ und $v \in V$, und definieren $F(x) = u$. Folglich existiert F , wenn sich jeder Vektor im \mathbb{R}^3 als Summe von Elementen aus U und V schreiben lässt. Und F ist eindeutig bestimmt, denn sei $x = u + v = w + z$ mit $u, w \in U$ und $v, z \in V$, dann folgt

$$U \ni u - w = z - v \in V.$$

Da wir aber $U \cap V = \{0\}$ angenommen haben, gilt $u - w = 0$, also $u = w$.

Man überprüft jetzt leicht, dass die Abbildung F auch linear ist. 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. Nach dem Homomorphiesatz 2.43 induziert F einen Isomorphismus

$$\mathbb{R}^3/V = \mathbb{R}^3/\ker F \cong \text{im } F = U.$$

Das Besondere hier ist, dass U selbst ein Unterraum von \mathbb{R}^3 ist mit $F|_U = \text{id}_U$.

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

$$x = u + v \quad \text{mit} \quad u = F(x) \in U \quad \text{und} \quad v = x - F(x) \in V,$$

und wir haben oben gesehen, dass diese Darstellung eindeutig ist. Somit liefern die Unterräume U und V ein Beispiel für die folgende Definition.

2.45. DEFINITION. Es sei M ein Rechts- R -Modul und $U, V \subset M$ Untermoduln. Die *Summe* von U und V ist gegeben durch

$$U + V = \{ u + v \mid u \in U, v \in V \} \subset M .$$

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.

2.46. BEISPIEL. Wir geben Beispiele von direkten Summen und komplementären 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

$$U = 2\mathbb{Z}/6\mathbb{Z} = \{[0], [2], [4]\} \cong \mathbb{Z}/3\mathbb{Z}$$

und $V = 3\mathbb{Z}/6\mathbb{Z} = \{[0], [3]\} \cong \mathbb{Z}/2\mathbb{Z}$

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 $p: M \rightarrow M/V$ aus Proposition 2.39.

2.47. 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*

$$U \times V \rightarrow U \oplus V \quad \text{mit} \quad (u, v) \mapsto u + v .$$

- (3) *Es sei $p: M \rightarrow M/V$ die Quotientenabbildung. Wenn U und V komplementäre Untermoduln sind, dann ist $p|_U: U \rightarrow M/V$ ein Modulisomorphismus.*

BEWEIS. Die Unterraumaxiome für $U + V$ gelten, da

$$\begin{aligned} 0_M &= 0_M + 0_M && \in U + V , \\ (t + v) + (u + w) &= (t + u) + (v + w) && \in U + V \\ \text{und} \quad (u + v) \cdot r &= u \cdot r + v \cdot r && \in U + V \end{aligned}$$

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

$$u' - u = v - v' \in U \cap V \implies u' - u = v - v' = 0_M .$$

Also ist die Abbildung in (2) auch injektiv.

Die Quotientenabbildung $p: M \rightarrow M/V$ ist linear nach Proposition 2.39. Die Inklusion $\iota: U \rightarrow M$ ist linear nach Bemerkung 2.35. Also ist auch die Abbildung $p|_U = p \circ \iota$ in (3) linear nach Proposition 2.29.

Sei $[m] \in M/V$ 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 $p|_U$ immer surjektiv.

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 $u = u'$, wenn die Summe direkt ist. Also ist $p|_U$ injektiv. \square

2.48. 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 2.44, wo man in Richtung von V auf verschiedene Ebenen in \mathbb{R}^3 projizieren kann. Das bedeutet, dass diese Beschreibung von M/V als Untermodul von M von der Wahl des Komplements U abhängt. Obwohl man oft leichter mit einem komplementären Untermodul U als mit dem Quotienten M/V arbeiten kann, ist es daher manchmal sinnvoll, den Quotienten M/V zu betrachten.

Wenn U und V gegeben sind, können wir $U \times V$ wie in Proposition 2.47 (2) als Modul betrachten und U und V mit den komplementären Untermoduln $U \times \{0\}, \{0\} \times V \subset M$ identifizieren. Wir nennen $U \times V$ die *direkte Summe* $U \oplus V$ von U und V .

Die direkte Summe erfüllt gleich zwei „universelle Eigenschaften“. Sei dazu $M = U \oplus V$, dann betrachten wir die Inklusionsabbildungen $\iota_U: U \rightarrow M$ und $\iota_V: V \rightarrow M$. Wenn wir wie oben $M/U \cong V$ und $M/V \cong U$ identifizieren, erhalten wir auch Projektionen $p_U: M \rightarrow U$ und $p_V: M \rightarrow V$, so dass insbesondere $m = p_U(m) + p_V(m)$ für alle $m \in M$.

2.49. PROPOSITION (Universelle Eigenschaften der direkten Summe). *Es sei M ein Rechts- R -Moduln und $U, V \subset M$ Untermoduln, so dass $M = U \oplus V$.*

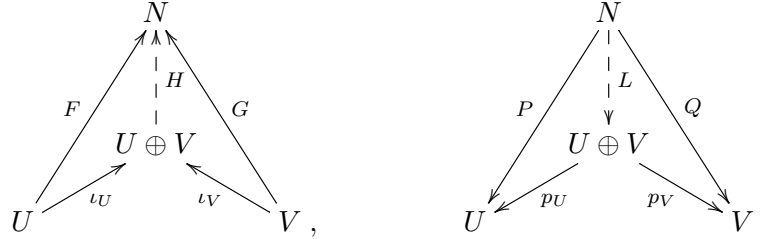
(1) *Die Inklusions- und Projektionsabbildungen erfüllen*

$$\begin{aligned} p_U \circ \iota_U &= \text{id}_U , & p_U \circ \iota_V &= 0: V \rightarrow U , \\ p_V \circ \iota_U &= 0: U \rightarrow V & \text{und} & & p_V \circ \iota_V &= \text{id}_V . \end{aligned}$$

(2) *Universelle Eigenschaft des Koproduktes: Sei N ein weiterer Rechts- R -Modul und seien $F: U \rightarrow N$ und $G: V \rightarrow N$ linear, dann existiert genau eine lineare Abbildung $H: U \oplus V \rightarrow N$, 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 $P: N \rightarrow U$ und $Q: N \rightarrow V$ linear, dann existiert genau eine lineare Abbildung $L: N \rightarrow U \oplus V$, 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

$$\begin{aligned} (p_U \circ \iota_U)(u) &= p_U(u + 0_M) = u = \text{id}_U(u), \\ (p_V \circ \iota_U)(u) &= p_V(u + 0_M) = 0 = 0(u) \in V. \end{aligned}$$

Also gilt $p_U \circ \iota_U = \text{id}_U$ 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 2.29. Sie leistet das Gewünschte, denn wegen (1) gilt

$$\begin{aligned} (F \circ p_U + G \circ p_V) \circ \iota_U &= F \circ \underbrace{p_U \circ \iota_U}_{=\text{id}_U} + G \circ \underbrace{p_V \circ \iota_U}_{=0} = F, \\ (F \circ p_U + G \circ p_V) \circ \iota_V &= F \circ p_U \circ \iota_V + G \circ p_V \circ \iota_V = G. \end{aligned}$$

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

$$\iota_U \circ P + \iota_V \circ Q: N \rightarrow M = U \oplus V$$

linear nach Proposition 2.29. Mithilfe von (1) überprüft man wieder, dass

$$p_U \circ (\iota_U \circ P + \iota_V \circ Q) = P \quad \text{und} \quad p_V \circ (\iota_U \circ P + \iota_V \circ Q) = Q. \quad \square$$

2.4. Linearkombinationen, Basen und Koordinaten

Bisher haben wir Moduln sehr abstrakt betrachtet. Auf der anderen Seite haben wir uns in den Abschnitten 1.4–1.6 die konkreten Vektorräume \mathbb{R}^n angeschaut, speziell für $n = 2$ und $n = 3$. Im Rest dieses Kapitels wollen wir eine Brücke zwischen beiden Welten schlagen. Damit das alles reibungslos funktioniert, betrachten wir nur noch Ringe mit Eins und unitäre Moduln.

2.50. BEMERKUNG. Es sei I eine Menge und M ein Rechts- R -Modul. Dann bilden die Abbildungen $\text{Abb}(I, M)$ wieder einen Rechts- R -Modul M^I . Für alle $f, g: I \rightarrow M$ und alle $r \in R$ definieren wir $f + g, f \cdot r \in M^I$ durch

$$(f + g)(i) = f(i) + g(i) \quad \text{und} \quad (f \cdot r)(i) = f(i) \cdot r \in M.$$

Die Gruppenaxiome (G1)–(G4) und die Modulaxiome (M1)–(M4) lassen sich für jedes Element $i \in I$ einzeln überprüfen. Beispielsweise folgt (M2) für M^I aus (M2) für M , da

$$a(i) \cdot (r + s) = a(i) \cdot r + a(i) \cdot s.$$

Der folgende Spezialfall ist zentral für die Vorlesung.

2.51. BEISPIEL. Es sei R ein Ring mit Eins und $n \in \mathbb{N}$. Wir fassen R als Rechts- R -Modul auf wie in Beispiel 2.21 (1) und bezeichnen das n -fache kartesische Produkt von R mit $R^n = \underbrace{R \times \cdots \times R}_{n \text{ Faktoren}}$. Traditionell schreibt man Elemente von R^n als *Spaltenvektoren*

$$(1) \quad R^n = \left\{ \left(\begin{array}{c} a_1 \\ \vdots \\ a_n \end{array} \right) \mid a_1, \dots, a_n \in R \right\}.$$

Wir identifizieren $a \in R^n$ mit einer Abbildung $a: \{1, \dots, n\} \rightarrow M$, indem wir jedem $i \in \{1, \dots, n\}$ das Element $a_i \in M$ zuordnen. Wie oben erhalten wir einen Rechts- R -Modul mit den Rechenoperationen

$$(2) \quad \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ \vdots \\ a_n + b_n \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \cdot r = \begin{pmatrix} a_1 \cdot r \\ \vdots \\ a_n \cdot r \end{pmatrix}.$$

Für alle $1 \leq j \leq n$ sei

$$(3) \quad e_j = \begin{pmatrix} \delta_{1j} \\ \vdots \\ \delta_{nj} \end{pmatrix} = j \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \in R^n$$

der i -te *Standardbasisvektor*, hierbei heißt

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

das *Kroneckersymbol*. Der Vektor e_j hat also als j -ten Eintrag die 1, und sonst überall 0. Wir nennen (e_1, \dots, e_n) die *Standardbasis* des R^n . Wir können jedes

Element $a \in R^n$ als Linearkombination der Standardbasis schreiben:

$$(4) \quad a = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \cdot a_1 + \cdots + \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \cdot a_n = \sum_{i=1}^n e_i \cdot a_i .$$

Man überzeugt sich leicht, dass diese Darstellung auch eindeutig ist, das heißt, aus $a = \sum_{i=1}^n e_i \cdot r_i$ mit $r_1, \dots, r_n \in R$ folgt $r_i = a_i$.

2.52. BEISPIEL. Wir können auf der Menge R^n analog die Addition wie oben und eine Linksmultiplikation $r \cdot (a_1, \dots, a_n) = (ra_1, \dots, ra_n)$ definieren, wobei wir die Elemente jetzt als *Zeilenvektoren* schreiben. Dann erhalten wir einen Links- R -Modul nR . Die Gruppen- und Modulaxiome werden wie oben bewiesen. Als abelsche Gruppen sind R^n und nR isomorph, als Moduln jedoch nur dann, wenn R kommutativ ist, siehe Bemerkung 2.23. Als Standardbasisvektoren wählen wir entsprechend

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

Auch in diesem Fall lässt sich jedes Element $a \in {}^nR$ eindeutig darstellen als

$$(a_1, \dots, a_n) = \sum_{i=1}^n a_i \cdot \varepsilon_i .$$

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

$$s_i = s_{i-1} + a_i \in G \quad \text{für } i = 1, \dots, n .$$

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

$$(2.1) \quad \sum_{i=1}^n a_i = s_n = a_1 + \cdots + a_n \in G .$$

Diese Konstruktion ist die Grundlage für die folgende Definition.

2.53. DEFINITION. Sei M ein Rechts- R -Modul, $n \in \mathbb{N}$, und seien $m_1, \dots, m_n \in M$. Für alle $r_1, \dots, r_n \in R$ heißt

$$(1) \quad \sum_{i=1}^n m_i \cdot r_i \in M .$$

eine *Linearkombination* der Elemente m_1, \dots, m_n .

2.54. BEMERKUNG. Linearkombinationen werden uns regelmäßig begegnen. Zum Beispiel haben wir im Beweis der Cauchy-Schwarz-Ungleichung 1.54 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 1.75 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.

Die folgende Überlegung ist die Grundlage für das Rechnen mit Matrizen.

2.55. SATZ (Universelle Eigenschaft des freien Moduls). *Es sei R ein Ring mit Eins, $n \in \mathbb{N}$, und M sei ein unitärer Rechts- R -Modul. Dann existiert eine bijektive Abbildung*

$$(1) \quad \Phi: \text{Hom}_R(R^n, M) \xrightarrow{\cong} M^n$$

mit $f \mapsto (f(e_1), \dots, f(e_n))$.

Die Umkehrabbildung Ψ ordnet einem Tupel $A = (a_1, \dots, a_n) \in M^n$ eine lineare Abbildung $\Psi_A: R^n \rightarrow M$ zu mit

$$(2) \quad \Psi_A \left(\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} \right) = \sum_{i=1}^n a_i \cdot r_i.$$

Mit anderen Worten ist eine lineare Abbildung $R^n \rightarrow M$ genau durch die Bilder der Standardbasisvektoren e_1, \dots, e_n bestimmt, die wir frei vorgeben dürfen. Das ist die *universelle Eigenschaft des freien Moduls R^n* . Wir schreiben das als Diagramm

$$\begin{array}{ccc} \{e_1, \dots, e_n\} & \hookrightarrow & R^n \\ & \searrow & \downarrow \\ & & M \end{array} \quad \begin{array}{c} \exists! \Psi_A \\ \downarrow \end{array}$$

Das Symbol „ $\exists!$ “ bedeutet „es gibt genau ein“. Wir hatten $\text{Hom}_R(R^n, M)$ in Folgerung 2.31 (4) als Links- $\text{End}_R(M)$ - und Rechts- $\text{End}_R(R^n)$ -Modul aufgefasst. Auch M^n trägt solche eine Struktur, uns interessiert M^n aber im Moment nur als Menge.

BEWEIS. Um die Bijektivität in (1) zu prüfen, definieren wir Ψ wie in (2). Für ein beliebiges Tupel $A = (a_1, \dots, a_n) \in M^n$, $r, s \in R^n$ und $t \in R$ gilt nach Beispiel 2.51 (2), dass

$$\begin{aligned} \Psi_A \left(\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} + \begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} \right) &= \sum_{i=1}^n a_i \cdot (r_i + s_i) = \sum_{i=1}^n a_i \cdot r_i + \sum_{i=1}^n a_i \cdot s_i \\ &= \Psi_A \left(\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} \right) + \Psi_A \left(\begin{pmatrix} s_1 \\ \vdots \\ s_n \end{pmatrix} \right) \\ \text{und} \quad \Psi_A \left(\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} \cdot t \right) &= \sum_{i=1}^n a_i \cdot (r_i \cdot t) = \sum_{i=1}^n (a_i \cdot r_i) \cdot t \\ &= \Psi_A \left(\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} \right) \cdot t. \end{aligned}$$

Das mittlere Gleichheitszeichen folgt jeweils durch vollständige Induktion. Also ist $\Psi_A: R^n \rightarrow M$ linear, und wir haben $\Psi: M^n \rightarrow \text{Hom}_R(R^n, M)$ konstruiert.

Wir starten mit $A \in M^n$. Aus der Definition von e_i in Beispiel 2.51 (3) und der Konstruktion von $\Psi_A: R^n \rightarrow M$ folgt, dass

$$\Psi_A(e_j) = \sum_{i=1}^n a_i \cdot \delta_{ij} = a_j,$$

also erhalten wir das ursprüngliche Tupel zurück.

Sei jetzt $f: R^n \rightarrow M$ rechts- R -linear und $A = \Phi(f) = (f(e_1), \dots, f(e_n))$. Um $\Psi_A = f$ zu zeigen, benutzen wir Beispiel 2.51 (4). Durch Induktion über n folgt aus Linearität von Ψ_A und f , dass

$$\begin{aligned} \Psi_A \left(\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} \right) &= \Psi_A \left(\sum_{i=1}^n e_i \cdot r_i \right) = \sum_{i=1}^n \Psi_A(e_i) \cdot r_i = \sum_{i=1}^n f(e_i) \cdot r_i \\ &= f \left(\sum_{i=1}^n e_i \cdot r_i \right) = f \left(\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} \right), \end{aligned}$$

wir erhalten also f zurück. Somit sind Φ und Ψ zueinander invers. \square

2.56. FOLGERUNG. *Es sei $f: M \rightarrow N$ eine lineare Abbildung zwischen unitären Rechts- R -Moduln, und es sei $A = (a_1, \dots, a_n)$ ein n -Tupel in M . Für alle $r_1, \dots, r_n \in R$ gilt dann*

$$f \left(\sum_{i=1}^n a_i \cdot r_i \right) = \sum_{i=1}^n f(a_i) \cdot r_i.$$

Wir sagen auch „lineare Abbildungen sind mit Linearkombinationen verträglich“, siehe Bemerkung 2.25 (2).

BEWEIS. Wir bezeichnen das n -Tupel $(f(a_1), \dots, f(a_n))$ in N mit B . Nach Satz 2.55 erhalten wir eine lineare Abbildungen $\Psi_B: R^n \rightarrow N$. Nach Proposition 2.29 ist $f \circ \Psi_A: R^n \rightarrow N$ auch linear. Da beide Abbildungen die Standardbasisvektoren auf dieselben Elemente $f(a_i) \in N$ abbilden, folgt $\Psi_B = f \circ \Psi_A: R^n \rightarrow N$. Für ein konkretes Element von R^n bedeutet das, dass

$$f \left(\sum_{i=1}^n a_i \cdot r_i \right) = (f \circ \Psi_A) \left(\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} \right) = \Psi_B \left(\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} \right) = \sum_{i=1}^n f(a_i) \cdot r_i. \quad \square$$

Mit Hilfe des Begriffs „Linearkombination“ können wir jetzt ganz klassisch sagen, wann ein Tupel A von Elementen ein Modul M erzeugt, linear unabhängig ist, oder eine Basis bildet. Im Anschluss überlegen wir uns, was das mit der Abbildung Ψ_A zu tun hat.

2.57. DEFINITION. Es sei M ein unitärer Rechts- R -Modul, $n \in \mathbb{N}$, und $A = (a_1, \dots, a_n)$ ein n -Tupel in M . Ein Element $m \in M$ heißt *als Linearkombination*

der a_1, \dots, a_n darstellbar, wenn es $r_1, \dots, r_n \in R$ gibt, so dass $\sum_{i=1}^n a_i \cdot r_i = m$. Das Erzeugnis von A (über R) in M ist die Menge

$$\langle A \rangle = \langle A \rangle_R = \left\{ \sum_{i=1}^n a_i \cdot r_i \mid r_1, \dots, r_n \in R \right\} \subset M.$$

Falls $M = \langle A \rangle$, heißt A ein Erzeugendensystem von M , und A erzeugt M (über R). Wenn es ein A wie oben gibt, das M erzeugt, heißt M endlich erzeugt (über R).

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

2.58. 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. Über R erzeugt $\{1\}$ nur die Teilmenge $\mathbb{R} \subset \mathbb{C}$, während $\{1, i\}$ eine Erzeugermenge über \mathbb{R} ist. Aus diesem Grund ist es manchmal wichtig, 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 und \mathbb{C} überabzählbar ist, ist \mathbb{C} über \mathbb{Q} nicht endlich erzeugt.

2.59. DEFINITION. Es sei M ein unitärer Rechts- R -Modul, $n \in \mathbb{N}$ und $A = (a_1, \dots, a_n)$ ein n -Tupel in M . Falls für alle $r_1, \dots, r_n \in R$ gilt, dass

$$0 = \sum_{i=1}^n a_i \cdot r_i \quad \implies \quad r_1 = \dots = r_n = 0,$$

dann heißt A linear unabhängig. Andernfalls heißt A linear abhängig.

Sei M ein Rechts- R -Modul. Eine (endliche) Basis von M ist ein linear unabhängiges Erzeugendensystem A von M . Ein endlich erzeugter unitärer Rechts- R -Modul M heißt frei (über R), wenn er eine Basis besitzt.

Beachte, dass wir Basen immer als Tupel, nicht als Teilmengen von M auffassen. Manche Autoren sprechen daher von „angeordneten Basen“. Später benutzen wir für Basen den Buchstaben B anstelle von A .

2.60. BEISPIEL. Es sei $n \geq 1$ und $M = \mathbb{Z}/n\mathbb{Z}$ der \mathbb{Z} -Modul aus Beispiel 2.40. Für alle $[a] \in \mathbb{Z}/n\mathbb{Z}$ gilt $[a] \cdot n = [an] = [0]$, 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

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

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 hat $\mathbb{Z}/n\mathbb{Z}$ keine Basis 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 $[0] = [1] \cdot r$ folgt $r = [0]$, da $[1]$ gleichzeitig das Einselement von R ist. Also ist E auch linear unabhängig über R . Es ist also auch bei linearer Abhängigkeit wichtig, den Grundring mit anzugeben.

2.61. BEISPIEL. Als Vektorraum über \mathbb{C} hat \mathbb{C} zum Beispiel die Basis (1). Als Vektorraum über \mathbb{R} bildet $(1, i)$ eine Basis.

2.62. FOLGERUNG (aus Satz 2.55). *Es sei M ein unitärer Rechts- R -Modul, $n \in \mathbb{N}$, es sei $A = (a_1, \dots, a_n)$ ein n -Tupel in M und $\Psi_A: R^n \rightarrow M$ die zugehörige Abbildung aus Satz 2.55. Dann gilt*

- (1) $\Psi_A: R^n \rightarrow M$ ist surjektiv $\iff A \in M^n$ erzeugt M ,
- (2) $\Psi_A: R^n \rightarrow M$ ist injektiv $\iff A \in M^n$ ist linear unabhängig,
- (3) $\Psi_A: R^n \rightarrow M$ ist bijektiv $\iff A \in M^n$ ist eine Basis von M .

BEWEIS. Aussage (1) folgt unmittelbar aus Definition 2.57. Zu (2) benutzen wir, dass Ψ_A nach Proposition 2.37 (1) genau dann injektiv ist, wenn $\ker \Psi_A = \{0\} \subset R^n$ gilt, was nach Definition 2.59 äquivalent zur linearen Unabhängigkeit von A ist. Schließlich folgt (3) aus (1) und (2). \square

2.63. DEFINITION. Es sei M ein freier Rechts- R -Modul mit Basis $B = (b_1, \dots, b_n)$, und es sei $m \in M$. Dann heißt die Abbildung Ψ_B aus Satz 2.55 die *Basisabbildung* von M zur Basis B , und ihre Umkehrabbildung die *Koordinatenabbildung* zur Basis B . Für $m \in M$ heißen $r_1, \dots, r_n \in R$ mit

$$\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} = \Psi_B^{-1}(m)$$

die *Koordinaten* von m bezüglich der Basis B .

Äquivalent zu $r = \Psi_B^{-1}(m) \in R^n$ ist somit die Koordinatendarstellung

$$m = \sum_{i=1}^n b_i \cdot r_i.$$

2.64. BEMERKUNG. Wir kommen noch einmal auf Satz 2.55 zurück. Um eine lineare Abbildung F von einem freien Modul M mit Basis $B = (b_1, \dots, b_n)$ in einen beliebigen Modul N anzugeben, können wir die Bilder $F(b_i) = a_i \in N$ der Basiselemente *frei* vorgeben. Sei nämlich $A = (a_1, \dots, a_n)$ das zugehörige n -Tupel und $\Psi_A: R^n \rightarrow N$ die entsprechende lineare Abbildung aus Satz 2.55. Dann ist $f = \Psi_A \circ \Psi_B^{-1}$ linear und bildet jeweils b_i auf a_i ab. Die *universelle Eigenschaft* eines freien Moduls gilt in diesem Sinne also für jeden Modul, der eine endliche Basis besitzt.

2.65. BEMERKUNG. Es sei R Ring mit Eins und M ein Rechts- R -Modul. In Definition 2.32 haben wir den dualen Links- R -Modul $M^* = \text{Hom}_R(M; R)$ eingeführt. Im Spezialfall $M = R^m$ folgt aus Satz 2.55, dass

$$(R^m)^* = \text{Hom}_R(R^m, R) = {}^m R$$

- (1) mit $(a_1, \dots, a_m) \begin{pmatrix} r_1 \\ \vdots \\ r_m \end{pmatrix} = \sum_{i=1}^m a_i \cdot r_i \in R$.

Für $a \in {}^mR$ und $s \in R$ ist die Linkswirkung definiert durch $(s \cdot a)(r) = s \cdot (a(r))$ für alle $r \in R^m$, genau wie in Beispiel 2.52. Somit ist der Links- R -Modul der m -elementigen Zeilen dual zum Rechts- R -Modul der m -elementigen Spalten.

Es sei wieder $(\varepsilon_i)_i$ die Standardbasis des Raumes mR aus Beispiel 2.52. Zwischen den Basen $(e_j)_j$ von R^m und $(\varepsilon_i)_i$ von mR besteht die folgenden Beziehung:

$$(2) \quad \varepsilon_i(e_j) = \sum_{k=1}^m \delta_{ik} \delta_{kj} = \delta_{ij};$$

wir sagen dazu, dass die Basis $(\varepsilon_i)_i$ *dual* zur Basis $(e_j)_j$ ist.

Für Links-Moduln N haben wir analog den Dualraum ${}^*N = {}_R \text{Hom}(N, R)$ definiert. Analog zu oben folgt ${}^*({}^mR) = R^m$, und wiederum ist die Basis $(e_j)_j$ zur Basis $(\varepsilon_i)_i$ dual.

2.66. PROPOSITION. *Es sei R ein Ring mit Eins und M ein freier Modul mit Basis $B = (b_1, \dots, b_m)$. Dann bilden die einzelnen Komponentenfunktionen $\beta_i = \varepsilon_i \circ \beta: M \rightarrow R$ der Koordinatenabbildung $\beta = \Psi_B^{-1}: M \rightarrow R^m$ zu B eine Basis $\beta = (\beta_i)_i$ des dualen Moduls B^* . Sie ist dual zur Basis B , das heißt, für alle i, j gilt*

$$(1) \quad \beta_i(b_j) = \delta_{ij}.$$

Wir dürfen die Koordinatenabbildung $\beta = \Psi_B^{-1}$ zu einer Basis B also als Basisabbildung des dualen Moduls auffassen.

BEWEIS. Die Abbildungen β_i sind als Komponenten von β wieder linear und somit Elemente des dualen Moduls M^* . Aus $b_j = \Psi_B(e_j)$ und $\beta = \Psi_B^{-1}$ folgt (1), denn

$$\beta_i(b_j) = (\varepsilon_i \circ \beta)(\Psi_B(e_j)) = \varepsilon_i(e_j) = \delta_{ij}$$

nach Bemerkung 2.65 (2).

Für ein beliebiges $\alpha \in M^*$ und $j \in \{1, \dots, m\}$ folgt

$$\alpha(b_j) = \sum_{i=1}^m \alpha(b_i) \cdot \delta_{ij} = \sum_{i=1}^m \alpha(b_i) \cdot \beta_i(b_j) = \left(\sum_{i=1}^m \alpha(b_i) \cdot \beta_i \right) (b_j).$$

Nach Bemerkung 2.64 wird α also dargestellt als Linearkombination

$$\alpha = \sum_{i=1}^m \alpha(b_i) \cdot \beta_i,$$

und die i -te Koordinate von α ist gerade $\alpha(b_i) \in R$. Das Tupel $(\beta_1, \dots, \beta_m)$ erzeugt also M^* . Es ist auch linear unabhängig, denn aus $0 = r_1 \cdot \beta_1 + \dots + r_m \cdot \beta_m$ folgt für jedes j , dass

$$r_j = \sum_{i=1}^m r_i \cdot \delta_{ij} = \left(\sum_{i=1}^m r_i \cdot \beta_i \right) (b_j) = 0. \quad \square$$

2.5. Matrizen

Wir wollen jetzt lineare Abbildungen durch Matrizen beschreiben. Das ist zum Beispiel dann wichtig, wenn man numerische Berechnungen durchführen will (also Berechnungen mit „echten“ Zahlen, nicht abstrakte Überlegungen). Es gibt Bücher, die Matrizen als den Hauptgegenstand der linearen Algebra darstellen. Wir wollen Matrizen eher als nützliche Rechenschemata verstehen. Im Vordergrund des Interesses werden weiterhin lineare Abbildungen stehen.

2.67. DEFINITION. Es sei R ein Ring und $m, n \in \mathbb{N}$. Eine $m \times n$ -Matrix über R ist eine Familie $F = (f_{ij})_{i=1\dots m, j=1\dots n}$ in R , geschrieben

$$(1) \quad F = \begin{pmatrix} f_{11} & \cdots & f_{1n} \\ \vdots & & \vdots \\ f_{m1} & \cdots & f_{mn} \end{pmatrix}.$$

Die Menge aller $m \times n$ -Matrizen über R wird mit $M_{m,n}(R)$ bezeichnet.

Wir definieren die *Matrixaddition* $+: M_{m,n}(R) \times M_{m,n}(R) \rightarrow M_{m,n}(R)$ durch

$$(2) \quad F + G = (f_{ij} + g_{ij})_{i=1\dots m, j=1\dots n} \in M_{m,n}(R)$$

für alle $G = (g_{ij})_{i=1\dots m, j=1\dots n} \in M_{m,n}(R)$, und die *Matrixmultiplikation* $\cdot: M_{\ell,m}(R) \times M_{m,n}(R) \rightarrow M_{\ell,n}(R)$ mit $\ell \in \mathbb{N}$ durch

$$(3) \quad H \cdot F = \left(\sum_{j=1}^m h_{ij} \cdot f_{jk} \right)_{i=1\dots \ell, k=1\dots n} \in M_{\ell,n}(R)$$

für alle $H = (h_{ij})_{i=1\dots \ell, j=1\dots m} \in M_{\ell,m}(R)$.

Wenn die Größe einer Matrix bekannt ist, schreiben wir $(f_{ij})_{i,j} \in M_{m,n}(R)$ — daraus ergibt sich, dass $1 \leq i \leq m$ und $1 \leq j \leq n$.

Die Matrixaddition erfolgt komponentenweise, genau wie in Beispiel 2.51. 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 so viele Spalten hat wie die zweite Zeilen. Die Matrixmultiplikation lässt sich am besten am folgenden Schema verdeutlichen:

$$\begin{pmatrix} \cdot & \cdots & \cdot \\ \vdots & & \vdots \\ f_{i1} & \cdots & f_{in} \\ \vdots & & \vdots \\ \cdot & \cdots & \cdot \end{pmatrix} \begin{pmatrix} \cdot & \cdots & g_{1k} & \cdots & \cdot \\ \vdots & & \vdots & & \vdots \\ \cdot & \cdots & g_{nk} & \cdots & \cdot \\ \vdots & & \vdots & & \vdots \\ \cdot & \cdots & \cdot & & \cdot \end{pmatrix} = \begin{pmatrix} \cdot & \cdots & \cdot \\ \vdots & & \vdots \\ f_{i1}g_{1k} + \cdots + f_{in}g_{nk} & & \vdots \\ \vdots & & \vdots \\ \cdot & \cdots & \cdot \end{pmatrix}$$

Hierbei steht F links, G oben, und das Produkt $F \cdot G$ unten rechts.

2.68. 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 :

$$(r) + (s) = (r + s) \quad \text{und} \quad (r) \cdot (s) = (r \cdot s) .$$

- (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 2.51. Wir können von rechts mit einer 1×1 -Matrix aus (2) multiplizieren und erhalten die skalare Multiplikation aus Beispiel 2.51 (2), denn

$$\begin{pmatrix} r_1 \\ \vdots \\ r_m \end{pmatrix} \cdot (s) = \begin{pmatrix} r_1 \cdot s \\ \vdots \\ r_m \cdot s \end{pmatrix} = \begin{pmatrix} r_1 \\ \vdots \\ r_m \end{pmatrix} \cdot s .$$

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 aus Beispiel 2.52. Multiplikation mit einer 1×1 -Matrix von links entspricht der Multiplikation mit einem Skalar.

Wir kommen jetzt zu allgemeinen Matrizen.

2.69. FOLGERUNG (aus Satz 2.55). *Es sei R ein Ring mit Eins und $m, n \in \mathbb{N}$. Dann existiert eine natürliche Bijektion*

$$(1) \quad \Phi: \text{Hom}_R(R^n, R^m) \rightarrow M_{m,n}(R) .$$

Dabei steht das Bild des Standardbasisvektors e_j von R^n unter $f: R^n \rightarrow R^m$ in der j -ten Spalte der Matrix $(f_{ij})_{i,j} = \Phi(f)$. Matrixmultiplikation $\cdot: M_{m,n}(R) \times R^n \rightarrow R^m$ entspricht dem Anwenden einer linearen Abbildung, genauer

$$(2) \quad f \left(\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} \right) = \Phi(f) \cdot \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} \in R^m .$$

Die Matrixaddition entspricht der Addition linearer Abbildungen, für $f, g \in \text{Hom}_R(R^n, R^m)$ gilt also

$$(3) \quad \Phi(f + g) = \Phi(f) + \Phi(g) .$$

Für $\ell, m, n \in \mathbb{N}$ seien $f: R^m \rightarrow R^\ell$ und $g: R^n \rightarrow R^m$ rechts- R -linear. Dann gilt

$$(4) \quad \Phi(f \circ g) = \Phi(f) \cdot \Phi(g) \in M_{\ell,n}(R) ,$$

die Matrixmultiplikation entspricht also der Verkettung linearer Abbildungen.

BEWEIS. Der Modul R^n ist frei mit der Standardbasis $\{e_1, \dots, e_n\}$, siehe Beispiel 2.51. Nach Satz 2.55 (1) existiert eine bijektive Abbildung

$$\Phi: \text{Hom}_R(R^n, R^m) \longrightarrow (R^m)^n .$$

Wir identifizieren $(R^m)^n$ mit $M_{m,n}(R)$, indem wir das j -te Element des Tupels in die j -te Spalte der Matrix $(f_{ij})_{i,j}$ eintragen, und erhalten (1).

Sei umgekehrt $F = (f_{ij})_{i,j} = \Phi(f) \in M_{m,n}(R)$ gegeben, das heißt, die j -te Spalte von F ist genau $f(e_j)$. Mit Folgerung 2.56 erhalten wir

$$f\left(\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix}\right) = f\left(\sum_{j=1}^n e_j \cdot r_j\right) = \left(\sum_{j=1}^n f_{ij} \cdot r_j\right)_{i=1,\dots,m} = (f_{ij})_{i,j} \cdot \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix}.$$

Die letzte Gleichung ist gerade die Definition 2.67 (3) der Matrixmultiplikation in dem Fall, dass der zweite Faktor $(r_j)_{j=1,\dots,n}$ eine Spalte ist.

Zu (3) seien $F = (f_{ij})_{i,j} = \Phi(f)$, $G = (g_{ij})_{i,j} = \Phi(g) \in M_{m,n}(R)$. Wir bestimmen $\Phi(f+g)$ wie in (1), indem wir die Bilder der Vektoren $e_k \in R^n$ berechnen. Nach Definition von $f+g$ in Proposition 2.29 gilt

$$(f+g)(e_k) = f(e_k) + g(e_k) = \begin{pmatrix} f_{1k} \\ \vdots \\ f_{mk} \end{pmatrix} + \begin{pmatrix} g_{1k} \\ \vdots \\ g_{mk} \end{pmatrix} = \begin{pmatrix} f_{1k} + g_{1k} \\ \vdots \\ f_{mk} + g_{mk} \end{pmatrix} \in R^m,$$

und das ist genau die k -te Spalte der Matrix $F+G = \Phi(f) + \Phi(g)$.

Zu (4) sei $F = (f_{ij})_{i,j} = \Phi(f) \in M_{\ell,m}(R)$ und $G = (g_{jk})_{j,k} = \Phi(g) \in M_{m,n}(R)$. Um die Matrix $\Phi(f \circ g)$ zu erhalten, müssen wir wegen (1) die Bilder der Vektoren $e_k \in R^n$ bestimmen. Nach (1) ist $g(e_k)$ die k -te Spalte von G . Nach (2) gilt

$$f(g(e_k)) = \left(\sum_{j=1}^m f_{ij} \cdot g_{jk}\right)_{i=1,\dots,\ell} = \begin{pmatrix} f_{11} \cdot g_{1k} + \cdots + f_{1m} \cdot g_{mk} \\ \vdots \\ f_{\ell 1} \cdot g_{1k} + \cdots + f_{\ell m} \cdot g_{mk} \end{pmatrix} \in R^\ell,$$

Also hat $\Phi(f \circ g)$ die gleiche k -te Spalte wie das Matrixprodukt $\Phi(f) \cdot \Phi(g)$. Daraus folgt unsere Behauptung. \square

2.70. BEMERKUNG. Nach Folgerung 2.69 bietet es sich an, Matrizen $F = (f_{ij})_{i,j} \in M_{m,n}(R)$ mit Hilfe von Φ mit den zugehörigen Abbildungen $f: R^n \rightarrow R^m$ zu identifizieren. Somit sei ab sofort

$$\text{Hom}_R(R^n, R^m) = M_{m,n}(R).$$

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“. Homogenität (L2) folgt jetzt aus dem Assoziativgesetz (R1) der Multiplikation, siehe auch Beispiel 2.26 (3) und Folgerung 2.31 (3).

Bei Zeilen ist es genau spiegelbildlich: hier wirken Skalare von links wegen Bemerkung 2.68 (4) und Matrizen von rechts, es folgt also

$${}_R\text{Hom}({}^mR, {}^nR) = M_{m,n}(R).$$

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.

2.71. FOLGERUNG. *Die Matrixmultiplikation ist assoziativ.*

BEWEIS. Diese Behauptung könnte man beispielsweise mit Hilfe der Definition 2.67 (3) der Matrixmultiplikation mit etwas Aufwand nachrechnen.

Einfacher ist es, Matrizen $F \in M_{\ell,m}(R) = \text{Hom}_R(R^m, R^\ell)$, $G \in M_{m,n}(R) = \text{Hom}_R(R^n, R^m)$ und $H \in M_{n,p}(R) = \text{Hom}_R(R^p, R^n)$ mit den entsprechenden linearen Abbildungen zu identifizieren. Da die Verkettung von Abbildungen assoziativ ist nach Bemerkung 2.4 (1), folgt aus Folgerung 2.69 (4), dass

$$F \cdot (G \cdot H) = F \circ (G \circ H) = (F \circ G) \circ H = (F \cdot G) \cdot H. \quad \square$$

2.72. 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 $M_n(R)$ bezeichnet. Die quadratische Matrix $E_n = (\delta_{ij})_{i,j} \in M_n(R)$ heißt *Einheitsmatrix*. Eine quadratische Matrix $F \in M_n(R)$ heißt *invertierbar*, wenn es eine Matrix $G \in M_n(R)$ mit $G \cdot F = E_n = F \cdot G$ gibt. In diesem Fall heißt G die zu F *inverse Matrix*; sie wird auch mit F^{-1} bezeichnet. Die Menge aller invertierbaren $n \times n$ -Matrizen heißt *allgemeine lineare Gruppe* und wird mit $GL(n, R)$ bezeichnet.

Wir übersetzen jetzt Folgerung 2.31 in die Matrizensprache.

2.73. FOLGERUNG (aus Folgerungen 2.31 und 2.69). *Es sei R ein Ring mit Eins und $m, n \geq 1$.*

- (1) *Die allgemeine lineare Gruppe $(GL(n, R), \cdot)$ ist eine Gruppe, und es gilt $GL(n, R) \cong \text{Aut}_R R^n$.*
- (2) *Die quadratischen $n \times n$ -Matrizen bilden einen Ring $(M_n(R), +, \cdot)$ mit Eins E_n , den Matrixring, und es gilt $M_n(R) \cong \text{End}_R R^n$.*
- (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 Folgerung 2.31 (1) und (2) bilden die Endomorphismen von R^n einen Ring $(\text{End}_R(R^n), +, \circ)$ und die Automorphismen eine Gruppe $(\text{Aut}_R(R^n), \circ)$. Folgerung 2.69 liefert einen Ringisomorphismus

$$\Phi: (\text{End}_R(R^n), +, \circ) \xrightarrow{\cong} (M_n(R), +, \cdot).$$

Die Einheitsmatrix entspricht id_{R^n} , denn für alle $m = (r_j)_j \in R^n$ gilt

$$E_n \cdot m = \left(\sum_{j=1}^n \delta_{ij} r_j \right)_i = (r_i)_i = m.$$

Sie ist die Eins in $M_n(R)$ und das neutrale Element in $GL(n, R)$, es folgt (2).

Wegen Folgerung 2.69 (4) ist F genau dann als lineare Abbildung umkehrbar, also ein Automorphismus, wenn F als Matrix invertierbar ist. In diesem Fall wird die Umkehrabbildung von F genau durch die inverse Matrix F^{-1} beschrieben. Einschränken von Φ liefert zu (2) den Gruppenisomorphismus

$$\Phi: (\text{Aut}_R(R^n), \circ) \xrightarrow{\cong} (GL(n, R), \cdot).$$

Die Punkte (3) und (4) folgen aus den entsprechenden Punkten in Folgerung 2.31 und Folgerung 2.69 (2) und (4). \square

Wir merken uns:

- (1) Die Einheitsmatrix E_n entspricht der Identität des R^n .
- (2) Inverse Matrizen entsprechen Umkehrabbildungen. Aus Proposition 2.3 folgt, dass die inverse Matrix eindeutig bestimmt ist.

Wir haben in Definition 2.72 zur Invertierbarkeit von F verlangt, dass sowohl $F \cdot G = E_n$ als auch $G \cdot F = E_n$ gilt. In einer Gruppe reicht es, wenn F ein Linksinverses besitzt, also $G \cdot F = E_n$ für ein G gilt. Aber G muss selbst invertierbar sein, um zu $GL(n, R)$ zu gehören, also kommen wir um die Forderung $F \cdot G = E_n$ nicht herum. Erst, wenn wir später mit quadratischen Matrizen über (Schief-) Körpern arbeiten, wird es reichen, nur $G \cdot F = E_n$ zu verlangen.

Zum Schluss dieses Abschnitts wollen wir auch in freien Moduln mit festen Basen mit Koordinaten und Matrizen rechnen.

2.74. BEMERKUNG. Es sei M ein freier Rechts- R -Modul mit Basis $B = (b_1, \dots, b_m)$. Für die Basisabbildung $\Psi_B: R^m \rightarrow M$ aus Definition 2.63 schreiben wir kurz

$$\Psi_B \left(\begin{pmatrix} r_1 \\ \vdots \\ r_m \end{pmatrix} \right) = B \begin{pmatrix} r_1 \\ \vdots \\ r_m \end{pmatrix} = \sum_{i=1}^m b_i \cdot r_i \in M.$$

Wir benutzen hier den gleichen Buchstaben für die Basisabbildung wie für die Basis, und tatsächlich verhält sich die Basisabbildung oben formal wie die Matrixmultiplikation der „Zeile“ B aus Modulelementen mit der Spalte $(r_i)_i \in R^m$.

Nach Folgerung 2.62 ist die Basisabbildung invertierbar. Ihre Umkehrabbildung nennen wir die Koordinatenabbildung $\beta = \Psi_B^{-1}$ und schreiben der Einfachheit halber

$$\begin{pmatrix} r_1 \\ \vdots \\ r_m \end{pmatrix} = \beta(v) = {}_B v \in R^m.$$

Beide Abbildungen sind linear nach Proposition 2.29. Das 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.

2.75. FOLGERUNG. Es sei R ein Ring mit Eins, es sei M ein freier Rechts- R -Modul mit Basis $B = (b_1, \dots, b_m)$ und N ein freier Rechts- R -Modul mit Basis $C = (c_1, \dots, c_n)$. Dann entspricht jeder linearen Abbildung $f: N \rightarrow M$ genau eine Matrix $A = {}_B f_C \in M_{m,n}(R)$, die Abbildungsmatrix oder darstellende Matrix von f bezüglich B und C , so dass das folgende Diagramm kommutiert.

$$(1) \quad \begin{array}{ccc} N & \xrightarrow{f} & M \\ C \uparrow & & \uparrow B \\ R^n & \xrightarrow{A = {}_B f_C} & R^m \end{array}$$

Dabei stehen in der j -ten Spalte von A die B -Koordinaten ${}_B(f(c_j))$ 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 $A \cdot (r_i)_i$, somit

$$(2) \quad {}_B(f(v)) = {}_B f_C \cdot C v .$$

Wir können uns das anhand des kommutativen Diagramms (1) oder der Formel (2) merken. Sei jetzt P ein weiterer R -Modul mit Basis D und $G: P \rightarrow N$ linear, dann gilt völlig analog

$${}_B(f \circ g)_D = {}_B f_C \cdot C g_D .$$

Wichtig ist hier wie in (2), dass wir auf beiden Seiten der Matrixmultiplikation die gleiche Basis von N verwenden.

BEWEIS. Wir bezeichnen die Umkehrabbildung der Basisabbildung B mit β und setzen

$$A = \beta \circ f \circ C ,$$

dann kommutiert das Diagramm offensichtlich. Die restlichen Aussagen ergeben sich aus Folgerung 2.69. \square

2.76. BEMERKUNG. Der Spezialfall $M = N$ und $f = \text{id}_M$ ist interessant. In diesem Fall erhalten wir das kommutative Diagramm

$$\begin{array}{ccc} & M & \\ C \nearrow & & \nwarrow B \\ R^n & \xrightarrow{A = {}_B \text{id}_C} & R^n . \end{array}$$

Multiplikation mit der Matrix A macht aus C -Koordinaten B -Koordinaten. Also besteht die j -te Spalte von $A = (f_{ij})_{i,j}$ aus den B -Koordinaten des Vektor c_j , das heißt

$$c_j = \sum_{i=1}^n b_i \cdot f_{ij} .$$

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“ $C = B \cdot A$. 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. Sei R Ring mit Eins, sei M ein R -Modul und $m \in \mathbb{N}$.

- (1) Es besteht eine Bijektion zwischen der Menge der angeordneten Basen (b_1, \dots, b_m) von M und den R -Modulisomorphismen $R^m \rightarrow M$.
- (2) Sei M frei mit Basis $B = (b_1, \dots, b_m)$. Dann besteht eine Bijektion zwischen der Menge der m -elementigen Basen von M und der allgemeinen linearen Gruppe $GL(m, R)$, die jeder Basis $C = (c_1, \dots, c_m)$ die Basiswechselmatrix A zuordnet.

Wenn M keine Basis der Länge m besitzt, sind insbesondere beide Mengen in (1) leer.

BEWEIS. Nach Satz 2.55 gibt es eine Bijektion $\Psi: M^m \cong \text{Hom}_R(R^m, M)$, und nach Folgerung 2.62 (3) ist $B = (b_1, \dots, b_m)$ genau dann eine Basis, wenn $\Psi_B: R^m \rightarrow M$ ein Isomorphismus ist. Es folgt (1).

Zu (2) sei $\beta: M \rightarrow R^m$ die Koordinatenabbildung zu B , und $C = (c_j)_j$ sei eine weitere Basis von M . Dann erhalten wir eine Basiswechselmatrix $A = \beta \circ C$ wie in Bemerkung 2.76. Da β und C Isomorphismen sind, ist A invertierbar nach Folgerung 2.73 (1).

Sei umgekehrt A eine invertierbare Matrix, dann ist $C = B \circ A: R^m \rightarrow M$ ein Isomorphismus, und $(c_1, \dots, c_m) = \Phi(C)$ eine Basis nach (1). Die zugehörige Basiswechselmatrix ist $\beta \circ (B \circ A) = A$. \square

2.78. BEMERKUNG. Wir können jetzt auch überlegen, wie sich die Abbildungsmatrix aus Folgerung 2.75 verhält, wenn wir eine der beiden Basen durch eine andere ersetzen. Wir betrachten dazu die kommutativen Diagramme

$$\begin{array}{ccc}
 & N & \xrightarrow{f} & M \\
 & \nearrow C & & \nearrow B \\
 R^n & \xrightarrow{A=BfC} & R^m & \xrightarrow{D \text{ id}_B} & R^m \\
 & & & & \searrow D
 \end{array}
 \quad \text{und} \quad
 \begin{array}{ccc}
 & N & \xrightarrow{f} & M \\
 & \nearrow E & & \nearrow C \\
 R^n & \xrightarrow{C \text{ id}_E} & R^n & \xrightarrow{A=BfC} & R^m \\
 & & & & \searrow B
 \end{array}$$

Hier ist D eine neue Basis von M und $D \text{ id}_B \in GL(m, R)$ die zugehörige Basiswechselmatrix, und E ist eine Basis von N und $C \text{ id}_E \in GL(n, R)$ die zugehörige Basiswechselmatrix. Es folgt

$$DfC = D \text{ id}_B \cdot BfC \quad \text{und} \quad BfE = BfC \cdot C \text{ id}_E .$$

Auch hier ist wieder wichtig, dass links und rechts vom Matrixmultiplikationszeichen „ \cdot “ die gleiche Basis benutzt wird.

2.6. Unendliche Indexmengen

In den Abschnitten 2.4, 2.5 haben wir uns nur mit endlich erzeugten freien Moduln beschäftigt. Einige, aber nicht alle Resultate gelten analog für freie Moduln zu unendlichen Mengen I . Wichtig ist dabei aber, dass wir immer nur

endliche Linearkombinationen bilden, denn mehr gibt die Konstruktion in (2.1) nicht her. Für unendliche Summen bräuchten wir Methoden aus der Analysis.

2.79. DEFINITION. Es sei R ein Ring mit Eins und I eine beliebige Menge. Der *freie Modul zur Indexmenge I* ist definiert als

$$R^{(I)} = \{ (r_i)_{i \in I} \mid \text{die Menge } \{ i \in I \mid r_i \neq 0 \} \text{ ist endlich} \} \subset R^I .$$

Man überzeugt sich leicht, dass $R^{(I)}$ ein Untermodul des Moduls R^I aus Bemerkung 2.50, also insbesondere selbst ein Rechts- R -Modul ist. Elemente von R^I heißen auch Familien in R mit Indexmenge I . Elemente von $R^{(I)}$ nennt man entsprechend *endliche Familien*. Die Notation $R^{(I)}$ ist nicht Standard.

Es sei $j \in I$, dann sei $e_j = (\delta_{ij})_{i \in I} \in R^{(I)}$ die Familie, deren einziger nichtverschwindender Eintrag eine Eins an der Stelle j ist. Wir nennen $(e_i)_{i \in I}$ die *Standardbasis* von $R^{(I)}$. Eine lineare Abbildung $f: R^{(I)} \rightarrow M$ bildet eine endliche Familie $(r_i)_{i \in I}$ auf die endliche Linearkombination

$$f((r_i)_{i \in I}) = \sum_{i \in I} f(e_i) \cdot r_i$$

ab. Das sind alle Linearkombinationen der $f(e_i) \in M$, die wir mit unseren Mitteln bilden können. Zur Berechnung der rechten Seite wählen wir zunächst eine endliche Teilmenge $J \subset I$, so dass $r_i = 0$ falls $i \notin J$. Dann suchen wir gemäß der Definitionen 1.26 und 1.31 eine Bijektion $\alpha: \underline{n} \rightarrow J$ für $n = \#J$ und setzen

$$\sum_{i \in I} a_i \cdot r_i = \sum_{k=0}^{n-1} a_{\alpha(k)} \cdot r_{\alpha(k)} ,$$

das ist jetzt eine endliche Summe wie in (2.1). Wenn wir J vergrößern, kommen nur Summanden der Form $a_j \cdot 0 = 0$ hinzu. Und wenn wir die Abbildung α abändern, vertauschen wir die Reihenfolge der Summation, was wegen der Kommutativität der Addition in M aber keine Rolle spielt. Also ist der Wert der Summe unabhängig von den Wahlen von J und α .

2.80. BEISPIEL. Es sei R ein kommutativer Ring mit Eins. Ein *Polynom* über R in der Variablen X ist ein Ausdruck der Form

$$P(X) = \sum_{i=0}^n a_i X^i \quad \text{für ein } n \in \mathbb{N} \text{ und } a_0, \dots, a_n \in R .$$

Der Raum aller Polynome wird mit $R[X]$ bezeichnet. Als R -Modul gilt $R[X] \cong R^{(\mathbb{N})}$. Wir dürfen $r \in R$ in P einsetzen und erhalten eine lineare Abbildung

$$R[X] \longrightarrow R \quad \text{mit} \quad P(X) \longmapsto P(r) = \sum_{i=0}^n a_i \cdot r^i .$$

In Analogie dazu entspricht $R^{\mathbb{N}}$ dem Raum $R[[X]]$ der *formalen Potenzreihen* in X über dem Ring R . Wir dürfen mit formalen Potenzreihen zwar wie in jedem Modul rechnen, aber wir dürfen keine Elemente von R mehr einsetzen, da wir keine unendlichen Summen ausrechnen können. In der Analysis lernen

Sie den Raum der „konvergenten Potenzreihen“ über \mathbb{R} oder \mathbb{C} kennen, in die man zumindest hinreichend kleine Zahlen einsetzen darf.

In Analogie zu Satz 2.55 gilt folgendes Resultat.

2.81. SATZ (Universelle Eigenschaft des freien Moduls). *Es sei R ein Ring mit Eins, I eine Menge, und M ein Rechts- R -Modul. Dann gibt es eine Bijektion*

$$\Phi: \text{Hom}_R(R^{(I)}, M) \xrightarrow{\cong} M^I \quad \text{mit} \quad f \longmapsto (f(e_i))_{i \in I}. \quad \square$$

Als Diagramm:

$$\begin{array}{ccc} I & \xrightarrow{e \cdot} & R^{(I)} \\ & \searrow A & \downarrow \exists! \Psi_A \\ & & M. \end{array}$$

BEWEIS. Für $A = (a_i)_{i \in I} \in M^I$ und $(r_i)_{i \in I} \in R^{(I)}$ setzen wir

$$\Psi_A((r_i)_{i \in I}) = \sum_{i \in I} a_i \cdot r_i \in M$$

wie in Satz 2.55 (2). Dann ist Ψ_A wieder eine lineare Abbildung, und es folgt

$$\Phi(\Psi_A) = (\Psi_A(e_i))_{i \in I} = \left(\sum_{j \in I} a_j \cdot \delta_{ji} \right)_{i \in I} = (a_i)_{i \in I} = A.$$

Umgekehrt sei $f: R^{(I)} \rightarrow M$ rechts- R -linear und $A = \Phi(f) = (f(e_i))_{i \in I}$, dann folgt

$$\Psi_A((r_i)_{i \in I}) = \sum_{i \in I} f(e_i) \cdot r_i = f\left(\sum_{i \in I} e_i \cdot r_i\right) = f((r_i)_{i \in I}). \quad \square$$

In Analogie zu den Definitionen 2.57 und 2.59 definieren wir das *Erzeugnis* $\langle A \rangle \subset M$ einer Familie A in M als $\text{im}(\Psi_A) \subset M$. Wir nennen A *linear unabhängig*, wenn $\ker(\Psi_A) = \{0\}$. Eine Basis ist wieder ein linear unabhängiges Erzeugendensystem von M . Dann gelten Folgerung 2.62 und Bemerkung 2.64 analog. Insbesondere dürfen wir einen Modul mit Basis $A \in M^I$ nach wie vor *frei* nennen.

2.82. BEMERKUNG. Anstelle von Bemerkung 2.65 gilt $(R^{(I)})^* \cong {}^I R$, dabei steht ${}^I R$ für den R -Linksmodul auf der Menge $\text{Abb}(I, R)$. Sei $(a_i)_{i \in I} \in {}^I R$ eine beliebige und $(r_i)_{i \in I} \in R^{(I)}$ eine endliche Familie, dann erhalten wir eine endliche Summe

$$\Psi_{(a_i)_{i \in I}}((r_i)_{i \in I}) = \sum_{i \in I} a_i \cdot r_i \in R,$$

und aus Satz 2.81 folgt, dass jedes Element von $(R^{(I)})^*$ von dieser Form ist.

Proposition 2.66 gilt daher für unendliche Indexmengen im Allgemeinen nicht mehr. Sei etwa $B \in M^I$ eine Basis und $\beta: M \rightarrow R^{(I)}$ die zugehörige

Koordinatenabbildung. Dann erzeugen die Komponentenfunktionen $(\beta_i)_{i \in I} \in M^*$ den dualen Modul im Allgemeinen nicht. Dazu betrachte

$$\alpha = \sum_{j \in I} \beta_j \quad \text{mit} \quad \alpha \left(\sum_{i \in I} b_i \cdot r_i \right) = \sum_{i, j \in I} \underbrace{\beta_j(b_i)}_{=\delta_{ij}} \cdot r_i = \sum_{j \in I} r_j \in R.$$

Jede endliche Linearkombination der β_j würde auf einem b_i verschwinden, im Gegensatz zu α , somit $\alpha \notin \langle (\beta_j)_{j \in I} \rangle$.

Wir können später beispielsweise zeigen, dass $\mathbb{R}[X] \cong \mathbb{R}^{(\mathbb{N})}$ eine abzählbare Basis besitzt, $R[[X]] \cong \mathbb{R}^{\mathbb{N}}$ jedoch nicht.

2.7. Zusammenfassung

Es folgt eine kurze Zwischenbilanz zum Ende des Abschnitts: In den Abschnitten 2.1 und 2.2 haben wir die Grundbegriffe kennengelernt: Gruppen, Ringe, (Schief-) Körper, Moduln beziehungsweise Vektorräume und lineare Abbildungen. Hier ging es vor allem um den Umgang mit Axiomen und Folgerungen daraus. Zunächst sind wir dabei in der Reihenfolge der Abschnitte 1.3 und 1.4 vorgegangen, später (über Ringen mit Eins) dann umgekehrt:

	abstrakt	konkret
Modul	M	R^n
Ring mit Eins	$\text{End}_R(M)$	$M_n(R)$
Gruppe	$\text{Aut}_R(M)$	$GL(n, R)$

Thema von Abschnitt 2.3 waren Unterräume, Quotienten und (direkte) Summen. Diese Konstruktionen schauen wir uns näher an, sobald wir mehr über Basen von Vektorräumen wissen. Wichtig sind hier ein Kriterium für Injektivität, die universelle Eigenschaft des Quotienten, und als Konsequenz der Homomorphiesatz 2.43.

In Abschnitt 2.4 haben wir Linearkombinationen, Erzeugendensysteme, lineare Unabhängigkeit und Basen betrachtet. Die universelle Eigenschaft 2.55 freier Moduln hat uns dann im Abschnitt 2.5 erlaubt, lineare Abbildungen zwischen freien Moduln als Matrizen zu schreiben. Matrizen ermöglichen zum einen konkrete Rechnungen mit linearen Abbildungen. Zum anderen verstehen wir mit ihrer Hilfe den Raum aller linearen Abbildungen besser. Die Existenz von Basen ist hierfür essentiell — im nächsten Kapitel lernen wir als erstes, dass endlich erzeugt Vektorräume stets Basen besitzen.

Abschnitt 2.6 gibt einen Ausblick auf unendlich erzeugte Moduln und Vektorräume. Er wird im Folgenden keine große Rolle mehr spielen.

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 Gleichungssysteme treten sowohl in der Praxis als auch in der Theorie häufig auf. Wir können 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 \mathbb{k} ein Schiefkörper, also zum Beispiel \mathbb{Q} , \mathbb{R} , \mathbb{C} , \mathbb{H} oder $\mathbb{Z}/p\mathbb{Z}$ für p prim. Wenn nichts anderes angegeben wird, seien alle \mathbb{k} -Vektorräume nach wie vor Rechts-Vektorräume, und alle Basen seien Tupel von Vektoren wie in Definition 2.59.

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.

Wir erinnern uns an das Erzeugnis $\langle \dots \rangle$ eines Tupels von Vektoren aus Definition 2.57 und an lineare Unabhängigkeit aus Definition 2.59. Wir arbeiten mit Rechts- \mathbb{k} -Vektorräumen, aber analoge Aussagen gelten auch für Links- \mathbb{k} -Vektorräume.

3.1. LEMMA. *Es sei V ein \mathbb{k} -Vektorraum, (v_1, \dots, v_n) ein linear unabhängiges Tupel von Vektoren aus V und $w \in V$. Es gilt $w \in \langle (v_1, \dots, v_n) \rangle$ genau dann, wenn das $(n+1)$ -Tupel (v_1, \dots, v_n, w) linear abhängig ist.*

BEWEIS. Zu „ \implies “ gelte $w \in \langle (v_1, \dots, v_n) \rangle$. Nach Definition 2.57 existieren $a_1, \dots, a_n \in \mathbb{k}$, so dass

$$w = \sum_{i=1}^n v_i \cdot a_i .$$

Nach Definition 2.59 ist (v_1, \dots, v_n, w) linear abhängig, da

$$0 = \sum_{i=1}^n v_i \cdot a_i + w \cdot \underbrace{(-1)}_{\neq 0}.$$

Zu „ \Leftarrow “ sei (v_1, \dots, v_n, w) linear abhängig. Nach Definition 2.59 existieren $a_1, \dots, a_n, b \in \mathbb{k}$, die nicht alle 0 sind, so dass

$$0 = \sum_{i=1}^n v_i \cdot a_i + w \cdot b.$$

Es folgt $b \neq 0$. Denn andernfalls wäre ein $a_i \neq 0$, und wir hätten

$$0 = \sum_{i=1}^n v_i \cdot a_i$$

im Widerspruch zur linearen Unabhängigkeit von (v_1, \dots, v_n) . Es folgt

$$w = \sum_{i=1}^n v_i \cdot (-a_i b^{-1}) \in \langle (v_1, \dots, v_n) \rangle. \quad \square$$

3.2. BEMERKUNG. Wir haben im Beweis dividiert und 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) ist linear unabhängig, aber $(2, 3)$ ist linear abhängig, da $2 \cdot 3 - 3 \cdot 2 = 0$. Dennoch ist 3 kein ganzzahliges Vielfaches von 2, also $2 \notin \langle (3) \rangle$. Die Voraussetzung, dass \mathbb{k} ein (Schiefe-) 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 \mathbb{k} -Vektorraum. Es sei (v_1, \dots, v_r) ein Tupel linear unabhängiger Vektoren, und $\{w_1, \dots, w_s\} \subset V$ sei ein endliches Erzeugendensystem. Dann gibt es $n \geq r$ und Zahlen $i(r+1), \dots, i(n) \in \{1, \dots, s\}$, so dass das Tupel*

$$(1) \quad (v_1, \dots, v_r, w_{i(r+1)}, \dots, w_{i(n)})$$

eine Basis von V bildet.

BEWEIS. Wir beginnen mit $n = r$ und dem n -Tupel $B_0 = (v_1, \dots, v_r)$. Wir setzen der Reihe nach $j = 1, \dots, s$, und nehmen an, dass $w_i \in \langle B_{j-1} \rangle$ für alle $i \leq j - 1$ gilt. Im Fall $j = 1$ ist das trivialerweise wahr.

Wenn $w_i \in \langle (v_1, \dots, v_r) \rangle$ gilt, setzen wir $B_j = B_{j-1}$. Es gilt $w_i \in \langle B_j \rangle$ für alle $i \leq j$, und wir machen mit dem nächsten j weiter.

Andernfalls hängen wir w_j an das Tupel B_{j-1} an, erhöhen n um 1, und nennen dann das neue n -Tupel B_j . Nach Lemma 3.1 ist B_j linear unabhängig. Außerdem gilt wieder $w_i \in \langle B_j \rangle$ für alle $i \leq j$. Wir merken uns, dass wir w_j angehängt haben, indem wir $i(n) = j$ setzen.

Nach s Schritten haben wir ein linear unabhängiges n -Tupel B_s der Form (1) konstruiert. Da $\langle B_s \rangle$ jeden der Erzeuger w_j enthält, folgt $\langle B_s \rangle = V$, also ist B_s eine Basis. \square

Endlich erzeugte Vektorräume V haben also immer Basen. Als nächstes wollen wir zeigen, dass alle Basen von V gleich viele Elemente haben.

3.4. SATZ (Basisaustauschsatz von Steinitz). *Es sei V ein \mathbb{k} -Vektorraum, es sei (v_1, \dots, v_r) ein linear unabhängiges Tupel, und (w_1, \dots, w_s) sei ein Erzeugendensystem. Dann gilt $r \leq s$.*

Der Name des Satzes ergibt sich aus dem „Austauschschritt“ im folgenden Beweis.

BEWEIS. Wir werden das Tupel (v_1, \dots, v_r) in mehreren Schritten zu einer Basis aus Einträgen des Tupels (w_1, \dots, w_s) umbauen. Dabei wird unser Tupel in keinem Schritt kürzer. Da das resultierende Tupel insbesondere linear unabhängig ist, kann es keinen Eintrag doppelt enthalten, also folgt die Behauptung.

Im ersten Schritt ergänzen wir (v_1, \dots, v_r) gemäß des Basisergänzungssatzes 3.3 mit Einträgen des Tupels (w_1, \dots, w_s) zu einer Basis B_0 . Dann hat B_0 mindestens r Einträge.

Wir setzen der Reihe nach $i = 1, \dots, r$ und starten mit einer Basis B_{i-1} , die mit v_i, \dots, v_r anfängt. Wir entfernen v_i und erhalten ein linear unabhängiges Tupel B'_i . Da B_{i-1} linear unabhängig ist, folgt $v_i \notin \langle B'_i \rangle$ aus Lemma 3.1, insbesondere ist B'_i kein Erzeugendensystem mehr. Also müssen wir mindestens einen Eintrag aus dem Tupel (w_1, \dots, w_s) hinzufügen, um mit Satz 3.3 eine neue Basis B_i zu bekommen. Sie ist somit nicht kürzer als B_{i-1} .

Am Ende besteht B_r aus mindestens r verschiedenen Einträgen des Tupels (w_1, \dots, w_s) . Es folgt $r \leq s$. \square

3.5. FOLGERUNG. *Es sei V ein endlich erzeugter \mathbb{k} -Vektorraum.*

- (1) *Dann existiert $n \in \mathbb{N}$ und eine Basis $B = (v_1, \dots, v_n)$ von V .*
- (2) *Jede andere Basis von V hat ebenfalls n Elemente.*
- (3) *Jedes n -elementige Tupel linear unabhängiger Vektoren in V ist eine Basis von V .*
- (4) *Jedes n -elementige Erzeugendensystem von V ist eine Basis von V .*

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, also gilt (1).

Zu (2) sei C eine beliebige Basis von V , möglicherweise sogar mit unendlicher Indexmenge I . 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 nur endlich viele Vektoren der Familie C benötigen, nämlich nur die, die in einer der Darstellungen der w_i mit Koeffizient $\neq 0$

vorkommen. Es sei I_0 die entsprechende endliche Teilmenge der Indexmenge I von C und $C_0: I_0 \rightarrow V$ die zugehörige Teilfamilie. Alle anderen Vektoren c_i mit $i \in I \setminus I_0$ 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.

Zu (3) sei (w_1, \dots, w_n) linear unabhängig, dann können wir mit Satz 3.3 zu einer Basis von V ergänzen, die nach (2) wieder Länge n hätte. Also ist (w_1, \dots, w_n) bereits eine Basis.

Zu (4) sei analog (w_1, \dots, w_n) ein Erzeugendensystem. Eine Teilmenge davon bildet nach Satz 3.3 eine Basis, die aber wieder Länge n hätte. Also ist (w_1, \dots, w_n) bereits eine Basis. \square

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*.

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 \mathbb{k} -Vektorraum. Wenn V endlich erzeugt ist, 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, und wir schreiben dafür auch „ $\dim V < \infty$ “. Wie in Bemerkung 1.32 (3) führen wir die Schreibweise „ $\dim V = \infty$ “ nicht ein, da nicht alle unendlichen Basen die gleiche Mächtigkeit haben.

3.8. FOLGERUNG. *Zwei endlichdimensionale \mathbb{k} -Vektorräume V und W sind genau dann isomorph, wenn $\dim V = \dim W$.*

Man sagt auch, endlichdimensionale \mathbb{k} -Vektorräume werden durch ihre Dimension *klassifiziert*. Analog werden endliche Mengen durch ihre Mächtigkeit klassifiziert, siehe Definitionen 1.26 und 1.31.

BEWEIS. Zu „ \implies “ sei $F: V \rightarrow W$ 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 $B = F \circ C: \mathbb{k}^n \rightarrow W$ ein Isomorphismus, und das Diagramm

$$\begin{array}{ccc} V & \xrightarrow{F} & W \\ C \uparrow & & \uparrow B \\ \mathbb{k}^n & \xrightarrow[\text{E}_n]{\text{id}_{\mathbb{k}^n}} & \mathbb{k}^n \end{array}$$

kommutiert. Wegen Proposition 2.77 (1) bilden $b_1 = B(e_1), \dots, b_n = B(e_n)$ eine Basis von W , so dass insbesondere $\dim W = n = \dim V$.

Zu „ \Leftarrow “ sei $n = \dim V = \dim W$. Wir wählen Basen von V und W mit Basisabbildungen $B: \mathbb{k}^n \rightarrow W$ und $C: \mathbb{k}^n \rightarrow V$. Nach Folgerung 2.62 (3) sind Basisabbildungen Isomorphismen. Wir erhalten also einen Isomorphismus $F = B \circ C^{-1}: V \rightarrow W$, so dass das obige Diagramm wieder kommutiert. \square

Wir erinnern uns an die Begriffe „direkte Summe“ und „komplementärer Unterraum“ aus Definition 2.45.

3.9. PROPOSITION. *Sei V ein endlichdimensionaler \mathbb{k} -Vektorraum 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. Jedes linear unabhängige Tupel von Vektoren in U ist in V ebenfalls linear unabhängig. Nach dem Basisaustauschsatz 3.4 kann solch ein Tupel also höchstens $\dim V$ viele Elemente haben, insbesondere ist es endlich. Aus den Übungen wissen wir auch, dass ein maximal linear unabhängiges Tupel in U eine Basis von U bildet. Also finden wir eine Basis $B = (v_1, \dots, v_r)$ der Länge $r = \dim U \leq n = \dim V$ von U . 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 $k_1, \dots, k_r \in \mathbb{k}$ und $\ell_{r+1}, \dots, \ell_n \in \mathbb{k}$ 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, \dots, v_n) . Nach Folgerung 2.62 (2) sind die Koordinaten von v eindeutig, also gilt $k_1 = \dots = k_r = 0 = \ell_{r+1} = \dots = \ell_n$. Insbesondere folgt $U \cap W = \{0\}$, also $V = U \oplus W$. \square

3.10. FOLGERUNG. *Es seien U und W zwei Unterräume eines endlichdimensionalen \mathbb{k} -Vektorraums V . Dann sind äquivalent*

- (1) $V = U \oplus W$,
- (2) $V = U + W$ und $\dim U + \dim W \leq \dim V$,
- (3) $U \cap W = \{0\}$ und $\dim U + \dim W \geq \dim V$.

BEWEIS. Die Richtungen „(1) \implies (2)“ und „(1) \implies (3)“ folgen sofort aus der Definition 2.45 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). \square

3.11. FOLGERUNG. *Es sei V ein \mathbb{k} -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 2.47 und 3.9 folgt

$$\dim(V/U) = \dim W = \dim V - \dim U. \quad \square$$

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 $e_j = (\delta_{ij})_{i \in \mathbb{N}}$. Wir betrachten zwei unendlichdimensionale Unterräume

$$U = \langle e_r, e_{r+1}, e_{r+2}, \dots \rangle \quad \text{und} \quad W = \langle e_0, e_2, e_4, \dots \rangle.$$

Beide sind als Vektorräume isomorph, denn wir können einen Isomorphismus $F: U \rightarrow W$ 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 2.47 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 $A \in M_{p,r}(\mathbb{k})$, $B \in M_{p,s}(\mathbb{k})$, $C \in M_{q,r}(\mathbb{k})$ und $D \in M_{q,s}(\mathbb{k})$, dann ist

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} a_{11} & \dots & a_{1r} & b_{11} & \dots & b_{1s} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{p1} & \dots & a_{pr} & b_{p1} & \dots & b_{ps} \\ c_{11} & \dots & c_{1r} & d_{11} & \dots & d_{1s} \\ \vdots & & \vdots & \vdots & & \vdots \\ c_{q1} & \dots & c_{qr} & d_{q1} & \dots & d_{qs} \end{pmatrix} \in M_{p+q,r+s}(\mathbb{k}).$$

3.13. SATZ (Rangsatz). *Es seien V und W endlich-dimensionale \mathbb{k} -Vektorräume, und es sei $F: V \rightarrow W$ 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 $r = n - \dim \ker F$. Wie im Beweis von Proposition 3.9 wählen wir 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 Proposition 2.47 (3) und dem Homomorphiesatz 2.43 erhalten wir einen Isomorphismus

$$\begin{array}{ccc} U & \xrightarrow{\cong} & V/\ker F & \xrightarrow{\cong} & \operatorname{im} F \\ & & \searrow & \nearrow & \\ & & & & \operatorname{im} F \end{array}$$

$F|_U$

Somit induziert die Basis (c_1, \dots, c_r) von U eine Basis (b_1, \dots, 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, \dots, 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

$$\dim V = \dim \ker F + \dim U = \dim \ker F + \dim \operatorname{im} F. \quad \square$$

3.14. 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 $A^t = (a_{ij})_{ji}$.

Transponieren macht zum Beispiel aus Zeilen Spalten und umgekehrt. In Büchern wird häufig $(r_1, \dots, r_n)^t$ für die Spalte $\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix}$ geschrieben.

3.15. DEFINITION. Es sei $F: V \rightarrow W$ linear, dann definieren wir den *Rang* von F durch $\text{rg } F = \dim \text{im } F$, falls $\text{im } F$ endlichdimensional ist, ansonsten nennen wir F *von unendlichem Rang*.

Es sei $A \in M_{m,n}(\mathbb{k})$ eine Matrix mit den Spalten $a_1, \dots, a_n \in \mathbb{k}^m$ und den Zeilen $\alpha_1, \dots, \alpha_m \in {}^m\mathbb{k}$, dann definieren wir den *Spaltenrang* von A durch $\text{rg}_S A = \dim \langle a_1, \dots, a_n \rangle$. Analog definieren wir den *Zeilenrang* von A durch $\text{rg}_Z A = \dim \langle \alpha_1, \dots, \alpha_m \rangle$.

In der Definition des Zeilenrangs fassen wir das Erzeugnis der Zeilen als Links- \mathbb{k} -Vektorraum auf.

3.16. BEISPIEL. Wir schauen uns Spalten- und Zeilenrang an Beispielen an.

- (1) Die „Telefonmatrix“ $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \in M_3(\mathbb{Q})$ hat Rang 2, denn je zwei Zeilen oder Spalten sind linear unabhängig, aber

$$\begin{pmatrix} 2 \\ 5 \\ 8 \end{pmatrix} 2 - \begin{pmatrix} 1 \\ 4 \\ 7 \end{pmatrix} - \begin{pmatrix} 3 \\ 6 \\ 9 \end{pmatrix} = 0 \quad \text{und} \quad 2(4, 5, 6) - (1, 2, 3) - (7, 8, 9) = 0.$$

- (2) Die Matrix $\begin{pmatrix} 1 & j \\ i & k \end{pmatrix} \in M_2(\mathbb{H})$ hat Rang 1, denn

$$\begin{pmatrix} 1 \\ i \end{pmatrix} \cdot j = \begin{pmatrix} j \\ k \end{pmatrix} \quad \text{und} \quad i \cdot (1, j) = (i, k).$$

- (3) Die Transponierte der obigen Matrix hat Rang 2, denn sie ist invertierbar mit inverser Matrix $\begin{pmatrix} 1 & i \\ j & k \end{pmatrix}^{-1} = \begin{pmatrix} 1/2 & -j/2 \\ -i/2 & -k/2 \end{pmatrix}$.

Manchmal heißt auch die folgende Proposition „Rangatz“.

3.17. PROPOSITION. *Es sei $A \in M_{m,n}(\mathbb{k})$.*

- (1) *Spalten- und Zeilenrang von A ändert sich nicht, wenn man von links oder rechts mit einer invertierbaren Matrix multipliziert.*
- (2) *Es gilt $\text{rg}_S A = \text{rg } A = \text{rg}_Z A$.*
- (3) *Es sei $A = {}_B F_C$ Matrixdarstellung einer linearen Abbildung $F: V \rightarrow W$ bezüglich Basen B von W und C von V , dann gilt $\text{rg } F = \text{rg } A$.*

BEWEIS. Sei A eine Matrix. Wie in Bemerkung 2.70 bezeichne $L_A: \mathbb{k}^n \rightarrow \mathbb{k}^m$ die (rechts- \mathbb{k} -lineare) Multiplikation mit A von Links, und $R_A: {}^m\mathbb{k} \rightarrow {}^m\mathbb{k}$ die (links- \mathbb{k} -lineare) Multiplikation mit A von Rechts, also

$$L_A(v) = A \cdot v \quad \text{und} \quad R_A(\omega) = \omega \cdot A.$$

Es seien wieder $a_1, \dots, a_n \in \mathbb{k}^m$ die Spalten von A . Dann gilt

$$\langle a_1, \dots, a_n \rangle = \langle L_A(e_1), \dots, L_A(e_n) \rangle = \text{im } L_A,$$

also gilt $\operatorname{rg}_S A = \operatorname{rg} L_A$. Für $\operatorname{rg}_Z A$ betrachten wir analog die Basis $\varepsilon_1, \dots, \varepsilon_m$ von ${}^m\mathbb{k}$ aus Beispiel 2.52 und erhalten

$$\langle \alpha_1, \dots, \alpha_m \rangle = \langle \varepsilon_1 \cdot A, \dots, \varepsilon_m \cdot A \rangle = \langle R_A(\varepsilon_1), \dots, R_A(\varepsilon_m) \rangle = \operatorname{im} R_A,$$

also gilt $\operatorname{rg}_Z A = \operatorname{rg} R_A$.

Es sei zunächst $B \in GL(m, \mathbb{k})$ eine invertierbare Matrix. Die zugehörige lineare Abbildung $L_B: \mathbb{k}^m \rightarrow \mathbb{k}^m$ ist ein Automorphismus, insbesondere bijektiv, siehe Folgerung 2.73 (1). Es gilt

$$\operatorname{im}(L_{BA}) = \{ B \cdot A \cdot v \mid v \in \mathbb{k}^n \} = \operatorname{im}(B|_{\operatorname{im} L_A}).$$

Die Abbildung $L_B|_{\operatorname{im} L_A}: \operatorname{im} L_A \rightarrow \operatorname{im} L_{BA}$ ist sicherlich immer noch injektiv und linear. Sie ist auch surjektiv, da wir das Bild entsprechend eingeschränkt haben. Somit sind $\operatorname{im} L_A$ und $\operatorname{im} L_{BA}$ isomorph, und es folgt

$$\operatorname{rg}_S(BA) = \dim \operatorname{im} L_{BA} = \dim \operatorname{im} L_A = \operatorname{rg}_S A.$$

Andererseits bilden $\varepsilon_1 \cdot B, \dots, \varepsilon_m \cdot B$ nach wie vor eine Basis von ${}^m\mathbb{k}$, da auch R_B ein Isomorphismus ist. Die Abbildung $R_{BA}: {}^m\mathbb{k} \rightarrow {}^m\mathbb{k}$ mit $\omega \mapsto \omega \cdot BA$ hat also das gleiche Bild wie R_A , und es gilt

$$\operatorname{rg}_Z(BA) = \dim \operatorname{im}(R_{BA}) = \dim \operatorname{im}(R_A) = \operatorname{rg}_Z A.$$

Also sind sowohl Spalten- als auch Zeilenrang unter Multiplikation mit einer invertierbaren Matrix von links invariant.

Sei jetzt $C \in GL(n, \mathbb{k})$ invertierbar. Ähnlich wie oben gilt jetzt

$$\operatorname{im} L_{AC} = \operatorname{im} L_A \quad \text{und} \quad \operatorname{im} R_A \cong \operatorname{im}(R_C|_{\operatorname{im} R_A}) = \operatorname{im} R_{AC},$$

und es folgt $\operatorname{rg}_S(AC) = \operatorname{rg}_S A$ und $\operatorname{rg}_Z(AC) = \operatorname{rg}_Z A$, also gilt (1).

Wir wählen jetzt Basen B von \mathbb{k}^m und C von \mathbb{k}^n wie in Satz 3.13. Es folgt (2), da

$$\begin{aligned} \operatorname{rg}_S(A) &= \operatorname{rg}_S(B^{-1} \cdot A \cdot C) = \operatorname{rg}_S \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} = r \\ &= \operatorname{rg}_Z \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} = \operatorname{rg}_Z(B^{-1} \cdot A \cdot C) = \operatorname{rg}_Z A. \end{aligned}$$

Matrixdarstellungen in (3) zu verschiedenen Basen unterscheiden sich um Multiplikation mit einer Basiswechsellmatrix von links oder von rechts. Nach (1) ist es also egal, wie wir B und C wählen, daher nehmen wir Basen wie im Rangsatz (3.13). Es folgt $\operatorname{im} F = \langle b_1, \dots, b_r \rangle$, also $\operatorname{rg} F = r = \operatorname{rg} A$. \square

3.18. FOLGERUNG. *Es sei $f: V \rightarrow W$ eine lineare Abbildung zwischen endlich-dimensionalen \mathbb{k} -Vektorräumen.*

- (1) *Es gilt $\operatorname{rg} f = \dim W$ genau dann, wenn f surjektiv ist.*
- (2) *Es gilt $\operatorname{rg} f = \dim V$ genau dann, wenn f injektiv ist,*
- (3) *Es gilt $\operatorname{rg} f = \dim V = \dim W$ genau dann, wenn f bijektiv ist.*

Analoge Aussagen gelten auch für Matrizen.

BEWEIS. Es gelte $\operatorname{rg} f = \dim W$, dann ist $\operatorname{im} f \subset W$ ein Unterraum voller Dimension. Nach Folgerung 3.5 (3) ist jede Basis von $\operatorname{im} f$ bereits eine Basis von W , somit gilt $W = \operatorname{im} f$, und f ist surjektiv. Die Gegenrichtung ist klar.

Sei jetzt $\operatorname{rg} f = \dim V$, dann folgt aus der Dimensionsformel im Rangsatz 3.13, dass $\dim \ker f = \dim V - \operatorname{rg} f = 0$. Es folgt $\ker f = 0$, also ist f injektiv nach Proposition 2.37 (1). Umgekehrt folgt $\operatorname{rg} f = \dim V$ aus $\ker f = \{0\}$.

Aussage (3) folgt aus (1) und (2). □

3.3. Lineare Gleichungssysteme

3.19. DEFINITION. Es sei V ein \mathbb{k} -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

$$A = a_0 + U = \{ a_0 + u \mid u \in U \} .$$

Ein affiner Unterraum $A = a + U$ heißt *endlichdimensional* mit $\dim A = \dim U$, wenn U endlichdimensional ist, sonst *unendlichdimensional*. Seien $U, W \subset V$ Untervektorräume, 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. Außerdem ist bei uns ein affiner Unterraum auch zu sich selbst parallel, dadurch wird Parallelität eine Äquivalenzrelation.

3.20. 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

$$a_1 + U = a_0 + (u_1 + U) = a_0 + U .$$

- (2) Ein affiner Unterraum ist genau dann ein Untervektorraum, wenn $0 \in A$. Die Richtung „ \implies “ folgt aus (U1), und „ \impliedby “ 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 2.38.
- (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 $A \in M_{m,n}(\mathbb{k})$, die sogenannte *linke Seite* und ein Vektor $b \in \mathbb{k}^m$, die *rechte Seite*, suchen wir alle Vektoren $x \in \mathbb{k}^n$, so dass $A \cdot x = b$. Das heißt, wir suchen die *Lösungsmenge*

$$L = \{ x \in \mathbb{k}^n \mid A \cdot x = b \} .$$

Wenn wir die Gleichung $A \cdot x = b$ ausschreiben, erhalten wir tatsächlich ein System linearer Gleichungen, nämlich

$$(*) \quad \begin{array}{ccccccc} a_{11} \cdot x_1 & + & \dots & + & a_{1n} \cdot x_n & = & b_1, \\ \vdots & & & & \vdots & & \vdots \\ a_{m1} \cdot x_1 & + & \dots & + & a_{mn} \cdot x_n & = & b_m. \end{array}$$

Wir nennen das Gleichungssystem $(*)$ *homogen*, wenn $b = 0$, und *inhomogen*, wenn $b \neq 0$. Das zu $A \cdot x = b$ gehörige homogene Gleichungssystem ist $A \cdot x = 0$.

Etwas allgemeiner können wir eine lineare Abbildung $F: V \rightarrow W$ und eine „rechte Seite“ $w \in W$ betrachten, und nach der „Lösungsmenge“

$$L = \{ v \in V \mid F(v) = w \} = F^{-1}(\{w\}),$$

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.

3.21. BEMERKUNG. Lineare Gleichungssysteme treten zum Beispiel beim Lösen der folgenden Probleme auf.

- (1) Betrachte $A \in M_{m,n}(\mathbb{k})$, 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 $b \in \mathbb{k}^m$ genau dann im Bild $\text{im } A$ von A , wenn das Gleichungssystem $A \cdot x = b$ (mindestens) eine Lösung hat.
- (3) Es sei $B \in M_n \mathbb{k}$ eine Basis des \mathbb{k}^n . Um die Koordinaten x eines Vektors $v \in \mathbb{k}^n$ 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 3.34.
- (4) Eine quadratische Matrix $A \in M_n(\mathbb{k})$ ist genau dann invertierbar, wenn eine Matrix $B \in M_n(\mathbb{k})$ mit $A \cdot B = E_n$ existiert (Übung). Um die Spalten b_1, \dots, 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

$$E = \left\{ \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} \cdot r + \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix} \cdot s \mid r, s \in \mathbb{R} \right\}$$

und

$$G = \left\{ \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} + \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix} \cdot t \mid t \in \mathbb{R} \right\},$$

dann bestimmen wir $G \cap E$ durch Lösen des Gleichungssystems

$$\begin{array}{rcl} 2 + r + s = 3 + 2t & & r + s - 2t = 1, \\ -r & = & 2 + t & \iff & -r & - & t = 2, \\ -s = 1 + t & & & & -s & - & t = 1. \end{array}$$

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 werden viele Probleme zunächst durch lineare Probleme approximiert. Anschließend sind dann lineare Gleichungssysteme zu lösen. Oftmals sind die auftretenden Matrizen „dünn besetzt“, das heißt, in jeder Zeile und/oder jeder Spalte stehen nur sehr wenige von 0 verschiedene Zahlen. Für solche Gleichungssysteme gibt es spezielle, effiziente, teils approximative Lösungsverfahren. Sie lernen sie in den entsprechenden Vorlesungen kennen.

Es folgen einfache, grundsätzliche Überlegungen zum Lösungsverhalten linearer Gleichungssysteme.

3.22. PROPOSITION. *Es sei $A \in M_{m,n}(\mathbb{k})$ und $b \in \mathbb{k}^m$.*

- (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*

$$\{ x \in \mathbb{k}^n \mid A \cdot x = b \} = x_0 + \ker A .$$

BEWEIS. Die Aussagen (1) und (2) sind gerade die Punkte (1) und (2) aus Bemerkung 3.21. Zu (3) beachten wir, dass aus $A \cdot x_0 = b$ folgt, dass

$$A \cdot x = b \iff A \cdot (x - x_0) = b - b = 0 \iff x - x_0 \in \ker A . \quad \square$$

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 $A \cdot v = 0$.

3.23. PROPOSITION. *Es seien $A \in M_{m,n}(\mathbb{k})$ und $b \in \mathbb{k}^m$. Die Lösungsmenge des linearen Gleichungssystems $A \cdot x = b$ verändert sich nicht, wenn man A und b von links mit der gleichen invertierbaren Matrix $B \in GL(m, \mathbb{k})$ multipliziert.*

BEWEIS. Es sei $x \in \mathbb{k}^n$ 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

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:

$$r \begin{pmatrix} 0 & \dots & 0 & 1 & a_{1,j_1+1} & \dots & a_{1,j_2-1} & * & a_{1,j_2+1} & \dots & a_{1,j_r-1} & * & a_{1,j_r+1} & \dots & a_{1,n} \\ 0 & & & & \dots & & 0 & 1 & a_{2,j_2+1} & \dots & a_{2,j_r-1} & * & a_{2,j_r+1} & \dots & a_{2,n} \\ \vdots & & & & & & & & & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & & & \dots & & & & & a_{r-1,j_r-1} & * & a_{r-1,j_r+1} & \dots & a_{r-1,n} \\ 0 & & & \dots & & & & & 0 & 1 & a_{r,j_r+1} & \dots & a_{r,n} \\ 0 & & & & & & \dots & & & & & & 0 \\ \vdots & & & & & & & & & & & & \vdots \\ 0 & & & & & & \dots & & & & & & 0 \end{pmatrix}.$$

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 3.27 unten, dass man bei einem Gleichungssystem in Zeilenstufenform die Lösungsmenge leicht ablesen kann.

3.26. SATZ (Gauß-Verfahren). *Jedes lineare Gleichungssystem lässt sich mit Hilfe elementarer Zeilenumformungen in (strenge) Zeilenstufenform bringen.*

Andere Namen sind *Gauß-Algorithmus*, *Gauß-Elimination*, sowie *Gauß-Jordan-Verfahren* für die strenge Zeilenstufenform.

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 3.25 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 3.25 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 $i > r$ (beziehungsweise für alle $i \neq r$).

Danach erhöhen wir q um 1, so dass jetzt $q = j$, und haben nun auch Punkt (1) (und gegebenenfalls auch (3)) in Definition 3.25 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. \square

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, die also keine (Schief-) Körper sind.

3.27. 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 $\text{im } A = \mathbb{k}^r \times \{0\} \subset \mathbb{k}^m$ von A besteht aus den Spalten $a_{j_i} = A(e_{j_i})$ für $i = 1, \dots, r$, insbesondere ist $\text{rg } A = r$.*
- (2) *Das Gleichungssystem (*) ist genau dann lösbar, wenn $b_{r+1} = \dots = b_m = 0$; in diesem Fall hat die Lösungsmenge die Gestalt*

$$\begin{aligned} & \{ x \in \mathbb{k}^n \mid A \cdot x = b \} \\ & = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{k}^n \mid x_{j_i} = b_i - \sum_{j=j_i+1}^n a_{ij} x_j \text{ für alle } i = 1, \dots, r \right\}, \end{aligned}$$

jede Lösung ist also eindeutig bestimmt durch die Angabe der Koordinaten x_j für alle $j \in \{1, \dots, n\} \setminus \{j_1, \dots, j_r\}$.

- (3) *Es sei A in strenger Zeilenstufenform, und es sei $\{k_{r+1}, \dots, k_n\} = \{1, \dots, n\} \setminus \{j_1, \dots, j_r\}$ eine Aufzählung der restlichen Spaltenindizes, dann erhalten wir eine Basis (c_{r+1}, \dots, c_n) von $\ker A$ aus Vektoren der Form*

$$c_\ell = e_{k_\ell} - \sum_{i=1}^r e_{j_i} \cdot a_{ik_\ell} \in \ker A \subset \mathbb{k}^n \quad \text{für } \ell = r+1, \dots, n.$$

Für die Basis von $\ker A$ in (2) benutzen wir die gleichen Buchstaben wie im Beweis des Rangsatzes 3.13.

BEWEIS. Zu Aussage (1) überlegen wir uns zunächst, dass 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 $j \in \{1, \dots, n\} \setminus \{j_1, \dots, j_r\}$ beliebig vorgeben, bestimmen die Zeilen $i = r, \dots, 1$ in umgekehrter Reihenfolge die fehlenden Koordinaten x_{j_r}, \dots, x_{j_1} eindeutig. Daraus folgt (2) sowie im $A = \mathbb{k}^r \times \{0\}$ und insbesondere $r = \text{rg } A$, also gilt auch (1).

Zu (3) wählen wir $b = 0$ und bestimmen Elemente c_ℓ der Lösungsmenge $\ker A$, indem wir für $p = r + 1, \dots, n$ die Koordinaten $x_{k_p} = \delta_{\ell p}$ vorgeben. Die restlichen Koordinaten sind gerade die x_{j_i} , $i = 1, \dots, r$. Wenn A in strenger Zeilenstufenform ist, bestimmen wir x_{j_i} durch die i -te Gleichung und erhalten

$$x_{j_i} = - \sum_{p=r+1}^n a_{ik_p} \cdot x_{k_p} = -a_{ik_\ell}.$$

Man überprüft anhand der Koordinaten $x_{k_{r+1}}, \dots, x_{k_n}$, dass diese Vektoren linear unabhängig sind. Sie erzeugen den Kern, bilden also eine Basis, da

$$\dim \ker A = n - \dim \text{im } A = n - r. \quad \square$$

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.

3.28. BEMERKUNG. Das Gauß-Verfahren kann benutzt werden, um viele verschiedene Probleme zu lösen. Einige davon haben wir in Bemerkung 3.21 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 3.24 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 3.23 zum alten äquivalent, und wir können die Lösungsmenge nach Proposition 3.27 (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 ein einzelnes Element der Lösungsmenge. Wenn die Lösungsmenge nicht leer ist, reicht es allerdings nach Proposition 3.22 (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 im $A \subset \mathbb{k}^m$ bestimmen. Wir bringen dazu A mit dem Gauß-Verfahren in strenge Zeilenstufenform BA , mit $B \in GL_m(\mathbb{k})$. Proposition 3.27 (3) liefert eine Basis von $\ker A = \ker(BA)$.

Nach Proposition 3.27 (1) bilden die Spalten j_1, \dots, j_r von BA eine Basis von $\text{im}(BA) = B \cdot \text{im} A$. Das sind aber genau die Bilder der Spalten j_1, \dots, j_r von A unter Multiplikation mit B . Da letztere ein linearer Isomorphismus ist, bilden die Spalten j_1, \dots, j_r von A eine Basis von $\text{im} A$.

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 \mathbb{k}^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 $\text{im} A$.

- (3) Es seien Vektoren $v_1, \dots, v_n \in \mathbb{k}^m$ gegeben. Wir möchten wissen, ob diese Vektoren linear unabhängig sind, und ob sie \mathbb{k}^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 $r = \text{rg} A = m$ gilt.

Und sie sind linear unabhängig, wenn $A \cdot x = 0$ nur eine Lösung besitzt. Nach Proposition 3.27 (2) ist das genau dann der Fall, wenn $\{j_1, \dots, j_r\} = \{1, \dots, n\}$, das heißt, wenn $r = \text{rg} A = n$ gilt.

- (4) Um eine Matrix $A \in M_n(\mathbb{k})$ 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 $\text{rg} A < n$ 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. Aus diesem Grund ist es geschickter, zunächst nur auf Zeilenstufenform hinzuarbeiten, und erst dann, wenn man weiß, dass die Matrix invertierbar ist, auch oberhalb der Diagonalen auszuräumen.

Für sehr große Matrizen ist das Gauß-Verfahren zu rechenaufwendig. Auch wenn die ursprüngliche Matrix nur wenige von 0 verschiedene Einträge pro Zeile und/oder Spalte enthielt, kann sich das bereits nach einigen Zwischenschritten ändern. 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. Daher benutzt man für große Matrizen andere, effizientere Verfahren.

3.4. Die Methode der kleinsten Quadrate

Eigentlich besprechen wir Skalarprodukte erst in Kapitel ?? . Wir führen das Standardskalarprodukt auf \mathbb{k}^n für $\mathbb{k} = \mathbb{C}$ oder \mathbb{H} bereits hier ein, da es uns einige nützliche Rechentechniken an die Hand gibt. Außerdem können wir damit die von Gauß und Legendre gefundene Methode der kleinsten Quadrate herleiten. Tatsächlich war diese Methode für Gauß möglicherweise der Hauptgrund, sich überhaupt mit linearen Gleichungssystemen zu beschäftigen.

Für die nächste Definition brauchen wir den Begriff der adjungierten Matrix. Wir erinnern uns an die komplexe und die quaternionische Konjugation aus den Definitionen 1.60 und 1.71, und die Rechenregeln aus Bemerkung 1.61 und Satz 1.72 (5), (6). Für $a \in \mathbb{R}$ sei wieder $\bar{a} = a$.

3.29. DEFINITION. Falls $\mathbb{k} = \mathbb{R}, \mathbb{C}$ oder \mathbb{H} , definieren wir die zu A *adjungierte Matrix* $A^* \in M_{n,m}(\mathbb{k})$ durch $A^* = (\bar{a}_{ij})_{j,i}$.

Für $\mathbb{k} = \mathbb{R}$ ist Adjungieren das gleiche wie Transponieren, siehe Definition 3.14.

3.30. DEFINITION. Es sei $\mathbb{k} = \mathbb{R}, \mathbb{C}$ oder \mathbb{H} . Wir definieren das *Standardskalarprodukt* $\langle \cdot, \cdot \rangle: \mathbb{k}^n \times \mathbb{k}^n \rightarrow \mathbb{k}$ durch

$$\langle v, w \rangle = \sum_{i=1}^n \bar{v}_i \cdot w_i = v^* \cdot w .$$

3.31. BEMERKUNG. Im Fall $\mathbb{k} = \mathbb{R}$ entspricht das genau dem Standardskalarprodukt aus Definition 1.52. Für $\mathbb{k} = \mathbb{C}$ und \mathbb{H} hat das Standardskalarprodukt für alle $v, w \in \mathbb{k}^n$ und alle $r \in \mathbb{k}$ die folgenden Eigenschaften.

- (1) Es ist *sesquilinear*. Das heißt, es ist linear im zweiten Argument und additiv im ersten Argument, aber anstelle von Homogenität gilt

$$\langle v \cdot r, w \rangle = \bar{r} \cdot \langle v, w \rangle .$$

- (2) Es ist *Hermiteisch*, das heißt, es gilt

$$\langle w, v \rangle = \overline{\langle v, w \rangle} .$$

Hieraus folgt insbesondere, dass $2 \operatorname{Re}\langle v, w \rangle = \langle v, w \rangle + \langle w, v \rangle$.

(3) Es ist *positiv definit*, das heißt, es gilt

$$\mathbb{R} \ni \langle v, v \rangle \geq 0 \quad \text{und} \quad \langle v, v \rangle = 0 \iff v = 0 .$$

Im Falle $\mathbb{k} = \mathbb{R}$ wird aus (1) Bilinearität, und aus (2) Symmetrie.

3.32. PROPOSITION. *Es sei R ein kommutativer Ring und $\ell, m, n \in \mathbb{N}$. Für alle $A \in M_{m,n}(R)$ und alle $B \in M_{\ell,m}(R)$ gilt*

$$(1) \quad (A^t)^t = A \quad \text{und} \quad A^t \cdot B^t = (B \cdot A)^t .$$

Es sei $\mathbb{k} = \mathbb{R}, \mathbb{C}$ oder \mathbb{H} und $\ell, m, n \in \mathbb{N}$. Für alle $A \in M_{m,n}(\mathbb{k})$, alle $B \in M_{\ell,m}(\mathbb{k})$ und alle $v \in \mathbb{k}^n, w \in \mathbb{k}^m$ gilt

$$(2) \quad (A^*)^* = A, \quad \langle w, Av \rangle = \langle A^*w, v \rangle \quad \text{und} \quad A^* \cdot B^* = (B \cdot A)^* .$$

Wir lassen den Beweis als Übung.

3.33. DEFINITION. Eine *Orthonormalbasis* ($\mathbb{k} = \mathbb{R}$) beziehungsweise eine (*quaternionisch*) *unitäre Basis* ($\mathbb{k} = \mathbb{C}, \mathbb{H}$) des \mathbb{k}^n ist ein Tupel $B = (b_1, \dots, b_n)$ von Vektoren im \mathbb{k}^n , so dass für alle i, j gilt

$$\langle b_i, b_j \rangle = \delta_{ij} .$$

3.34. PROPOSITION. *Ein Tupel $B = (b_1, \dots, b_n)$ ist genau dann eine Orthonormal- beziehungsweise unitäre Basis des \mathbb{k}^n , wenn die Matrix B mit den Spalten b_1, \dots, b_n invertierbar ist mit $B^{-1} = B^*$. Wenn das so ist, ist B eine Basis, und für jeden Vektor $v \in \mathbb{R}^n$ gilt*

$$v = \sum_{i=1}^n b_i \cdot \langle b_i, v \rangle .$$

Man beachte, dass die Matrix B jetzt tatsächlich die Matrix der Basisabbildung B ist, so dass die Merkregel aus Bemerkung 2.74 hier wirklich richtig ist. Im Spezialfall einer Orthonormalbasis wird die Koordinatenabbildung also gegeben durch $B^{-1} = B^*$. Im Allgemeinen lässt sich das Inverse einer Matrix nicht so leicht bestimmen, und allgemeine Verfahren zum Invertieren von Matrizen lernen wir später in diesem und im nächsten Kapitel kennen.

BEWEIS. In den Übungen haben wir bereits gezeigt, dass orthonormale Tupel von Vektoren linear unabhängig sind, und die Darstellung der Koordinatenabbildung überprüft. Aus Folgerung 3.5 (3) folgt, dass B eine Basis ist. Wir berechnen noch

$$B^* \cdot B = \left(\sum_{k=1}^n \bar{b}_{ki} b_{kj} \right)_{i,j} = (\langle b_i, b_j \rangle)_{i,j}$$

und schließen daraus, dass $B^{-1} = B^*$ genau dann, wenn B eine Orthonormalbasis ist. \square

Wenn man etwas ausmessen muss, dann macht man oft viele Messungen, in der Hoffnung, dass sich die Fehler der einzelnen Messungen dabei in etwa ausgleichen. Danach muss man den tatsächlichen Wert „schätzen“.

3.35. BEISPIEL. Wir wollen den Energieverbrauch eines Autos bei konstanter Geschwindigkeit pro zurückgelegter Strecke messen (physikalisch gesehen ist das eine Kraft). Dass wir überhaupt Energie verbrauchen, selbst wenn wir nicht beschleunigen, liegt an verschiedenen Typen von Reibung. Beispielsweise gibt es die Rollreibung der Räder auf der Straße und der Achsen in ihren Kugellagern, sowie den Strömungswiderstand der Karosserie an der umgebenden Luft. Wir modellieren das durch ein Polynom zweiten Grades für die Reibungskraft

$$F(v) = a_1 + a_2v + a_3v^2,$$

dabei sei v die Geschwindigkeit. Jetzt geht es darum, a_1 , a_2 und a_3 zu bestimmen (a_3 ist übrigens der c_w -Wert).

Wenn wir die Reibungskraft F_1 , F_2 , F_3 bei drei Geschwindigkeiten v_1 , v_2 , v_3 messen, erhalten wir ein Gleichungssystem in den drei Unbekannten a_1 , a_2 , a_3 mit drei Gleichungen

$$\begin{aligned} 1 \cdot a_1 + v_1 \cdot a_2 + v_1^2 \cdot a_3 &= F_1 \\ 1 \cdot a_1 + v_2 \cdot a_2 + v_2^2 \cdot a_3 &= F_2 \\ 1 \cdot a_1 + v_3 \cdot a_2 + v_3^2 \cdot a_3 &= F_3 \end{aligned}$$

Das können wir mit dem Gaußverfahren eindeutig lösen, wenn keine zwei Geschwindigkeiten gleich sind.

Wenn wir stattdessen hundertmal messen, bekommen wir hundert Gleichungen in nach wie vor nur drei Unbekannten. In Matrixschreibweise $V \cdot a = F$ mit

$$V = \begin{pmatrix} 1 & v_1 & v_1^2 \\ \vdots & \vdots & \vdots \\ 1 & v_{100} & v_{100}^2 \end{pmatrix} \in \mathbb{R}^{100 \times 3} \quad \text{und} \quad F = \begin{pmatrix} F_1 \\ \vdots \\ F_{100} \end{pmatrix} \in \mathbb{R}^{100}.$$

Dieses Gleichungssystem ist in der Regel unlösbar.

Es sei jetzt allgemeiner $Ax = b$ ein Gleichungssystem mit $A \in \mathbb{k}^{m \times n}$ und $b \in \mathbb{k}^m$ für $\mathbb{k} = \mathbb{R}$, \mathbb{C} oder \mathbb{H} . Wir suchen nicht mehr nach einer exakten Lösung, sondern versuchen, die Norm von $Ax - b$ zu minimieren. Geometrisch gesehen suchen wir denjenigen Punkt Ax im Unterraum $\text{im}(A) \subset \mathbb{k}^m$, der am nächsten am Punkt $b \in \mathbb{k}^m$ liegt bezüglich des Euklidischen Abstands, siehe Abschnitt 1.4 im Fall $\mathbb{k} = \mathbb{R}$.

3.36. SATZ (Methode der kleinsten Quadrate). *Es $A \in M_{m,n}(\mathbb{k})$ und $b \in \mathbb{k}^m$ für $\mathbb{k} = \mathbb{R}$, \mathbb{C} oder \mathbb{H} . Dann ist das Gleichungssystem $A^*Ax = A^*b$ immer lösbar, je zwei Lösungen unterscheiden sich um ein Element von $\ker A$, und $\|Ax - b\|$ nimmt genau auf der Lösungsmenge das Minimum an.*

Im obigen Beispiel müssten wir also $V^*V \cdot a = V^* \cdot F$ lösen. Das ist jetzt nur noch ein Gleichungssystem mit drei Gleichungen in drei Unbekannten. Das Minimum von $\|V \cdot a - F\|$ — also der Wert für ein a aus der Lösungsmenge — ist eine untere Schranke für die Messgenauigkeit.

BEWEIS. Zunächst nehmen wir an, es gäbe eine Lösung $x_0 \in \mathbb{k}^n$ des Gleichungssystems

$$(*) \quad A^*Ax = A^*b,$$

wobei wir die Multiplikationszeichen der Kürze halber weglassen. Sei $x \in \mathbb{k}^n$ beliebig, dann rechnen wir mit Hilfe von Bemerkung 3.31 (2), (3) und Proposition 3.32 (2) nach, dass

$$\begin{aligned} \|Ax - b\|^2 &= (A(x - x_0) + Ax_0 - b)^*(A(x - x_0) + Ax_0 - b) \\ &= \|Ax_0 - b\|^2 + 2\operatorname{Re}\langle A(x - x_0), Ax_0 - b \rangle + \|A(x - x_0)\|^2 \\ &= \|Ax_0 - b\|^2 + 2\operatorname{Re}\langle x - x_0, \underbrace{A^*Ax_0 - A^*b}_{=0} \rangle + \|A(x - x_0)\|^2 \\ &\geq \|Ax_0 - b\|^2. \end{aligned}$$

Gleichheit gilt offensichtlich genau dann, wenn $x - x_0 \in \ker A$.

Zur Lösbarkeit sei B ein Produkt von Elementarmatrizen, so dass BA^* in Zeilenstufenform ist. Da B invertierbar ist, ist auch B^* invertierbar mit inverser Matrix $(B^*)^{-1} = (B^{-1})^*$. Also ist $A^*Ax = A^*b$ genau dann lösbar, wenn $(BA^*)(BA^*)^*y = (BA^*)b$ lösbar ist, denn y ist eine Lösung des neuen Systems genau dann, wenn $x = B^*y$ eine Lösung von (*) ist.

Ohne Einschränkung sei also A^* bereits in Zeilenstufenform vom Rang r . Dann ist A in „Spaltenstufenform“, als Blockmatrix geschrieben also $A = (C \ 0)$ mit $C \in M_{m,r}(\mathbb{k})$ und $\operatorname{rg} C = r$. Wir erhalten

$$\begin{aligned} A^*A &= \begin{pmatrix} C^* \\ 0 \end{pmatrix} \cdot (C \ 0) = \begin{pmatrix} C^*C & 0 \\ 0 & 0 \end{pmatrix} \\ \text{und} \quad A^*b &= \begin{pmatrix} C^* \\ 0 \end{pmatrix} \cdot b = \begin{pmatrix} C^*b \\ 0 \end{pmatrix}. \end{aligned}$$

Wenn wir $x = \begin{pmatrix} y \\ z \end{pmatrix}$ mit $y \in \mathbb{k}^r$ und $z \in \mathbb{k}^{n-r}$ schreiben, ist (*) jetzt äquivalent zum Gleichungssystem

$$(\dagger) \quad C^*C \cdot y = C^*b$$

— an z wird also keine Bedingung gestellt.

Da $C \in M_{m,r}(\mathbb{k})$ Rang r hat, gilt $\dim \ker C = \dim \mathbb{k}^r - \operatorname{rg} C = 0$ nach Satz 3.13. Also ist C injektiv. Dann ist C^*C invertierbar, denn für alle $v \in \mathbb{k}^r$ gilt wegen Proposition 3.32 und Bemerkung 3.31 (3), dass

$$\langle v, C^*Cv \rangle = \langle Cv, Cv \rangle = \|Cv\|^2 \geq 0,$$

mit Gleichheit genau dann, wenn $Cv = 0$. Da C injektiv ist, ist das zu $v = 0$ äquivalent. Nun kann $\langle v, C^*Cv \rangle > 0$ nur gelten, wenn $C^*Cv \neq 0$, somit ist auch C^*C injektiv. Da C^*C eine quadratische Matrix ist, ist C^*C nach Satz 3.13 auch surjektiv, also ist (\dagger) lösbar. Aber dann ist auch das System (*) lösbar. \square

3.37. BEMERKUNG. Wenn das ursprüngliche Gleichungssystem $Ax = b$ lösbar ist, findet die Methode der kleinsten Quadrate genau die Lösungsmenge, denn die Lösungen von $Ax = b$ minimieren dann den Ausdruck $\|Ax - b\|$.

Wenn das ursprüngliche Gleichungssystem $Ax = b$ nicht lösbar ist, können wir das Minimum von $\|Ax - b\|$ als ein Maß für die Unlösbarkeit auffassen. Man beachte, dass sich zwei Lösungen des neuen Systems $A^*Ax = A^*b$ wieder genau um ein Element aus $\ker A$ unterscheiden, siehe Proposition 3.22 (3).

Wir haben hier die einfachste Variante der Methode der kleinsten Quadrate vorgestellt. Wenn die Zielfunktion F nicht mehr linear von den Parametern a_i abhängt, kann man das Problem nicht mehr mit Methoden der linearen Algebra lösen.

3.5. Zusammenfassung

Wir ziehen wieder Bilanz. Im ersten Abschnitt haben wir die Basissätze von Steinitz kennengelernt. Sie sind sehr mächtige Hilfsmittel, um abstrakte Probleme der linearen Algebra zu lösen, etwa Existenz von Basen, Existenz komplementärer Unterräume, und so weiter. Im zweiten Abschnitt haben wir diese Methoden benutzt, um Dimensionsformeln zu zeigen. Gleichzeitig liefern die Beweise der Steinitz-Sätze auch Algorithmen zur Konstruktion von Basen, die man für explizite Rechnungen nutzen kann.

Im zweiten Abschnitt ging es um die Dimension — die entscheidende Invariante für endlich erzeugte Vektorräume — und den Rang — die entscheidende Invariante für Abbildungen zwischen ihnen. Dimensionsformeln beschreiben das Verhalten diverser Konstruktionen in der linearen Algebra, etwa Summen von Unterräumen, Quotienten, oder Kern und Bild linearer Abbildungen.

Im dritten Abschnitt haben wir vordergründig lineare Gleichungssysteme kennengelernt und mit dem Gauß-Verfahren gelöst. Das Gauß-Verfahren kann aber noch mehr: es ist unser „Schweizer Messer“ für viele kleine bis mittelgroße Probleme der linearen Algebra. Wir kennen bereits weitere „Klingen“ zur Bestimmung von Kern und Bild linearer Abbildungen und zum Invertieren von Matrizen.

Der letzte Abschnitt behandelt die Methode der kleinsten Quadrate in einfachen Fällen. Sie ermöglicht es uns beispielsweise, Parameter anhand von Messungen zu schätzen. Weitere Schätz- und Approximationsverfahren lernen Sie in Stochastik und Numerik kennen. Historisch gesehen war die Methode der kleinsten Quadrate vermutlich der Grund für Gauß, sich überhaupt mit linearen Gleichungssystemen zu beschäftigen — das sogenannte Gauß-Verfahren selbst war übrigens in China schon wenige Jahrhunderte nach Christi Geburt bekannt, und in Europa ebenfalls schon vor seiner Beschreibung durch Gauß.

KAPITEL 4

Determinanten

In den nächsten Kapiteln wollen wir Endomorphismen von Vektorräumen beziehungsweise freien R -Moduln V verstehen, also lineare Abbildungen $F: V \rightarrow V$. Endomorphismen endlich erzeugter freier Moduln werden durch quadratische Matrizen $A \in M_n(R)$ dargestellt. In diesem Kapitel lernen wir eine erste, 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. Wir benötigen in den folgenden Kapiteln aber auch Determinanten von Matrizen über dem Polynomring eines Körpers.

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 \mathbb{k} immer einen Körper bezeichnen.

4.1. Volumina und Determinantenfunktionen

In Bemerkung 1.70 (2) haben wir die Volumina von Parallelotopen im \mathbb{R}^3 ausgerechnet. Im \mathbb{R}^n wollen wir entsprechend das n -dimensionale Volumen

$$\text{vol}(v_1, \dots, v_n)$$

eins von Vektoren $v_1, \dots, v_n \in \mathbb{R}^n$ aufgespannten Parallelotops bestimmen. Wir möchten, dass dieser Volumenbegriff zwei Eigenschaften hat, nämlich *positive Homogenität* und *Scherungsinvarianz*: Für alle n -Tupel (v_1, \dots, v_n) , alle $i, j \in \{1, \dots, n\}$ mit $i \neq j$ und alle $\ell \in \mathbb{R}$ soll gelten

$$(1) \quad \text{vol}(v_1, \dots, v_{i-1}, v_i \cdot \ell, v_{i+1}, \dots, v_n) = \text{vol}(v_1, \dots, v_n) \cdot |\ell| ;$$

$$(2) \quad \text{vol}(v_1, \dots, v_{i-1}, v_i + v_j \cdot \ell, v_{i+1}, \dots, v_n) = \text{vol}(v_1, \dots, v_n) .$$

Bedingung (2) lässt sich mit dem Cavalierischen Prinzip begründen: die Querschnitte von beiden Parallelotopen mit affinen Unterräumen parallel zu $\langle v_1, \dots, \widehat{v}_i, \dots, v_n \rangle$ haben jeweils dasselbe Volumen, wenn man v_i um ein Vielfaches von v_j abändert.

Da für allgemeine Körper kein Absolutbetrag definiert ist, ist Bedingung (1) im allgemeinen nicht sinnvoll. Wir ersetzen sie daher durch Homogenität in

jedem einzelnen Argument und fordern die Eigenschaften

$$(1') \quad \omega(v_1, \dots, v_{i-1}, v_i \cdot \ell, v_{i+1}, \dots, v_n) = \omega(v_1, \dots, v_n) \cdot \ell,$$

$$(2) \quad \omega(v_1, \dots, v_{i-1}, v_i + v_j \cdot \ell, v_{i+1}, \dots, v_n) = \omega(v_1, \dots, v_n)$$

für ein „Volumen“ $\omega(v_1, \dots, v_n)$ mit Vorzeichen“, wobei $v_1, \dots, v_n \in \mathbb{k}^n$. Falls $\mathbb{k} = \mathbb{R}$ oder \mathbb{C} und ω die Bedingungen (1') und (2) erfüllt, erfüllt $\text{vol} = |\omega|$ die Bedingungen (1) und (2) und liefert daher einen Volumenbegriff.

Außerdem lassen sich aus den Bedingungen (1') und (2) zwei weitere Bedingungen ableiten, mit denen wir später besser arbeiten können. Zum einen gilt $\omega(v_1, \dots, v_n) = 0$ falls $v_i = v_j$ für zwei Indizes $i \neq j$. Dazu „scheren“ wir v_i um $-v_j$ und erhalten 0 als i -tes Argument, was wegen Homogenität (2) impliziert, dass das Ergebnis 0 wird.

Zum anderen ist ω in jedem Argument additiv (und daher wegen (2) in jedem Argument linear). Dazu betrachten wir $\omega(v_1 + w, v_2, \dots, v_n)$ für v_1, \dots, v_n und $w \in \mathbb{k}^n$ und unterscheiden zwei Fälle: wenn (v_1, \dots, v_n) linear abhängig sind, sei einer der Vektoren eine Linearkombination der restlichen, etwa v_1 , dann folgt aus Scherungsinvarianz und Homogenität, dass

$$\omega(v_1, \dots, v_n) = \omega\left(\sum_{j=2}^n v_j \cdot \ell_j, v_2, \dots, v_n\right) = \omega(0, v_2, \dots, v_n) = 0.$$

Wenn (w, v_1, \dots, v_2) linear unabhängig sind, tauschen wir v_1 und w und betrachten den zweiten Fall. Andernfalls überprüft man, dass auch $(v_1 + w, v_2, \dots, v_n)$ linear abhängig sind, und erhält

$$\omega(v_1 + w, v_2, \dots, v_n) = 0 = \omega(v_1, \dots, v_n) + \omega(w, v_2, \dots, v_n).$$

Wir dürfen also annehmen, dass (v_1, \dots, v_n) eine Basis bilden, und schreiben

$$w = \sum_j v_j \cdot \ell_j.$$

Aus Scherungsinvarianz (2) und Homogenität (1') folgt

$$\begin{aligned} \omega(v_1 + w, v_2, \dots, v_n) &= \omega\left(v_1 + \sum_j v_j \cdot \ell_j, v_2, \dots, v_n\right) \\ &= \omega(v_1 \cdot (1 + \ell_1), v_2, \dots, v_n) \\ &= \omega(v_1, \dots, v_n) + \omega(v_1, \dots, v_n) \cdot \ell_1 \\ &= \omega(v_1, \dots, v_n) + \omega\left(\sum_j v_j \cdot \ell_j, v_2, \dots, v_n\right) \\ &= \omega(v_1, \dots, v_n) + \omega(w, v_2, \dots, v_n). \end{aligned}$$

Die Linearität in den anderen Argumenten ergibt sich genauso.

Soviel zur Motivation. Ab jetzt sei R ein kommutativer Ring, M ein R -Moduln M und $k \in \mathbb{N}$.

4.1. DEFINITION. Es sei M ein R -Modul, $k \in \mathbb{N}$, und $\alpha: M^k \rightarrow R$ 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

$$(1) \quad M \rightarrow R \quad \text{mit} \quad w \mapsto \alpha(v_1, \dots, v_{i-1}, w, v_{i+1}, \dots, v_k)$$

linear ist. Sie heißt *alternierend* oder auch *alternierende Form*, wenn für alle $i = 1, \dots, k-1$ gilt, dass

$$(2) \quad \alpha(v_1, \dots, v_k) = 0 \quad \text{falls } v_{i+1} = v_i.$$

Die Menge aller alternierenden multilinearen Abbildungen $\alpha: M^k \rightarrow R$ wird mit $\Lambda^k M^*$ bezeichnet. Falls V ein n -dimensionaler \mathbb{k} -Vektorraum ist, heißt eine alternierende multilineare Abbildung $\omega: V^n \rightarrow \mathbb{k}$ 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 $\mathbb{R}^3 \rightarrow \mathbb{R}$ mit $(x, y, z) \mapsto \langle x \times y, z \rangle$ aus Satz 1.69. Wegen Bemerkungen 1.53 (1) und 1.68 (1), (1') ist das Spatprodukt multilinear, und wegen Bemerkung 1.68 (2) und Satz 1.69 (1) ist es alternierend. Also ist das Spatprodukt eine Determinantenfunktion.

4.3. PROPOSITION. *Es sei M ein R -Modul und $\alpha: M^k \rightarrow R$ multilinear. Dann sind die folgenden Aussagen äquivalent.*

- (1) *Die Abbildung α ist alternierend,*
- (2) *Aus $v_i = v_j$ für zwei Indizes $i \neq j$ folgt $\alpha(v_1, \dots, v_k) = 0$.*

Die Aussagen (1) und (2) implizieren die Eigenschaft

- (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*

$$\alpha(v_1, \dots, v_{i-1}, v_j, v_{i+1}, \dots, v_{j-1}, v_i, v_{j+1}, \dots, v_k) = -\alpha(v_1, \dots, v_k).$$

Wenn $v_i = v_j$ für $i \neq j$ gilt, folgt aus Behauptung (3) durch „Vertauschen“ der beiden gleichen Einträge zunächst nur $\alpha(v_1, \dots, v_n) = -\alpha(v_1, \dots, v_n)$, also $2\alpha(v_1, \dots, v_n) = 0$. Nur wenn wir in R durch 2 teilen dürfen, zum Beispiel in einem Körper der Charakteristik $\chi(\mathbb{k}) \neq 2$, ist (3) zu (1) und (2) äquivalent.

BEWEIS. Da wir Aussage (3) gleich brauchen, beginnen wir mit „(1) \implies (3)“ und betrachten zunächst den Fall $j = i + 1$. Dann folgt

$$\begin{aligned} \alpha(v_1, \dots, v_k) &= \alpha(v_1, \dots, v_k) + \underbrace{\alpha(v_1, \dots, v_i, v_i, v_{i+2}, \dots, v_k)}_{=0} \\ &= \alpha(v_1, \dots, v_i, v_i + v_{i+1}, v_{i+2}, \dots, v_k) \\ &\quad - \underbrace{\alpha(v_1, \dots, v_{i-1}, v_i + v_{i+1}, v_i + v_{i+1}, v_{i+2}, \dots, v_k)}_{=0} \end{aligned}$$

$$\begin{aligned}
&= \alpha(v_1, \dots, v_{i-1}, -v_{i+1}, v_i + v_{i+1}, v_{i+2}, \dots, v_k) \\
&\quad + \underbrace{\alpha(v_1, \dots, v_{i-1}, -v_{i+1}, -v_{i+1}, v_{i+2}, \dots, v_k)}_{=0} \\
&= -\alpha(v_1, \dots, v_{i-1}, v_{i+1}, v_i, v_{i+2}, \dots, v_k) .
\end{aligned}$$

Also ändert sich das Vorzeichen, wenn man zwei benachbarte Vektoren vertauscht. Der allgemeine Fall folgt durch Induktion über $p = j - i$, denn

$$\begin{aligned}
\alpha(v_1, \dots, v_k) &= -\alpha(v_1, \dots, v_{i-1}, v_{j-1}, v_{i+1}, \dots, v_{j-2}, v_i, v_j, v_{j+1}, \dots, v_k) \\
&= \alpha(v_1, \dots, v_{i-1}, v_{j-1}, v_{i+1}, \dots, v_{j-2}, v_j, v_i, v_{j+1}, \dots, v_k) \\
&= -\alpha(v_1, \dots, v_{i-1}, v_j, v_{i+1}, \dots, v_{j-2}, v_{j-1}, v_i, v_{j+1}, \dots, v_k) .
\end{aligned}$$

Dabei haben wir nur Argumente im Abstand von weniger als p vertauscht.

Zu „(1) \implies (2)“ benutzen wir (3). Es gelte $v_i = v_j$ für $i + 1 < j$, so dass die Behauptung nicht unmittelbar aus (1) folgt. Wegen (3) gilt dann

$$\begin{aligned}
\alpha(v_1, \dots, v_{j-1}, v_i, v_{j+1}, \dots, v_n) \\
= -\alpha(v_1, \dots, v_{i-1}, v_{j-1}, v_{i+1}, \dots, v_{j-2}, v_i, v_i, v_{j+1}, \dots, v_n) = 0 .
\end{aligned}$$

Die Richtung „(2) \implies (1)“ ist klar. \square

4.4. BEMERKUNG. Wir haben in der Motivation von einem „Volumen mit Vorzeichen“ Homogenität (1') und Scherungsinvarianz gefordert. Daraus haben wir die Bedingungen an eine Determinantenfunktion in Definition 4.1 hergeleitet. Umgekehrt sind Determinantenfunktionen per definitionem homogen. Sie sind wegen Proposition 4.3 (2) auch scherungsinvariant, denn

$$\begin{aligned}
\alpha(v_1, \dots, v_{i-1}, v_i + v_j \cdot \ell, v_{i+1}, \dots, v_n) \\
= \alpha(v_1, \dots, v_n) + \alpha(v_1, \dots, v_{i-1}, v_j, v_{i+1}, \dots, v_n) \cdot \ell = \alpha(v_1, \dots, v_n) .
\end{aligned}$$

Also sind Determinantenfunktionen gerade „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 2.30. Aber man braucht Kommutativität von R bereits, um überhaupt multilineare Abbildungen mit zwei oder mehr Argumenten zu bekommen, wie die folgende Rechnung zeigt:

$$\begin{aligned}
\alpha(v_1, \dots, v_k) \cdot r \cdot s &= \alpha(v_1 \cdot r, v_2, \dots, v_k) \cdot s = \alpha(v_1 \cdot r, v_2 \cdot s, v_3, \dots, v_k) \\
&= \alpha(v_1, v_2 \cdot s, v_3, \dots, v_k) \cdot r = \alpha(v_1, \dots, v_k) \cdot s \cdot r .
\end{aligned}$$

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 “ mit verschiedenen Volumenbegriffen 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 $n = 1$ setzen wir $\omega_0(r) = r \in R$ 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 $\varepsilon_n(x)$, siehe Bemerkung 2.65. Wir definieren ω_n rekursiv durch

$$(*) \quad \omega_n(x_1, \dots, x_n) = \sum_{i=1}^n (-1)^{i+n} \varepsilon_n(x_i) \omega_{n-1}(x'_1, \dots, \widehat{x'_i}, \dots, x'_n) \in R,$$

wobei ein Dach über einem Eintrag gerade „Weglassen“ bedeutet. Diese Konstruktion liefert zugleich ein erstes Verfahren zur Berechnung von ω_n , die Laplace-Entwicklung, siehe Satz 4.16 unten.

4.6. PROPOSITION. *Es sei R ein kommutativer Ring mit Eins, dann ist die oben konstruierte Abbildung $\omega_n: R^n \rightarrow R$ alternierend, multilinear, und erfüllt*

$$\omega_n(e_1, \dots, e_n) = 1.$$

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 $i \in \{1, \dots, n-1\}$. 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

$$\omega_n(e_1, \dots, e_n) = (-1)^{n+n} \varepsilon_n(e_n) \omega_{n-1}(e'_1, \dots, e'_{n-1}) = 1. \quad \square$$

Als nächstes überlegen wir uns, dass der Raum $\Lambda^n V^*$ genau eindimensional ist. Zunächst erinnern wir uns an die Automorphismengruppe $\text{Aut}(M)$ einer Menge aus Beispiel 2.5. Es sei weiterhin ω_n die soeben auf R^n definierte Determinantenfunktion.

4.7. DEFINITION. Es sei $n \in \mathbb{N}$. Die *symmetrische Gruppe S_n in n Elementen* ist definiert als $S_n = \text{Aut}(\{1, \dots, n\})$, ihre Elemente $S_n \ni \sigma: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ heißen *Permutationen*.

Es sei R ein kommutativer Ring mit Eins. Wir definieren das *Vorzeichen* oder auch *Signum* einer Permutation $\sigma \in S_n$ durch

$$\text{sign}(\sigma) = \omega_n(e_{\sigma(1)}, \dots, e_{\sigma(n)}).$$

Unter einer *Transposition* verstehen wir eine Permutation $\tau = \tau_{ij} \in S_n$, die nur zwei Elemente i und j mit $1 \leq i < j \leq n$ vertauscht, also

$$\tau_{ij}(k) = \begin{cases} j & \text{falls } k = i, \\ i & \text{falls } k = j, \text{ und} \\ k & \text{sonst.} \end{cases}$$

4.8. PROPOSITION. Jede Permutation $\sigma \in S_n$ kann als Produkt $\sigma = \tau_1 \circ \dots \circ \tau_k$ von Transpositionen $\tau_1, \dots, \tau_k \in S_n$ geschrieben werden, und es gilt

$$(1) \quad \text{sign}(\sigma) = (-1)^k .$$

Für $\rho, \sigma \in S_n$ gilt dann

$$(2) \quad \text{sign}(\rho \circ \sigma) = \text{sign}(\rho) \cdot \text{sign}(\sigma) \quad \text{und} \quad \text{sign}(\sigma^{-1}) = \text{sign}(\sigma) .$$

Dabei fassen wir die Identität als „leeres Produkt“ mit $k = 0$ auf. Im allgemeinen sind weder k noch τ_1, \dots, τ_k durch σ eindeutig bestimmt, allein das Vorzeichen ist eine Invariante. Nach (1) gilt stets $\text{sign}(\sigma) \in \{1, -1\}$, unabhängig vom Ring R . Allerdings könnte $1 = -1$ in R gelten (Beispiel: $R = \mathbb{Z}/2\mathbb{Z}$); in diesem Fall verliert das Vorzeichen seine Information.

BEWEIS. Wir beweisen die erste Aussage durch Induktion über n . Für $n = 1$ gibt es nur eine Permutation, die Identität, mit

$$\text{sign}(\text{id}_{\{1\}}) = \omega_1(e_1) = 1 .$$

Sei die Aussage für alle $\sigma' \in S_{n-1}$ bewiesen, und sei $\sigma \in S_n$. Falls $\sigma(n) = n$, sei $\sigma' = \sigma|_{\{1, \dots, n-1\}} \in S_{n-1}$. Da σ' ein Produkt von Transpositionen aus S_{n-1} ist, 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 $\tau_1 \circ \dots \circ \tau_k$. Da $\tau = \tau^{-1}$, folgt

$$\sigma = \tau \circ \tau_1 \circ \dots \circ \tau_k .$$

Wir beweisen (1) für $\sigma = \tau_1 \circ \dots \circ \tau_k = \sigma' \circ \tau_k$ durch Induktion über k . Der Induktionsanfang für $k = 0$ ist klar, denn $\text{sign}(\text{id}) = \omega_n(e_1, \dots, e_n) = 1$ nach Propositionen 4.6. Angenommen, $\sigma = \sigma' \circ \tau_k$, und τ_k vertausche i und j . Aus Proposition 4.3 (3) folgt dann

$$\begin{aligned} \text{sign}(\sigma) &= \omega_n(e_{\sigma'(1)}, \dots, \underbrace{e_{\sigma'(j)}}_i, \dots, \underbrace{e_{\sigma'(i)}}_j, \dots, e_{\sigma'(n)}) \\ &= -\omega_n(e_{\sigma'(1)}, \dots, e_{\sigma'(n)}) = -(-1)^{k-1} = (-1)^k . \end{aligned}$$

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

$$\text{sign}(\sigma) \cdot \text{sign}(\sigma^{-1}) = \text{sign}(\sigma \cdot \sigma^{-1}) = \text{sign}(\text{id}) = 1 . \quad \square$$

In der folgenden Proposition zeigen wir die Eindeutigkeit einer bestimmten Determinantenfunktion. Der Beweis liefert uns eine zweite Berechnungsmethode der Standard-Determinantenfunktion ω_n , die sogenannte Leibniz-Formel, siehe Satz 4.13 unten.

4.9. PROPOSITION. *Es sei R ein kommutativer Ring mit Eins, $r \in R$ und M ein freier R -Modul mit Basis $B = (b_1, \dots, b_n)$. Dann existiert genau eine Determinantenfunktion $\omega \in \Lambda^n M^*$ mit*

$$\omega(b_1, \dots, b_n) = r .$$

Sei ω_B die obige Determinantenfunktion zu $r = 1$, dann ist $\Lambda^n M^$ ein freier R -Modul mit Basis (ω_B) .*

BEWEIS. Zur Eindeutigkeit bestimmen wir den Wert von $\omega(v_1, \dots, v_n)$ für Modulelemente

$$v_j = \sum_{i=1}^n b_i \cdot a_{ij} \in R^n \quad \text{für } j = 1, \dots, n .$$

Als erstes schließen wir aus Multilinearität, dass

$$\begin{aligned} \omega(v_1, \dots, v_n) &= \omega\left(\sum_{i=1}^n b_i \cdot a_{i1}, \dots, \sum_{i=1}^n b_i \cdot a_{in}\right) \\ &= \sum_{i_1=1}^n \cdots \sum_{i_n=1}^n \omega(b_{i_1}, \dots, b_{i_n}) \cdot a_{i_1 1} \cdots a_{i_n n} . \end{aligned}$$

Als nächstes dürfen wir wegen 4.3 (2) wir alle Summanden weglassen, bei denen $i_j = i_k$ für $j \neq k$. Somit ist die Abbildung von der Menge $\{1, \dots, n\}$ in sich mit $j \mapsto i_j$ injektiv, und da die Menge endlich ist, auch surjektiv. Wir können die Indizes i_1, \dots, i_n also durch eine Permutation beschreiben und erhalten

$$\omega(v_1, \dots, v_n) = \sum_{\sigma \in S_n} \omega(b_{\sigma(1)}, \dots, b_{\sigma(n)}) \cdot a_{\sigma(1),1} \cdots a_{\sigma(n),n} .$$

Nach Proposition 4.8 können wir σ als Produkt von k Transpositionen schreiben. Wie im Beweis von Proposition 4.8 (1) geht $\omega(b_{\sigma(1)}, \dots, b_{\sigma(n)})$ aus $\omega(b_1, \dots, b_n)$ hervor, indem man k -fach je zwei Argumente vertauscht. Wegen Proposition 4.3 (3) ist ω eindeutig bestimmt durch

$$\begin{aligned} \omega(v_1, \dots, v_n) &= \sum_{\sigma \in S_n} \text{sign}(\sigma) \omega(b_1, \dots, b_n) \cdot a_{\sigma(1),1} \cdots a_{\sigma(n),n} \\ (*) \quad &= \sum_{\sigma \in S_n} \text{sign}(\sigma) r \cdot a_{\sigma(1),1} \cdots a_{\sigma(n),n} . \end{aligned}$$

Es sei $B: R^n \rightarrow M$ die Basisabbildung, siehe Bemerkung 2.74, und es sei wieder $v_j = B(a_j)$ mit $a_j = (a_{ij})_i \in R^n$. Wir definieren zunächst eine alternierende multilineare Abbildung ω_B mit

$$\omega_B(v_1, \dots, v_n) = \omega_n(a_1, \dots, a_n) , \quad \text{so dass} \quad \omega_B(b_1, \dots, b_n) = 1 .$$

Nach Proposition 4.6 ist ω_n multilinear und alternierend, also auch ω_B . Wir erhalten die gesuchte Form ω als

$$\omega = \omega_B \cdot r = \omega_B \cdot \omega(b_1, \dots, b_n).$$

Aufgrund der obigen Eindeutigkeitsaussage sind alle $\omega \in \Lambda^n M^*$ von dieser Gestalt, also bildet (ω_B) eine Basis von $\Lambda^n M^*$. \square

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.

4.10. BEMERKUNG. Es seien M, N Moduln über R und $F: M \rightarrow N$ linear, dann definieren wir für alle k eine Abbildung $F^*: \Lambda^k N^* \rightarrow \Lambda^k M^*$ durch

$$(1) \quad (F^*(\alpha))(v_1, \dots, v_k) = \alpha(F(v_1), \dots, F(v_k))$$

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 $F^*(\alpha): M^k \rightarrow R$. 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

$$\begin{aligned} (F^*(\alpha))(x \cdot r + y \cdot s, v_2, \dots, v_k) &= \alpha(F(x \cdot r + y \cdot s), F(v_2), \dots, F(v_k)) \\ &= \alpha(F(x) \cdot r + F(y) \cdot s, F(v_2), \dots, F(v_k)) \\ &= \alpha(F(x), F(v_2), \dots, F(v_k)) \cdot r + \alpha(F(y), F(v_2), \dots, F(v_k)) \cdot s \\ &= (F^*(\alpha))(x, v_2, \dots, v_k) \cdot r + (F^*(\alpha))(y, v_2, \dots, v_k) \cdot s. \end{aligned}$$

Also ist $F^*(\alpha)$ multilinear.

Und $F^*(\alpha)$ ist auch alternierend, denn

$$(F^*(\alpha))(v_1, \dots, v_i, v_i, \dots, v_k) = \alpha(F(v_1), \dots, F(v_i), F(v_i), \dots, F(v_k)) = 0.$$

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 $F^*: \Lambda^k N^* \rightarrow \Lambda^k M^*$ ist linear, denn für alle $\alpha,$

$\beta \in \Lambda^k N^*$, alle $r, s \in R$ und alle $v_1, \dots, v_k \in M$ gilt

$$\begin{aligned}
 (2) \quad & (F^*(\alpha \cdot r + \beta \cdot s))(v_1, \dots, v_k) \\
 &= (\alpha \cdot r + \beta \cdot s)(F(v_1), \dots, F(v_k)) \\
 &= \alpha(F(v_1), \dots, F(v_k)) \cdot r + \beta(F(v_1), \dots, F(v_k)) \cdot s \\
 &= (F^*(\alpha) \cdot r + F^*(\beta) \cdot s)(v_1, \dots, v_k) .
 \end{aligned}$$

Schließlich seien $F: M \rightarrow N$ und $G: L \rightarrow M$ lineare Abbildungen, dann gilt $(F \circ G)^* = G^* \circ F^*: \Lambda^k N^* \rightarrow \Lambda^k L^*$, denn

$$\begin{aligned}
 (3) \quad & ((F \circ G)^*(\alpha))(\ell_1, \dots, \ell_k) = \alpha(F(G(\ell_1)), \dots, F(G(\ell_k))) \\
 &= (F^*(\alpha))(G(\ell_1), \dots, G(\ell_k)) = (G^*(F^*(\alpha)))(\ell_1, \dots, \ell_k) .
 \end{aligned}$$

Man beachte, dass Zurückholen die Reihenfolge der beteiligten Abbildungen vertauscht.

Es sei M ein freier R -Modul mit Basis $B = (b_1, \dots, b_n)$. In Proposition 4.9 haben wir gesehen, dass $\Lambda^n M^* \cong R$ ein freier Modul mit einelementiger Basis (ω_B) ist. Dabei ist $\omega_B \in \Lambda^n M^*$ das Element mit $\omega_B(b_1, \dots, b_n) = 1$. Sei jetzt $F \in \text{End}_R(M)$, dann ist $F^* \in \text{End}_R(\Lambda^n M^*)$ nach der obigen Bemerkung, aber $\text{End}_R(\Lambda^n M^*) \cong R$, da $\Lambda^n V^* \cong R$. Also existiert zu jedem $F \in \text{End } M$ ein Skalar $a = \det F \in R$, so dass

$$F^* \omega = \omega \cdot a \quad \text{für alle } \omega \in \Lambda^n M^* .$$

Um a zu bestimmen, wählen wir eine Basis (b_1, \dots, b_n) , definieren ω_B wie in Proposition 4.9, und überlegen uns, dass

$$\begin{aligned}
 \omega_B(F(b_1), \dots, F(b_n)) &= (F^*(\omega_B))(b_1, \dots, b_n) \\
 &= (\omega_B \cdot a)(b_1, \dots, b_n) = (\omega_B)(b_1, \dots, b_n) \cdot a = a .
 \end{aligned}$$

Im Spezialfall $M = R^n$ mit der Standardbasis sind die Vektoren $F(e_1), \dots, F(e_n)$ 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.

4.11. DEFINITION. Es sei R ein kommutativer Ring mit Eins, M ein freier R -Modul mit einer n -elementigen Basis, wobei $n \geq 1$, und $F \in \text{End}_R(M)$ ein Endomorphismus. Dann ist die *Determinante* von F der eindeutige Skalar $\det F \in R$, so dass

$$(1) \quad F^* \omega = \omega \cdot \det F \quad \text{für alle } \omega \in \Lambda^n M^* .$$

Wir definieren die *Determinante* einer Matrix $A \in M_n(R)$ mit den Spalten $a_1, \dots, a_n \in R^n$ durch

$$(2) \quad \det A = \omega_n(a_1, \dots, a_n) .$$

Im Falle $n = 0$ folgt $\det() = 1$, da $\omega_0() = 1$. In Gleichung (1) haben wir für jeden Endomorphismus $F \in \text{End}_R M$ 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. Wichtig ist dabei immer, dass wir nur Determinanten von Endomorphismen definieren können. Abbildungen zwischen verschiedenen Vektorräumen haben keine wohldefinierte Determinante, es sei denn, wir geben auf beiden Räumen eine Basis vor — nur in diesem Fall können wir überhaupt Volumina vergleichen.

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.

4.12. SATZ. *Sei V ein freier R -Modul mit einer n -elementigen Basis, und es seien $F, G \in \text{End } V$, dann gilt*

$$(1) \quad \det(F \circ G) = \det F \cdot \det G ,$$

d.h., die Determinante ist multiplikativ. Für Matrizen $A, B \in M_n(R)$ gilt entsprechend

$$(2) \quad \det(A \cdot B) = \det A \cdot \det B .$$

BEWEIS. Die Multiplikativität von \det über einem Körper \mathbb{k} folgt direkt aus der Kompositionsregel in Bemerkung 4.10 (3), denn für alle $\omega \in \Lambda^n V^*$ gilt

$$\omega \cdot \det(F \circ G) = (F \circ G)^* \omega = G^* \circ F^* \omega = F^* \omega \cdot \det G = \omega \cdot \det G \cdot \det F .$$

Indem wir $\omega = \omega_n \neq 0$ wählen, folgt (1). Sei $F \in \text{Aut } V$, dann ist F invertierbar nach Definition 2.30, also existiert eine Umkehrabbildung F^{-1} mit

$$\det F \cdot \det F^{-1} = \det(F \circ F^{-1}) = \det(\text{id}_V) = 1 .$$

Insbesondere folgt $\det F \in \mathbb{k}^\times = \mathbb{k} \setminus \{0\}$ mit $(\det F)^{-1} = \det(F^{-1})$, und außerdem ist $\det: \text{Aut } V \rightarrow \mathbb{k}^\times$ ein Gruppenhomomorphismus.

Wir erhalten (2) als Spezialfall für $M = R^n$, da $\text{End}_R M = M_n(R)$. □

4.13. SATZ (Leibniz-Formel). *Für jede Matrix $A \in M_n(R)$ mit $n \geq 1$ gilt*

$$\det A = \sum_{\sigma \in S(n)} \text{sign}(\sigma) \cdot \prod_{j=1}^n a_{\sigma(j),j} = \sum_{\rho \in S(n)} \text{sign}(\rho) \cdot \prod_{i=1}^n a_{i,\rho(i)} .$$

BEWEIS. Die erste Formel ist (*) aus dem Beweis von Proposition 4.9. Sei ρ die Umkehrabbildung von σ , dann erhalten wir die zweite Formel, indem wir j durch $\rho(i)$ ersetzen. □

Wir wollen jetzt ein etwas effizienteres Verfahren zum Berechnen von Determinanten kennenlernen, genauer gesagt, eine Verallgemeinerung der Formel (*) für ω_n . 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

$$A_{ij} = \begin{pmatrix} a_{11} & \cdots & a_{1,j-1} & a_{1,j+1} & \cdots & a_{1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{i-1,1} & \cdots & a_{i-1,j-1} & a_{i-1,j+1} & \cdots & a_{i-1,n} \\ a_{i+1,1} & \cdots & a_{i+1,j-1} & a_{i+1,j+1} & \cdots & a_{i+1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{n1} & \cdots & a_{n,j-1} & a_{n,j+1} & \cdots & a_{nn} \end{pmatrix} \in M_{n-1}(R).$$

4.16. 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*

$$(1) \quad \det(A) = \sum_{j=1}^n (-1)^{i+j} a_{ij} \cdot \det(A_{ij}).$$

Entwicklung nach der j -ten Spalte. Für alle $j \in \{1, \dots, n\}$ gilt

$$(2) \quad \det(A) = \sum_{i=1}^n (-1)^{i+j} a_{ij} \cdot \det(A_{ij}).$$

BEWEIS. Wir betrachten die durch die rechte Seite von Formel (1) induktiv definierte Abbildung $\omega: M_n(R) \rightarrow R$ und zeigen wie im Beweis von Proposition 4.6, dass sie multilinear und alternierend in den Spalten von A ist. Aufgrund der Eindeutigkeitsaussage in Proposition 4.9 und Definition 4.11 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

$$\omega(E_n) = \sum_{j=1}^n (-1)^{i+j} \delta_{ij} \cdot \det((E_n)_{ij}) = \det(E_{n-1}) = 1,$$

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 und Folgerung 4.15 benutzen. \square

4.17. 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 $i, j \in \{1, \dots, n\}$ mit $i > j$ ($i < j$). Eine Matrix heißt *in strikter oberer/unterer Dreiecksgestalt*, wenn zusätzlich $a_{ii} = 0$ für alle $i \in \{1, \dots, n\}$.

Somit ist die linke Matrix unten eine obere Dreiecksmatrix, und die rechte sogar in strikter Dreiecksgestalt:

$$\begin{pmatrix} a_{11} & & \dots & a_{1n} \\ 0 & a_{22} & & \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & a_{nn} \end{pmatrix}, \quad \begin{pmatrix} 0 & a_{12} & \dots & a_{1n} \\ \vdots & \ddots & \ddots & \vdots \\ & & & a_{n-1,n} \\ 0 & \dots & & 0 \end{pmatrix}.$$

Außerdem erinnern wir uns an Blockmatrizen, siehe Satz 3.13.

4.18. 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*

$$\det \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} = \det(A) \cdot \det(D) = \det \begin{pmatrix} A & 0 \\ C & D \end{pmatrix}$$

$$\text{und} \quad \det \begin{pmatrix} B & A \\ D & 0 \end{pmatrix} = (-1)^{k\ell} \det(A) \cdot \det(D) = \det \begin{pmatrix} 0 & A \\ D & C \end{pmatrix}.$$

- (2) *Es sei A eine obere oder untere Dreiecksmatrix, dann gilt*

$$\det(A) = \prod_{i=1}^n a_{ii}.$$

BEWEIS. Es reicht, eine der vier Gleichungen in (1) zu beweisen. Die anderen lassen sich daraus ableiten, indem man die ersten k Zeilen mit den letzten ℓ vertauscht, und/oder die ersten k Spalten mit den letzten ℓ . Die zugehörigen Permutationen haben jeweils das Vorzeichen $(-1)^{k\ell}$, was auch die Vorzeichen in der zweiten Zeile erklärt.

Es sei also $M = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix}$. Wir zeigen durch Induktion über k , dass $\det(M) = \det(A) \cdot \det(D)$. Als Induktionsanfang wählen wir $k = 0$, so dass $M = A$, und vereinbaren, dass $\det(\) = 1$.

Für den Induktionsschritt entwickeln wir nach der ersten Spalte und erhalten

$$\det M = \sum_{i=1}^{k+\ell} (-1)^{i+1} m_{i1} \det(M_{i1}) = \sum_{i=1}^k (-1)^{i+1} a_{i1} \det(M_{i1}),$$

da $m_{i1} = 0$ für $i > k$. Für $1 \leq i \leq k$ erhalten wir eine Matrix der Form

$$M_{i1} = \begin{pmatrix} A_{i1} & * \\ 0 & D \end{pmatrix}.$$

Nach Induktionsvoraussetzung gilt $\det(M_{i1}) = \det(A_{i1}) \cdot \det(D)$. Das heißt, der obere rechte Block in M_{i1} trägt nicht zur Determinanten bei. Also erhalten wir

$$\det M = \left(\sum_{i=1}^k (-1)^{i+1} a_{i1} \det(A_{i1}) \right) \cdot \det(D) = \det(A) \cdot \det(D),$$

wobei wir im letzten Schritt die Laplace-Entwicklung der Matrix A benutzt haben.

Auch Behauptung (2) beweisen wir nur für obere Dreiecksmatrizen, und zwar induktiv über n mit Hilfe von (1) für $k = 1$. Diesmal trägt nur $i = 1$ bei, und die Matrix A_{11} ist wieder eine obere Dreiecksmatrix. Induktiv folgt

$$\det A = a_{11} \cdot \det(A_{11}) = \prod_{i=1}^n a_{ii}. \quad \square$$

4.19. 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 3.26 berechnen. Wegen Folgerung 4.18 müssen wir unsere Matrix nicht auf strenge Zeilenstufenform bringen; es reicht obere Dreiecksgestalt.

Wir modifizieren das im Beweis von Satz 3.26 beschriebene Verfahren, angewandt auf eine Matrix A , wie folgt. Wir beginnen mit einem Vorfaktor $a_0 = 1$ und erhalten nach dem r -ten Schritt

$$\begin{aligned} \det A &= \dots = a_r \cdot \det \begin{pmatrix} 1 & a_{12} & & \dots & & a_{1,n} \\ 0 & \ddots & \ddots & & & \vdots \\ & \ddots & 1 & a_{r,r+1} & \dots & a_{r,n} \\ \vdots & & 0 & a_{r+1,r+1} & \dots & a_{r+1,n} \\ & & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & a_{n,r+1} & \dots & a_{n,n} \end{pmatrix} \\ &= a_r \cdot \det \begin{pmatrix} a_{r+1,r+1} & \dots & a_{r+1,n} \\ \vdots & & \vdots \\ a_{n,r+1} & \dots & a_{n,n} \end{pmatrix} \end{aligned}$$

Hierbei haben wir Folgerung 4.18 (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 mit-schleppen.

Falls wir im Laufe des Verfahrens eine Spalte überspringen („1. Fall“ im Beweis von Satz 3.26) 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 3.28 (4) verfahren.

Ansonsten ändern wir dann, wenn wir im ersten Schritt tauschen müssen, das Vorzeichen der Vorfaktors wegen Folgerung 4.15 (5). Vor dem Normieren multiplizieren wir den Vorfaktor mit a_{rr} und erhalten $a_r = a_{rr} a_{r-1}$ 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 Dreiecksmatrix mit Einsen auf der Diagonalen (also $a_{11} = \dots = a_{nn} = 1$). Nach Folgerung 4.18 ist diese Determinante 1, also ist a_n die Determinante der ursprünglichen Matrix.

Wir betrachten den Rechenaufwand. Dabei zählen wir nur Multiplikationen und Divisionen, da die anderen Rechenschritte weniger aufwändig sind.

- (1) In der Leibniz-Formel summieren wir über $n!$ Permutationen, und bei jeder müssen wir $(n-1)$ -mal multiplizieren. Der Aufwand ist insgesamt mit $n! \cdot (n-1)$ Multiplikationen sehr hoch.
- (2) Bei der Laplace-Entwicklung benötigt man eigentlich mehr als $n!$ Multiplikationen. Wenn wir alle Determinanten von Untermatrizen zwischenspeichern, reichen $n(2^{n-1} - 1)$ Multiplikationen, der Speicheraufwand ist aber ähnlich hoch. Dafür wird das Verfahren deutlich effizienter, wenn die Matrix viele Nullen enthält.
- (3) Das Gaußverfahren kommt mit $\frac{n^3-3}{3} + n - 1$ Multiplikationen und Divisionen aus. Man kann es etwas abkürzen, indem man die Determinante der letzten 2×2 - oder 3×3 -Matrix mit Laplace ausrechnet — das spart genau einen Rechenschritt.

Für kleine n ergeben sich folgende Zahlen:

n	2	3	4	5	6	...	10
Leibniz	2	12	72	480	3 600	...	32 659 200
Laplace	2	9	28	75	186	...	5 110
Gauß	2	9	22	43	74	...	338

4.20. DEFINITION. Es sei $A \in M_n(R)$. Die *Adjunkte* von A ist definiert als

$$\text{adj } A = ((-1)^{i+j} \det(A_{ji}))_{i,j} \in M_n(R) .$$

Trotz der ähnlichen Namen hat die Adjunkte nichts mit der adjungierten Matrix aus Definition 3.29 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*

$$\det A \in R^\times = \{ r \in R \mid \text{es gibt ein } s \in R \text{ mit } rs = 1 \} ,$$

und in diesem Fall gilt

$$(1) \quad A^{-1} = (\det A)^{-1} \text{adj } A .$$

Wenn $\det A \in R^\times$, ist das Gleichungssystem $A \cdot x = b$ für alle $b \in R^n$ eindeutig lösbar mit

$$(2) \quad x_i = \frac{\det A_i}{\det A} , \quad \text{wobei } A_i = (a_1, \dots, a_{i-1}, b, a_{i+1}, \dots, a_n) \in M_n(R) .$$

Wir nennen R^\times auch die *Einheitengruppe* oder *multiplikative Gruppe* von R , und ihre Elemente *Einheiten*. Wegen Satz 4.12 liefert die Determinante einen Gruppenhomomorphismus $\det: \text{Aut}(V) \rightarrow R^\times$.

BEWEIS. Sei $A'_{ij} \in M_n(\mathbb{k})$ diejenige Matrix, die wir erhalten, indem wir in A die i -te Spalte durch eine Kopie der j -ten ersetzen. Außerdem sei $\text{adj } A = (c_{ij})_{i,j}$. Wir berechnen

$$\begin{aligned} \text{adj } A \cdot A &= \left(\sum_{k=1}^n c_{ik} a_{kj} \right)_{i,j} = \left(\sum_{k=1}^n (-1)^{i+k} \det(A_{ki}) \cdot a_{kj} \right)_{i,j} \\ &= (\det A'_{ij})_{i,j} = \det A \cdot E_n. \end{aligned}$$

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 4.16 (2).

Wenn $A \in M_n(R)$ in R invertierbar ist, folgt $\det A \cdot \det A^{-1} = 1$ aus Satz 4.12 (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

$$x_i = \det A^{-1} (\text{adj } A \cdot b)_i = \frac{1}{\det A} \sum_{j=1}^n (-1)^{i+j} \det(A_{ji}) \cdot b_j = \frac{\det A_j}{\det A}. \quad \square$$

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 3.28 (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 $A = \begin{pmatrix} 1+i & 1+j \\ 1-j & 1-i \end{pmatrix}$ ist invertierbar (Übung), aber es gilt

$$ad - bc = (1+i)(1-i) - (1+j)(1-j) = 2 - 2 = 0.$$

Als letztes wollen wir die Ableitung der Determinante berechnen.

4.23. DEFINITION. Es sei $A \in M_n(R)$, dann definieren wir die *Spur* von A durch

$$\text{tr } A = \sum_{i=1}^n a_{ii} \in R.$$

4.24. FOLGERUNG. *Es sei $\mathbb{k} = \mathbb{R}$ oder \mathbb{C} und $A: (a, b) \rightarrow M_n(\mathbb{k})$ 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

$$\begin{aligned} (\det A)'(t) &= \sum_{j=1}^n \det((a_1, \dots, a_{j-1}, b_j, a_{j+1}, \dots, a_n)) \\ &= \sum_{i,j=1}^n (-1)^{i+j} b_{ij} \cdot \det(A_{ij}) = \sum_{i,j=1}^n b_{ij} c_{ji} = \operatorname{tr}(B \cdot \operatorname{adj} A). \end{aligned}$$

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. \square

4.3. Orientierung reeller Vektorräume

Eine einfache Folgerung aus Satz 4.12 ist die Möglichkeit, endlich erzeugte Vektorräume zu „orientieren“. Wir lassen nur Körper $\mathbb{k} \subset \mathbb{R}$ zu, damit wir vom „Vorzeichen“ eines Elements von \mathbb{k} sprechen können.

4.25. DEFINITION. Sei $\mathbb{k} \subset \mathbb{R}$ ein Körper, und sei V ein n -dimensionaler \mathbb{k} -Vektorraum. Seien (x_1, \dots, x_n) und (y_1, \dots, y_n) zwei Basen von V mit $y_j = \sum_{i=1}^n x_i a_{ij}$. Dann heißen die Basen *gleich orientiert*, wenn die Basiswechselmatrix $A = (a_{ij})_{i,j} \in \operatorname{End}(\mathbb{k}^n)$ positive Determinante hat.

4.26. FOLGERUNG. *Sei V ein \mathbb{k} -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, \dots, b_n) für die $\omega(b_1, \dots, b_n) > 0$ beziehungsweise $\omega(b_1, \dots, b_n) < 0$ gilt.*

BEWEIS. Es seien B, C Basen von V . Wir betrachten den Basiswechsel

$$\begin{array}{ccc} & V & \\ C \nearrow & & \nwarrow B \\ \mathbb{k}^n & \xrightarrow{A} & \mathbb{k}^n \end{array}.$$

Da Basiswechsel nach Proposition 2.77 invertierbar sind, hat A ein Inverses $A^{-1} \in \text{End}(\mathbb{k}^n)$. Also folgt $\det A \neq 0$.

Wenn wir $\omega \in \Lambda^n V^* \neq 0$, dann folgt

$$\omega(c_1, \dots, c_n) = (A^* \omega)(b_1, \dots, b_n) = \det A \cdot \omega(b_1, \dots, b_n).$$

Also sind die Basen B und C genau dann gleich orientiert, wenn $\omega(b_1, \dots, b_n)$ und $\omega(c_1, \dots, c_n)$ das gleiche Vorzeichen haben. Da „hat das gleiche Vorzeichen wie“ eine Äquivalenzrelation auf $\mathbb{k}^\times = \mathbb{k} \setminus \{0\} \subset \mathbb{R}^\times$ 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 $(-b_1, b_2, \dots, b_n)$ und (b_1, \dots, b_n) verschieden orientiert sind. \square

4.27. DEFINITION. Sei $\mathbb{k} \subset \mathbb{R}$ ein Körper. Eine *Orientierung* eines endlich erzeugten \mathbb{k} -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 $F \in \text{Aut } V$ 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.

4.28. BEISPIEL. Auf dem Vektorraum \mathbb{R}^n definieren wir die *Standard-Orientierung* so, dass die Standard-Basis e_1, \dots, e_n positiv orientiert ist. Für die Standard-Determinantenfunktion gilt

$$\omega_n(e_1, \dots, e_n) = 1 > 0,$$

also ist sie positiv bezüglich der Standard-Orientierung.

In Bemerkung 1.70 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 1.70 (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 1.70 (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.

4.29. BEMERKUNG. In den Übungen haben Sie die *orthogonale 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 1.52 erhalten. Für alle $A \in O(n)$ gilt $\det A \in \{\pm 1\}$, da

$$O(n) = \{ A \in M_n(\mathbb{R}) \mid A^t \cdot A = E_n \},$$

siehe auch Proposition 3.34. Außerdem haben wir die *spezielle orthogonale Gruppe* $SO(n)$ 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

$$GL(n, \mathbb{R})^+ = \{ A \in GL(n, \mathbb{R}) \mid \det A > 0 \} \subset GL(n, \mathbb{R})$$

der orientierungserhaltenden Automorphismen. Als nächstes gibt es auch eine Untergruppe

$$\{ A \in GL(n, \mathbb{R}) \mid |\det A| = 1 \} \subset GL(n, \mathbb{R})$$

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 $GL(n, \mathbb{k})$ nur $SL(n, \mathbb{k})$ für alle \mathbb{k} sinnvoll definiert.

Schließlich können wir mit Hilfe der Determinante (und der ersten Cramerschen Regel) die allgemeine lineare Gruppe aus Definition 2.72 auch über beliebigen kommutativen Ringen mit Eins (oder Körpern) leicht charakterisieren, und die spezielle lineare Gruppe wie folgt definieren:

$$\begin{aligned} GL(n, R) &= \{ A \in M_n(R) \mid \det A \in R^\times \}, \\ SL(n, R) &= \{ A \in M_n(R) \mid \det A = 1 \}. \end{aligned}$$

4.4. Zusammenfassung

Determinanten sind wichtige Invarianten linearer Endomorphismen. Im nächsten Kapitel werden wir sie benutzen, um Eigenwerte von Endomorphismen zu bestimmen. Im Zusammenhang mit der mehrdimensionalen Integral-Transformationsformel wird sie auch wieder benötigt.

Um eine Anschauung für die Determinante zu bekommen und einen Zusammenhang zum Spatprodukt im \mathbb{R}^3 herzustellen, haben wir im Abschnitt 4.1 zunächst Determinantenfunktionen als „orientierte Volumina“ eingeführt (wobei wir aber erst im letzten Abschnitt gesehen haben, dass das Vorzeichen eines Volumens etwas mit seiner Orientierung zu tun hat). Die Axiome für Determinanten gehen auf Weierstraß zurück. Den Räumen $\Lambda^k V^*$ mit $k < \dim V$

können Sie später im Zusammenhang mit dem Satz von Stokes oder der de Rham-Kohomologie wieder begegnen.

Im zweiten Abschnitt haben wir Determinanten von Endomorphismen als „Skalierungsfaktoren“ für Volumina eingeführt. Viele Lehrbücher führen Determinanten stattdessen zunächst für Matrizen explizit mit Hilfe der Leibniz-Formel oder des Laplaceschen Entwicklungssatzes ein, müssen dann aber den Produktsatz 4.12 etwas umständlicher beweisen. Bei uns wirkt die Definition zwar etwas komplizierter, hilft uns aber dafür eher, die Bedeutung der Determinanten zu verstehen.

Wir haben verschiedene Rechenverfahren für Determinanten kennengelernt, dabei ist das Gauß-Verfahren für mittelgroße Matrizen über einem Körper das schnellste, falls viele Einträge nicht 0 sind. Wenn wir (wie im nächsten Abschnitt) über Ringen arbeiten müssen, oder wenn eine Matrix nur wenige von 0 verschiedene Einträge enthält, bevorzugen wir die Laplace-Entwicklung.

Die Cramerschen Regeln zum Invertieren von Matrizen und zum Lösen von Gleichungssystemen sind aufgrund ihres hohen Rechenaufwandes eher von theoretischem Interesse, wie wir bei der Ableitung der Determinanten gesehen haben. Das gleiche gilt für die Leibniz-Formel. Immerhin motiviert die Cramersche Regel den Namen „Determinante“ als Invariante, die die eindeutige Lösbarkeit eines quadratischen linearen Gleichungssystems bestimmt („determiniert“).

Im letzten Abschnitt haben wir gesehen, wie das Vorzeichen der Determinanten über \mathbb{R} uns die Möglichkeit gibt, von Orientierungen zu sprechen. Auch dieser Begriff wird Ihnen noch häufiger begegnen. Außerdem haben wir einige typische Matrixgruppen kennengelernt.

Notation

\in , 3 $\{\dots\}$, 4 \emptyset , 4 \subset , 5 \subsetneq , 5 \cap , 5 \cup , 5 \setminus , 6 \times (Mengen), 6 (\dots) , 6 \mathcal{P} , 6 $\{\dots \dots\}$, 6 $F: M \rightarrow N$, 6 Abb, 7 im , 7 F^{-1} , 7 id , 7 \circ , 7 $F _U$, 8 \mathbb{N} , 10 \underline{n} , 10 $\overline{\mathbb{N}}$, 10 $\#$, 11 \leq , 11 \mathbb{Z} , 18 \mathbb{Q} , 20 \mathbb{R} , 21 \mathbb{R}^n , 21 $\langle \cdot, \cdot \rangle$, 22 $\ \cdot\ $, 22 \angle , 22 i , 24 \mathbb{C} , 24	Re , 25 Im , 25 $\bar{\cdot}$, 25 $ \cdot $, 26 \arg , 27 \times (Vektoren), 29 \mathbb{H} , 31 j, k , 33 Aut , 39 $\equiv \text{mod}$, 41 \mathbb{Z}/n , 41 \mathbb{k}^\times , 44 $a n$, 45 ggT , 46 $\text{Hom}_R, {}_R \text{Hom}$, 50 $\text{Iso}_R, {}_R \text{Iso}$, 52 $\text{End}_R, {}_R \text{End}$, 52 $\text{Aut}_R, {}_R \text{Aut}$, 52 $M^*, {}^*M$, 53 \ker , 55 $U + V$, 59 $U \oplus V$, 59 M^I , 62 R^n , 62 $\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix}$, 62 e_1, \dots, e_n , 62 δ_{ij} , 62 ${}^n R$, 63 (r_1, \dots, r_n) , 63 $\varepsilon_1, \dots, \varepsilon_n$, 63 $\sum_{i=1}^n$, 63 $\exists!$, 64
---	--

$\langle A \rangle$, 66
 $\begin{pmatrix} f_{11} & \cdots & f_{1n} \\ \vdots & & \vdots \\ f_{m1} & \cdots & f_{mn} \end{pmatrix}$, 69
 $M_{m,n}(R)$, 69
 $M_n(R)$, 72
 E_n , 72
 F^{-1} , 72
 $GL(n, R)$, 72
 Bv , 73
 Bf_C , 74
 $B \text{id}_C$, 74
 $R^{(I)}$, 76
 $R[X]$, 76
 $R[[X]]$, 76
 ${}^I R$, 77
 \dim , 82
 A^t , 86
 rg , 86
 rg_S, rg_Z , 86
 $a_0 + U$, 88
 P_{ij} , 91
 $M_i(k)$, 91
 $E_{ij}(k)$, 91
 A^* , 96
 vol , 101
 $\Lambda^k M^*$, 103
 S_n , 105
 sign , 105
 F^* , 108
 \det , 109
 R^\times , 115
 $O(n), SO(n)$, 119
 $GL(n, \mathbb{R})^+$, 119
 $SL(n, \mathbb{R})$, 119

Stichwortverzeichnis

- Abbildung, 6
 - Basis-, 67, 73
 - induzierte, 15
 - Koordinaten-, 67, 73
 - lineare, 48
 - multilineare, 103
 - Null-, 51
 - Quotienten-, 15, 56
 - Umkehr-, 9, 39
- Abbildungsmatrix, 74, 85
- abgeschlossen, 54
- Ableitung, 51
- Absolutbetrag, 22
 - auf \mathbb{C} , 26
- Addition, 13, 40
 - Matrix-, 69, 70
 - Vektor-, 21, 27
- additiv, 48
- Adjunkte, 115
- Äquivalenzklasse, 15, 20
- Äquivalenzrelation, 9, 14, 16, 20, 41, 88
- Algorithmus
 - Euklidischer, **46**
 - Gauß-Verfahren, **92**, 94–96
- alternierend, 103
- antisymmetrisch, 29, 103
- Argument, 27
- Assoziativgesetz, 14, 18, 20, 24, 37, 40
- Automorphismus, 39
 - Anti-, 32
 - Modul-, 52
 - orientierungserhaltender, 118
 - orientierungsumkehrender, 118
 - Vektorraum-, 52
 - volumenerhaltender, 119
- Axiome
 - Äquivalenzrelation, 14
 - Gruppe, 37
 - Homomorphismus, 48
 - Körper, 42
 - Lineare Abbildung, 48
 - Mengenlehre, 5
 - Modul, 47
 - Ordnung, 11
 - Peano- für \mathbb{N} , 10
 - Ring, 40
 - Untermodul, 54
 - Vektorraum, 47
- Basis, 66, 77, 80–82
 - angeordnete, 66
 - duale, 68
 - Orthonormal-, 97
 - Standard-, 62, 76, 118
 - unitäre, 97
 - quaternionisch, 97
- basisunabhängig, 110
- Basiswechsel, 74, 117
- Beweis
 - indirekter, 4
- bijektiv, 7, 8
- Bild, 7, 55, 89, 95
- Charakteristik, 44
- Cramersche Regel, **115**
- definit
 - positiv, 22
- Definition
 - rekursive, 10, 12, 63
- Definitionsbereich, 7
- Determinante, 109, 110–119
- Determinantenfunktion, 103, 117
 - Standard-, 105, 107, 118
- Differenz
 - von Mengen, 6
- Dimension, 82
- Dimensionsformel
 - Komplement, 83
 - lineare Abbildung, 85
 - Summe, 84
- disjunkt, 5
- Distributivgesetz, 14, 18, 20, 24, 40, 47
- Division
 - mit Rest, 41, 45

- Drehung, 33, 35
- Dreiecksgestalt, 113
 - strikte, 113
- dual, 61
- Durchschnitt, 5
- Eigenschaft
 - universelle
 - freier Modul, 64, 67, **77**
 - Koprodukt, 60
 - Produkt, 61
 - Quotient, 15, 57
- Einheit, 116
- Eins, 40
- Einschränkung, 8
- Element, 3
 - Eins-, 40
 - inverses, 19, 20, 37, 38
 - neutrales, 14, 18, 20, 24, 37, 38, 40, 54
 - Null-, 40, 48
- endlich, 11
- endlich erzeugt, 66
- endlichdimensional, 82, 88
- Endomorphismus
 - Modul-, 52
 - Vektorraum-, 52
- Erzeugendensystem, 66, 77, 80–82
- Erzeugnis, 66, 77
- Euklidischer Algorithmus, **46**
- Familie, 76
 - endliche, 76
- Form
 - alternierende, 103
 - zurückgeholte, 108
- Gauß-Verfahren, **92**, 94–96, 114
- Gleichheit
 - Abbildungen, 7
 - gleichmächtig, 9
- Gleichungssystem
 - lineares, 88–96
 - homogenes, 89
 - inhomogenes, 89
- Graph, 6
- Gruppe, 37
 - abelsche, 37, 40
 - additive, 38, 40
 - Automorphismen-
 - Modul, 53
 - Einheiten-, 116
 - lineare
 - allgemeine, 72, 75, 119
 - spezielle, 119
 - multiplikative, 44, 116
 - orthogonale, 119
 - spezielle, 119
 - symmetrische, 105
 - Unter-, 55
 - zyklische
 - Ordnung n , 42
 - unendliche, 38
- Halbordnung, 11
- homogen, 48
 - positiv, 101
- Homomorphismus
 - Modul-, 48
 - Vektorraum-, 50
- Identität, 7, 39
 - Graßmann-, 29, 34
 - Jacobi-, 29
- Imaginärteil, 25, 31
- Induktion
 - vollständige, 12
- injektiv, 7, 8
- Inklusion, 8
- Inverses
 - additives, 19, 24
 - multiplikatives, 19, 21, 24
- Isometrie
 - der Ebene, 28
 - des Raumes, 35
 - lineare, 119
 - orientierungserhaltende, 119
- isomorph, 82
- Isomorphismus
 - Modul-, 52
 - Vektorraum-, 52
- Kern, 55, 89, 95
- Klassifikation, 82
- Körper, 42
 - angeordneter, 21
 - archimedisch, 21
 - vollständig, 21
 - endlicher, 45
 - Schief-, 42
 - Teil-, 55
- Kommutativgesetz, 14, 18, 20, 24, 37, 40
- Komplement, 6, 59, 83
- kongruent, 41
- Konjugation
 - komplexe, 25
 - quaternionische, 31
- Koordinaten, 67
- Kürzungsregel, 14, 19, 38, 44
- Laplace-Entwicklung, 105, **112**
- Leibniz-Formel, **110**, 111
- linear, 22, 29, 48

- linear abhängig, 66, 95
- linear unabhängig, 66, 77, 79–82, 95
- Linearisierung, 51
- Linearkombination, 50, 63, 76
- Lösung
 - allgemeine, 90
 - spezielle, 90
- Mächtigkeit, 11
- Matrix, 69
 - Abbildungs-, 74, 85
 - adjungierte, 96
 - Basiswechsel-, 74, 75, 117
 - Block-, 85, 113
 - darstellende
 - Abbildung, 74
 - Dreiecks-, 113
 - Einheits-, 72
 - Elementar-, 91, 95
 - inverse, 72, 95, 115
 - invertierbare, 72, 95, 115
 - quadratische, 72
 - transponierte, 86
- Menge, 3, 4
 - endliche, 11
 - Lösungs-, 88
 - unendliche, 11
- Methode der kleinsten Quadrate, 98
- Modul
 - dualer, 53, 68
 - freier, 66, 67–68, 76
 - Links-, 47, 71
 - Null-, 47
 - Quotienten-, 56
 - Rechts-, 47, 71
 - unitärer, 47
 - Unter-, 54
- modulo, 41, 56
- multilinear, 103
- Multiplikation, 13, 40
 - komplexe, 24
 - geometrische Interpretation, 27
 - Matrix-, 69, 70–75
 - Quaternionen-, 31
 - skalare, 21, 47, 70
 - Verträglichkeit, 47
- multiplikativ, 26
- Norm
 - auf \mathbb{C} , 26
 - Euklidische, 22
- Normalform
 - lineare Abbildung, 85
- Null, 40, 48
- Nullmodul, 47
- Nullteiler, 44
- Ordnung, 11, 25
- Orientierung, 30, 118
 - Standard-, 118
- orientierungserhaltend, 118, 119
- orientierungsumkehrend, 118
- Paar, 6
- parallel, 88
- Parallelotop, 30, 101
- Peano-Axiome, 10
- Permutation, 105
- Polardarstellung, 27
- Polynom, 76
- Potenz, 13
- Potenzmenge, 6, 14
- Potenzreihe
 - formale, 76
 - konvergente, 77
- Primzahl, 45
- Produkt
 - kartesisches, 6, 16
 - Kreuz-, 29, 118
 - Skalar-
 - Standard-, 22, 96
 - Spat-, 29, 103, 118
- Quadrate
 - Methode der kleinsten, 98
- Quaternionen, 31, 32–36
- Quotientenmenge, 15, 17
- Quotientenraum, 56, 88
- Rang, 86
 - Spalten-, 86
 - Zeilen-, 86
- Realteil, 25, 31
- Regel
 - Cramer, **115**
 - Sarrus, 111, 118
- Relation, 11
 - Äquivalenz-, 9, 14, 16, 20, 41, 88
 - antisymmetrisch, 11
 - reflexiv, 11, 14
 - symmetrisch, 14
 - transitiv, 11, 14
- Repräsentanten, 15
- Restklasse, 41
- Ring, 40
 - Endomorphismen, 53
 - kommutativer, 40
 - Matrix-, 72
 - mit Eins, 40
 - Null-, 41
 - unitärer, 40

- Unter-, 55
- Russelsche Antinomie, **4**
- Sarrussche Regel, 111, 118
- Satz, 4
 - Basisaustausch-, **81**
 - Basisergänzungs-, **80**
 - Cauchy-Schwarz-Ungleichung, 23
 - Cosinus-, 24
 - Euklidischer Algorithmus, **46**
 - Fundamental- der Algebra, 26
 - Gauß-Verfahren, **92**, 94–96, 114
 - Homomorphie-, **57**
 - Laplace-Entwicklung, 105, **112**
 - Leibniz-Formel, **110**, 111
 - Methode der kleinsten Quadrate, **98**
 - Rang-, **85**, 86, 93
 - Steinitz
 - Basisaustausch-, **81**
 - Basisergänzungs-, **80**
 - scherungsinvariant, 101
 - Schiefkörper, 42
 - Seite
 - linke, 88
 - rechte, 88
 - Signum, *105*
 - Skalarprodukt
 - Standard-, *22*, 96
 - komplexes, 96
 - quaternionisches, 96
 - Spiegelung, 27
 - Punkt-, 35
 - Spin, 35
 - Spur, *116*
 - subadditiv, 26
 - Summe, 63
 - direkte, 84
 - von Untermoduln, *59*
 - direkte, *59*, 84
 - surjektiv, 7, 8
 - Symbol
 - Kronecker-, 62
 - symmetrisch, 22
- Teiler, 45
 - größter gemeinsamer, 46
- Teilmenge, 5
 - echte, 5
- total (Ordnung), 11
- Transposition, 106
- Tupel, 6
- Umkehrabbildung, 9, 39
- undendlichdimensional, 82
- unendlichdimensional, 88
- Ungleichung
 - Cauchy-Schwarz-, 23
- Untermodul, *54*
 - komplementärer, *59*
- Unterraum, *54*
 - affiner, 88
 - komplementärer, *59*, 83
- Urbild, 7, 89
- Vektor
 - Basis-
 - Standard-, *62*
 - Null-, 22, 48
 - Spalten-, 62
 - Zeilen-, 63
- Vektorraum, *47*
 - dualer, *53*
 - Quotienten-, *56*
 - Unter-, *54*
- Vereinigung, 5
- Verkettung, 7, 39
- Verknüpfungen, 13
- Verschiebung, 35
- Verträglichkeit
 - der Multiplikation, 47
- Volumen, 30, 101
- Vorzeichen
 - Permutation, *105*
- Wertebereich, 7
- Winkel, *22*, 33
- wohldefiniert, 16
- Wurzel, 28
- Zahlen
 - ganze, *18*
 - komplexe, *24*, 25–28
 - Polardarstellung, 27
 - natürliche, 14
 - rationale, *20*
 - reelle, 21
- Zeilenstufenform, *91*, 93–96
 - strenge, *91*, 95
- Zeilenumformung
 - elementare, *91*, 92