Lineare Algebra

Sebastian Thomas

Manuskript (provisorisch)
Sommersemester 2013

Carl von Ossietzky Universität Oldenburg
Institut für Mathematik

Version: 28. Januar 2014.

Dieses Vorlesungsmanuskript entstand während der Veranstaltung *Lineare Algebra*; gehalten an der Carl von Ossietzky Universität im Sommersemester 2013. Es befindet sich momentan noch im Aufbau.

Inhaltsverzeichnis

Vorwort

Dieses Manuskript ist provisorisch.
Mein Dank für Korrekturen gilt Thu Huong Monika Nguyen.
Für weitere Hinweise auf Fehler und Unklarheiten bin ich dankbar.

Oldenburg, 31. Juli 2013
Sebastian Thomas

Kapitel I

Grundlagen

1 Mengen und Abbildungen

In diesem ersten Abschnitt wiederholen wir kurz einige Konzepte der naiven Mengenlehre.

Mengen und Teilmengen

Unter einer *Menge* verstehen wir eine „Zusammenfassung von bestimmten, wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen“. Ist X eine Menge, so bezeichnen wir diejenigen Objekte, die durch X zusammengefasst werden, als die *Elemente* von X. Ist x ein Element von X, so schreiben wir $x \in X$. Ist x kein Element von X, so schreiben wir $x \notin X$. Mengen X und Y sind gleich, geschrieben $X = Y$, falls sie die gleichen Elemente enthalten, d.h. falls aus $x \in X$ stets $x \in Y$ folgt und falls aus $x \in Y$ stets $x \in X$ folgt.
Mengen werden durch Beschreibungen oder Aufzählungen notiert. Ist X eine Menge bestehend aus genau denjenigen Objekten, die eine gegebene Eigenschaft φ erfüllen, so schreiben wir $\{x \mid x \text{ erfüllt } \varphi\} := X$. Für gegebene Objekte $a_1, a_2, a_3, \dots$ schreiben wir $\{a_1, a_2, a_3, \dots\} := \{x \mid x = a_1 \text{ oder } x = a_2 \text{ oder } x = a_3 \text{ oder } \dots\}$. Nicht jede Eigenschaft beschreibt eine Menge (Stichwort „Russelsches Paradoxon“).
Die Menge, welche keine Elemente enthält, heißt *leere Menge* und wird mit $\emptyset$ bezeichnet.
Außerdem gehen wir in diesem Kurs davon aus, dass wir die Mengen der *natürlichen Zahlen*, der *natürlichen Zahlen mit Null*, der *ganzen Zahlen*, der *rationalen Zahlen* bzw. der *reellen Zahlen*, in dieser Reihenfolge bezeichnet mit $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$ bzw. $\mathbb{R}$, kennen.
Es sei eine Menge X gegeben. Eine *Teilmenge* von X ist eine Menge U so, dass X alle Elemente von U enthält, d.h. so, dass aus $u \in U$ stets $u \in X$ folgt. Eine Teilmenge U von X heißt *echt* (oder *strikt*), falls $U \neq X$ gilt. Ist U eine Teilmenge von X, so schreiben wir $U \subseteq X$. Ist U keine Teilmenge von X, so schreiben wir $U \nsubseteq X$. Ist U eine echte Teilmenge von X, so schreiben wir $U \subset X$. Für eine Eigenschaft φ schreiben wir $\{x \in X \mid x \text{ erfüllt } \varphi\} := \{x \mid x \in X \text{ und } x \text{ erfüllt } \varphi\}$ für die Teilmenge derjenigen Elemente von X, welche φ erfüllt. Die Menge aller Teilmengen von X heißt *Potenzmenge* von X und wird mit $\mathrm{Pot}(X) := \{U \mid U \subseteq X\}$ bezeichnet.

Mengenoperationen

Es seien X und Y Mengen. Die Menge $X \cap Y := \{x \mid x \in X \text{ und } x \in Y\}$ heißt *Schnitt* von X und Y. Die Menge $X \cup Y := \{x \mid x \in X \text{ oder } x \in Y\}$ heißt *Vereinigung* von X und Y. Ist $X \cap Y = \emptyset$, so sagen wir, dass X und Y *disjunkt voneinander* sind, und schreiben in diesem Fall auch $X \dot\cup Y := X \cup Y$ für die *disjunkte Vereinigung* von X und Y. Es gelten jeweils Assoziativgesetze und Kommutativgesetze für Schnitt und Vereinigung, und Schnitt und Vereinigung sind miteinander verträglich über die Distributivgesetze.
Die Menge $X \setminus Y := \{x \mid x \in X \text{ und } x \notin Y\}$ heißt *Differenz* von X und Y. Die de Morganschen Regeln beschreiben eine Kompatibilität von Differenz, Schnitt und Vereinigung.
Zu Objekten x, y können wir das *geordnete Paar* von x und y bilden, es wird als (x, y) notiert. Für Objekte x, x', y, y' gilt genau dann $(x, y) = (x', y')$, wenn $x = x'$ und $y = y'$ ist. Für Mengen X und Y heißt die Menge $X \times Y := \{(x, y) \mid x \in X, y \in Y\}$ das *kartesische Produkt* von X und Y.

Abbildungen

Es seien Mengen X und Y gegeben. Eine *Abbildung* (oder *Funktion*) von X nach Y besteht aus X und Y zusammen mit einer Teilmenge f von $X \times Y$ so, dass es für jedes $x \in X$ genau ein $y \in Y$ mit $(x, y) \in f$ gibt. Unter Missbrauch der Notation bezeichnen wir sowohl die besagte Abbildung als auch die Teilmenge von $X \times Y$ mit f. Die Menge X wird *Startmenge* von f genannt, die Menge Y wird *Zielmenge* von f genannt. Für eine Abbildung f mit Startmenge X und Zielmenge Y schreiben wir $f\colon X \to Y$. Für $(x, y) \in f$ heißt y das *Bild* von x unter f, es heißt x ein *Urbild* von y unter f, und wir schreiben $f(x) := y$ oder $x \mapsto f(x)$. Die *Menge aller Abbildungen von X nach Y* bezeichnen wir mit $\operatorname{Map}(X, Y) := \{f \mid f \text{ ist eine Abbildung von } X \text{ nach } Y\}$.
Wir betonen, dass zu einer Abbildung $f\colon X \to Y$ die Startmenge X und die Zielmenge Y dazugehören. Insbesondere sind Abbildungen $f\colon X \to Y$ und $f'\colon X' \to Y'$ genau dann gleich, d.h. es gilt $f = f'$, wenn $X = X'$, $Y = Y'$ und $f(x) = f'(x)$ für alle $x \in X$ gilt.
Für Abbildungen $f\colon X \to Y$ und $g\colon Y \to Z$ heißt $g \circ f\colon X \to Z$, $x \mapsto g(f(x))$ das *Kompositum* von f und g. Die Komposition von Abbildungen ist assoziativ, aber nicht kommutativ.
Für jede Menge X haben wir die Abbildung $\mathrm{id} = \mathrm{id}_X\colon X \to X$, $x \mapsto x$, genannt *Identität* (oder *identische Abbildung*) auf X. Für jede Abbildung $f\colon X \to Y$ ist $f \circ \mathrm{id}_X = \mathrm{id}_Y \circ f = f$.
Eine Abbildung $f\colon X \to Y$ heißt *invertierbar*, falls es eine *inverse Abbildung* zu f gibt, d.h. eine Abbildung $g\colon Y \to X$ mit $g \circ f = \mathrm{id}_X$ und $f \circ g = \mathrm{id}_Y$. Da es zu f höchstens eine inverse Abbildung gibt, ist diese durch f eindeutig festgelegt und wird mit f^{-1} bezeichnet.

Injektivität und Surjektivität

Es sei eine Abbildung $f\colon X \to Y$ gegeben. Wir sagen, dass f *injektiv* ist, falls f verschiedene Elemente aus X auf verschiedene Elemente in Y abbildet, dass f *surjektiv* ist, falls jedes Element aus Y das Bild eines Elements aus X unter f ist, und dass f *bijektiv* ist, falls f injektiv und surjektiv ist. Es ist f genau dann invertierbar, wenn f bijektiv ist.
Für $U \subseteq X$ heißt $f(U) := \{f(u) \mid u \in U\} := \{y \in Y \mid \text{es gibt ein } u \in U \text{ mit } y = f(u)\}$ das *Bild* von U unter f. Der Spezialfall $\operatorname{Im} f := f(X)$ wird auch das *Bild* von f genannt. Für $V \subseteq Y$ heißt $f^{-1}(V) := \{x \in X \mid f(x) \in V\}$ das *Urbild* von V unter f. Für ein $y \in Y$ heißt $f^{-1}(\{y\})$ die *Faser* von f über y.

Familien

Es seien Mengen I und X gegeben. Eine *Familie* in X über I ist eine Teilmenge x von $I \times X$ so, dass es für alle $i \in I$ genau ein $y \in X$ mit $(i, y) \in x$ gibt. Die Menge I wird *Indexmenge* von x genannt, ihre Elemente heißen *Indizes* von x. Für $(i, y) \in x$ heißt y die *Komponente* von x an der Stelle i, wir schreiben $x_i := y$. Für eine Familie x in X über I schreiben wir auch $(x_i)_{i \in I} := x$. Die *Menge aller Familien in X über I* bezeichnen wir mit $X^I := \{x \mid x \text{ ist eine Familie in } X \text{ über } I\}$. Für $n \in \mathbb{N}_0$ schreiben wir auch $X^n := X^{[1,n]}$, wobei $[1, n] = \{i \in \mathbb{Z} \mid 1 \leq i \leq n\}$ das *ganzzahlige* Intervall bezeichne, und notieren die Elemente als $(x_1, \ldots, x_n) := (x_i)_{i \in [1,n]}$.
Eine Familie in X über I ist also, bis auf die Indexnotation, im Wesentlichen dasselbe wie eine Abbildung von I nach X; bei Abbildungen fassen wir lediglich noch Start- und Zielmenge als Bestandteile auf, bei Familien nicht. Dies ermöglicht uns, auch von einer Familie über I zu sprechen, ohne dass wir explizit angeben müssen, in welcher Menge X diese Familie liegt. Ferner gilt $U^I \subseteq X^I$ für eine Teilmenge U von X (etwa $\mathbb{Q}^n \subseteq \mathbb{R}^n$ für $n \in \mathbb{N}_0$), aber $\operatorname{Map}(I, U) \nsubseteq \operatorname{Map}(X, U)$. Familien x und y über I sind genau dann gleich, d.h. es gilt $x = y$, wenn $x_i = y_i$ für alle $i \in I$ ist.
Nichtsdestotrotz fassen wir Familien hin und wieder auch als Abbildungen auf (etwa wenn wir komponieren wollen), d.h. wir gehen von einer Familie x in X über I zur entsprechenden Abbildung $I \to X$, $i \mapsto x_i$ über. Diese Abbildung wird dann unter Missbrauch der Notation auch wieder mit x bezeichnet. Dies ermöglicht uns etwa, für eine gegebene Abbildung $f\colon X \to Y$ von der Familie $f \circ x$ in Y über I zu sprechen: das ist gerade die Familie, welche der Abbildung $f \circ x\colon I \to Y$ entspricht, also der Familie mit den Stellen $(f \circ x)_i = f(x_i)$ für $i \in I$.

2 Äquivalenzrelationen und Quotientenmengen

Ziel dieses Abschnitts ist es, den Begriff der (absoluten) Gleichheit von Objekten abzuschwächen und zu formalisieren, was wir unter einer „Gleichheit unter einem gewissen Gesichtspunkt“ verstehen. Hierzu dient der

Begriff der Äquivalenzrelation.

Relationen

Äquivalenzrelationen sind spezielle Relationen, welche wir nun zunächst einführen werden.

(1.1) Definition (Relation)**.** Es sei eine Menge X gegeben. Eine *Relation* (genauer *binäre Relation*) auf X ist eine Teilmenge r von $X \times X$. Falls $(x, y) \in r$, so sagen wir, *dass x bzgl. r in Relation zu y steht* und schreiben $x\ r\ y$.

(1.2) Beispiel.

(a) Für $m, n \in \mathbb{N}$ gelte genau dann $m < n$, wenn es ein $p \in \mathbb{N}$ mit $n = p + m$ gibt. Die Relation $<$ auf $\mathbb{N}$ ist die übliche *Striktordnung* auf den natürlichen Zahlen. Als Teilmenge von $\mathbb{N} \times \mathbb{N}$ ist $<$ gegeben durch $\{(m, n) \in \mathbb{N} \times \mathbb{N} \mid \text{es existiert ein } p \in \mathbb{N} \text{ mit } n = p + m\}$.

(b) Für $m, n \in \mathbb{N}$ gelte genau dann $m \mid n$, lies m *teilt* n, wenn ein $q \in \mathbb{N}$ existiert mit $n = qm$. Die Relation $\mid$ auf $\mathbb{N}$ wird *Teilbarkeitsrelation* (oder *Teilbarkeit*) auf $\mathbb{N}$ genannt. Als Teilmenge von $\mathbb{N} \times \mathbb{N}$ ist $\mid$ gegeben durch $\{(m, n) \in \mathbb{N} \times \mathbb{N} \mid \text{es existiert ein } q \in \mathbb{N} \text{ mit } n = qm\}$.

(c) Auf jeder Menge X haben wir folgende Relation: Für $x, y \in X$ gelte genau dann $x = y$, wenn x und y gleich sind. Wir nennen $=$ die *Gleichheitsrelation* (oder *Gleichheit*) auf X. Als Teilmenge von $X \times X$ ist $=$ gegeben durch $= = \{(x, x) \mid x \in X\}$.

(d) Auf jeder Menge X haben wir die *Allrelation*, welche als Teilmenge von $X \times X$ durch $\{(x, y) \mid x, y \in X\} = X \times X$ gegeben ist.

Wie in Beispiel (1.2)(a), (b), (c) schon angedeutet, ist es üblich, Relationen durch Angabe der Eigenschaft, welche für die in Relation stehenden Elemente erfüllt ist, zu definieren. Dies ist äquivalent zur Angabe der Teilmenge des kartesischen Produkts und meistens etwas leserlicher.

(1.3) Definition (Transitivität, Reflexivität, Symmetrie)**.** Es seien eine Menge X und eine Relation r auf X gegeben.

(a) Wir sagen, dass r *transitiv* ist, falls für $x, y, z \in X$ aus $x\ r\ y$ und $y\ r\ z$ stets $x\ r\ z$ folgt.

(b) Wir sagen, dass r *reflexiv* ist, falls für $x \in X$ stets $x\ r\ x$ gilt.

(c) Wir sagen, dass r *symmetrisch* ist, falls für $x, y \in X$ aus $x\ r\ y$ stets $y\ r\ x$ folgt.

(1.4) Beispiel.

(a) Die übliche Striktordnung $<$ auf den natürlichen Zahlen ist transitiv, aber nicht reflexiv und nicht symmetrisch.

(b) Die Teilbarkeitsrelation $\mid$ auf den natürlichen Zahlen ist transitiv und reflexiv, aber nicht symmetrisch.

(c) Für jede Menge X ist die Gleichheitsrelation $=$ auf X transitiv, reflexiv und symmetrisch.

Beweis.

(a) Es seien $m, n, p \in \mathbb{N}$ mit $m < n$ und $n < p$ gegeben. Dann gibt es $q, r \in \mathbb{N}$ mit $n = q + m$ und $p = r + n$. Es folgt $p = r + n = r + q + m$, also $m < p$. Folglich ist $<$ transitiv.

Für kein $m \in \mathbb{N}$ gibt es ein $p \in \mathbb{N}$ mit $m = p + m$, d.h. es gilt $m < m$ für kein $m \in \mathbb{N}$. Insbesondere ist $<$ nicht reflexiv.

Es seien $m, n \in \mathbb{N}$ mit $m < n$ gegeben. Dann gibt es ein $p \in \mathbb{N}$ mit $n = p + m$. Gäbe es ein $q \in \mathbb{N}$ mit $m = q + n$, so wäre $m = q + n = q + p + m$ und damit $q + p = 0$. Da mit $p, q \in \mathbb{N}$ dann aber auch $0 = q + p \in \mathbb{N}$ sein müsste, ist dies ein Widerspruch. Folglich gilt $n < m$ nicht. Insbesondere ist $<$ nicht symmetrisch.

(b) Siehe Aufgabe 3(a). □

Äquivalenzrelationen

(1.5) Definition (Äquivalenzrelation)**.** Es sei eine Menge X gegeben. Eine *Äquivalenzrelation* auf X ist eine Relation auf X, welche transitiv, reflexiv und symmetrisch ist.

(1.6) Beispiel.

(a) Für $x, y \in \mathbb{R}$ gelte genau dann $x \; c \; y$, wenn $x = y$ oder $x = -y$ ist. Dann ist c eine Äquivalenzrelation auf $\mathbb{R}$.

(b) Für $x, y \in \mathbb{Z}$ gelte genau dann $x \equiv_2 y$, wenn x und y entweder beide gerade oder beide ungerade sind. Dann ist $\equiv_2$ eine Äquivalenzrelation auf $\mathbb{Z}$.

(c) Es ist $\{(1,1),(2,2),(3,3),(4,4),(1,2),(2,1),(1,4),(4,1),(2,4),(4,2)\}$ eine Äquivalenzrelation auf $[1,4]$.

(d) Für jede Menge X ist die Gleichheitsrelation $=$ auf X eine Äquivalenzrelation auf X.

Beweis.

(a) Es seien $x, y, z \in \mathbb{R}$ mit $x \; c \; y$ und $y \; c \; z$ gegeben. Dann gilt $x = y$ oder $x = -y$, sowie $y = z$ oder $y = -z$. Wir erhalten

$$x = \begin{cases} y, & \text{falls } x = y, \\ -y, & \text{falls } x = -y \end{cases} \Bigg\} = \begin{cases} z, & \text{falls } x = y,\ y = z, \\ -z, & \text{falls } x = y,\ y = -z, \\ -z, & \text{falls } x = -y,\ y = z, \\ -(-z), & \text{falls } x = -y,\ y = -z \end{cases} \Bigg\}$$

$$= \begin{cases} z, & \text{falls } x = y,\ y = z \text{ oder } x = -y,\ y = -z, \\ -z, & \text{falls } x = y,\ y = -z \text{ oder } x = -y,\ y = -z. \end{cases}$$

Also ist $x = z$ oder $x = -z$, und damit $x \; c \; z$. Folglich ist c transitiv.

Da für alle $x \in \mathbb{R}$ wegen $x = x$ auch $x \; c \; x$ gilt, ist c reflexiv.

Es seien $x, y \in \mathbb{R}$ mit $x \; c \; y$ gegeben. Dann gilt $x = y$ oder $x = -y$, also auch $y = x$ oder $y = -x$ und damit $y \; c \; x$. Folglich ist c symmetrisch.

Insgesamt ist c eine Äquivalenzrelation auf $\mathbb{R}$.

(b) Es seien $x, y, z \in \mathbb{Z}$ mit $x \equiv_2 y$ und $y \equiv_2 z$ gegeben. Wenn x gerade ist, dann ist wegen $x \equiv_2 y$ auch y gerade und wegen $y \equiv_2 z$ dann auch z gerade. Wenn x ungerade ist, dann ist wegen $x \equiv_2 y$ auch y ungerade und wegen $y \equiv_2 z$ dann auch z ungerade. Also sind x und z entweder beide gerade oder beide ungerade, d.h. es gilt $x \equiv_2 z$. Folglich ist $\equiv_2$ transitiv.

Da x entweder gerade oder ungerade ist, ist $\equiv_2$ reflexiv.

Die Symmetrie von $\equiv_2$ folgt aus der symmetrischen Definition von $\equiv_2$.

Insgesamt ist $\equiv_2$ eine Äquivalenzrelation auf $\mathbb{Z}$. □

Die bzgl. einer Äquivalenzrelation in Relation stehenden Elemente wollen wir nun zu Teilmengen zusammenfassen:

(1.7) Definition (Äquivalenzklasse)**.** Es seien eine Menge X und eine Äquivalenzrelation c auf X gegeben. Für $x \in X$ heißt $[x] = [x]_c := \{\tilde{x} \in X \mid \tilde{x} \; c \; x\}$ die *Äquivalenzklasse* von x in X bzgl. c, und es heißt x ein *Repräsentant* von $[x]_c$.

Wir greifen die Beispiele aus (1.6) noch einmal auf:

(1.8) Beispiel.

(a) Für $x, y \in \mathbb{R}$ gelte genau dann $x \; c \; y$, wenn $x = y$ oder $x = -y$ ist. Dann ist $[x]_c = \{x, -x\}$ für $x \in \mathbb{R}$.

(b) Für $x, y \in \mathbb{Z}$ gelte genau dann $x \equiv_2 y$, wenn x und y entweder beide gerade oder beide ungerade sind. Dann ist $[0]_{\equiv_2} = 2\mathbb{Z} = \{2q \mid q \in \mathbb{Z}\}$ und $[1]_{\equiv_2} = 2\mathbb{Z} + 1 = \{2q + 1 \mid q \in \mathbb{Z}\}$.

(c) Es sei $c := \{(1,1),(2,2),(3,3),(4,4),(1,2),(2,1),(1,4),(4,1),(2,4),(4,2)\}$. Dann ist $[1]_c = [2]_c = [4]_c = \{1,2,4\}$ und $[3]_c = \{3\}$.

(d) Es sei X eine Menge. Dann ist $[x]_= = \{x\}$ für alle $x \in X$.

(1.9) Proposition. Es seien eine Menge X und eine Äquivalenzrelation c auf X gegeben.

(a) Für $x \in X$ ist $x \in [x]_c$.

(b) Für $x, y \in X$ sind die folgenden Bedingungen äquivalent:

(i) Es ist $[x]_c = [y]_c$.

(ii) Es ist $[x]_c \subseteq [y]_c$.

(iii) Es gilt $x \; c \; y$.

Beweis.

(a) Da c reflexiv ist, haben wir $x \; c \; x$ und damit $x \in [x]$ für alle $x \in X$.

(b) Es seien $x, y \in X$ gegeben.

Wenn $[x] \subseteq [y]$ gilt, dann haben wir $x \in [x] \subseteq [y]$ nach (a) und somit $x \; c \; y$. Es sei also umgekehrt angenommen, dass $x \; c \; y$ gilt. Für alle $\tilde{x} \in [x]$ haben wir $\tilde{x} \; c \; x$, die Transitivität von c liefert also $\tilde{x} \; c \; y$, d.h. $\tilde{x} \in [y]$. Folglich ist $[x] \subseteq [y]$.

Somit gilt genau dann $[x] \subseteq [y]$, wenn $x \; c \; y$ ist; wir haben also die Äquivalenz von Bedingung (ii) und Bedingung (iii) gezeigt. Nun ist aber c symmetrisch, d.h. aus $x \; c \; y$ folgt $y \; c \; x$. Folglich impliziert $[x] \subseteq [y]$ bereits $[y] \subseteq [x]$ und damit $[x] = [y]$. Da $[x] = [y]$ aber stets $[x] \subseteq [y]$ impliziert, sind auch Bedingung (i) und Bedingung (ii) äquivalent.

Insgesamt sind Bedingung (i), Bedingung (ii) und Bedingung (iii) äquivalent. □

Quotientenmengen

Als nächstes wollen wir die Äquivalenzklassen bzgl. einer Äquivalenzrelation wieder zu einer Menge zusammenfassen:

(1.10) Definition (Quotientenmenge)**.** Es seien eine Menge X und eine Äquivalenzrelation c auf X gegeben. Die *Menge aller Äquivalenzklassen* in X bzgl. c bezeichnen wir mit

$$X/c := \{[x]_c \mid x \in X\}.$$

Wir nennen X/c auch die *Quotientenmenge* (oder den *Quotienten*) von X modulo c und $\mathrm{quo} = \mathrm{quo}^{X/c} \colon X \to X/c$, $x \mapsto [x]_c$ die *Quotientenabbildung* von X/c.

Wir bestimmen die Quotientenmenge im Fall von Beispiel (1.6)(c):

(1.11) Beispiel. Es sei $c := \{(1,1),(2,2),(3,3),(4,4),(1,2),(2,1),(1,4),(4,1),(2,4),(4,2)\}$. Dann ist

$$[1,4]/c = \{[1],[2],[3],[4]\} = \{[1],[3]\}.$$

Unter der Quotientenmenge einer Menge X bzgl. einer Äquivalenzrelation c auf X stellen wir uns eine Art „Vergröberung“ der Menge X vor. Diejenigen Elemente in X, welche in X nur äquivalent bzgl. c sind, werden über die Quotientenabbildung zu gleichen Elementen in der Quotientenmenge.

(1.12) Proposition. Es seien eine Menge X und eine Äquivalenzrelation c auf X gegeben.

(a) Es ist $X/c = \{\mathrm{quo}(x) \mid x \in X\}$.

(b) Für $x, y \in X$ gilt genau dann $\mathrm{quo}(x) = \mathrm{quo}(y)$ in X/c, wenn $x \; c \; y$ in X ist.

Beweis.

(a) Nach Definition (1.10) ist

$$X/c = \{[x] \mid x \in X\} = \{\mathrm{quo}(x) \mid x \in X\}.$$

(b) Es seien $x, y \in X$ gegeben. Nach Definition (1.10) ist $\mathrm{quo}(x) = [x]$. Somit ist genau dann $\mathrm{quo}(x) = \mathrm{quo}(y)$ in X/c, wenn $[x] = [y]$ in X/c gilt. Letzteres ist nach Proposition (1.9)(b) aber äquivalent zu $x \; c \; y$ in X. □

Proposition (1.12) gibt uns eine abstrakte Beschreibung von X/c für eine Menge X und eine Äquivalenzrelation c auf X. Man beachte, dass in dieser Beschreibung keine Aussage mehr über die genaue Beschaffenheit der Elemente von X/c, welche ja selbst Teilmengen von X waren, getroffen wird. Elemente sind von der Form $\mathrm{quo}(x)$ für ein $x \in X$, und wir haben eine Charakterisierung, wann $\mathrm{quo}(x) = \mathrm{quo}(y)$ für $x, y \in X$ gilt (nämlich genau dann, wenn $x \; c \; y$). Umso beachtlicher ist es, dass für fast alle Anwendungszwecke diese theoretische Beschreibung von X/c in Abhängigkeit von X und c genügt; d.h. für fast alle Aspekte genügen uns diese zwei formalen Eigenschaften, und es ist egal, wie das Element $\mathrm{quo}(x)$ von X/c für $x \in X$ „im Einzelnen aussieht“. Wir werden, nichtsdestotrotz, im Folgenden meistens der kürzeren und damit lesefreundlicheren Notation $[x]$ den Vorzug geben.

(1.13) Korollar. Es seien eine Menge X und eine Äquivalenzrelation c auf X gegeben.

(a) Die Quotientenabbildung $\mathrm{quo}\colon X \to X/c$ ist surjektiv.

(b) Für jedes $K \in X/c$ ist die Faser von quo über K gerade

$$\mathrm{quo}^{-1}(\{K\}) = K.$$

Beweis.

(a) Nach Proposition (1.12)(a) ist $X/c = \{\mathrm{quo}(x) \mid x \in X\} = \mathrm{Im}\,\mathrm{quo}$, d.h. $\mathrm{quo}\colon X \to X/c$ ist surjektiv.

(b) Es sei $K \in X/c$ gegeben. Nach (a) ist $\mathrm{quo}\colon X \to X/c$ surjektiv, d.h. es gibt ein $x \in X$ mit $K = \mathrm{quo}(x)$. Proposition (1.12)(b) liefert

$$\begin{aligned}\mathrm{quo}^{-1}(\{K\}) = \mathrm{quo}^{-1}(\{\mathrm{quo}(x)\}) = \{\tilde{x} \in X \mid \mathrm{quo}(\tilde{x}) = \mathrm{quo}(x)\} = \{\tilde{x} \in X \mid \tilde{x} \; c \; x\} = [x] = \mathrm{quo}(x)\\ = K.\end{aligned}$$

□

(1.14) Korollar. Es seien eine Menge X und eine Äquivalenzrelation c auf X gegeben. Für jede Abbildung $g\colon X/c \to Y$ gilt

$$\mathrm{Im}\, g = \mathrm{Im}(g \circ \mathrm{quo})$$

Beweis. Nach Korollar (1.13)(a) haben wir

$$\mathrm{Im}\, g = \{g(z) \mid z \in X/c\} = \{g(\mathrm{quo}(x)) \mid x \in X\} = \mathrm{Im}(g \circ \mathrm{quo}).$$

□

(1.15) Definition (Transversale)**.** Es seien eine Menge X und eine Äquivalenzrelation c auf X gegeben. Eine *Transversale* (oder ein *Repräsentantensystem*) von X bzgl. c ist eine Teilmenge T von X so, dass es für jedes $K \in X/c$ genau ein $t \in T$ mit $K = [t]_c$ gibt.

Wir bestimmen einige Transversalen für die Äquivalenzrelationen aus Beispiel (1.6):

(1.16) Beispiel.

(a) Für $x, y \in \mathbb{R}$ gelte genau dann $x \; c \; y$, wenn $x = y$ oder $x = -y$ ist. Dann sind $\mathbb{R}_{\geq 0} = \{x \in \mathbb{R} \mid x \geq 0\}$, $\mathbb{R}_{\leq 0} = \{x \in \mathbb{R} \mid x \leq 0\}$ und $\{x \in \mathbb{R} \mid x < -2 \text{ oder } 0 \leq x \leq 2\}$ Transversalen von $\mathbb{R}$ bzgl. c.

(b) Für $x, y \in \mathbb{Z}$ gelte genau dann $x \equiv_2 y$, wenn x und y entweder beide gerade oder beide ungerade sind. Dann sind $\{0, 1\}$, $\{1, 2\}$, $\{-3, 88\}$ Transversalen von $\mathbb{Z}$ bzgl. $\equiv_2$.

(c) Es sei $c := \{(1,1), (2,2), (3,3), (4,4), (1,2), (2,1), (1,4), (4,1), (2,4), (4,2)\}$. Dann sind $\{1, 3\}$, $\{2, 3\}$, $\{3, 4\}$ Transversalen von $[1, 4]$ bzgl. c.

(d) Es sei X eine Menge. Dann ist X die einzige Transversale von X bzgl. $=$.

(1.17) Bemerkung. Es seien eine Menge X und eine Äquivalenzrelation c auf X gegeben. Eine Teilmenge T von X ist genau dann eine Transversale von X bzgl. c, wenn die Restriktion $\mathrm{quo}|_T \colon T \to X/c$ eine Bijektion ist.

Beweis. Siehe Aufgabe 5(a). □

(1.18) Bemerkung. Es seien eine Menge X und eine Äquivalenzrelation c auf X gegeben.

(a) Es sei eine Transversale T von X bzgl. c gegeben und es sei $s \colon X/c \to X$ definiert durch $s := \mathrm{inc}^T \circ (\mathrm{quo}|_T)^{-1}$. Dann ist $\mathrm{Im}\, s = T$ und $\mathrm{quo} \circ s = \mathrm{id}_{X/c}$.

(b) Für jede Abbildung $s \colon X/c \to X$ mit $\mathrm{quo} \circ s = \mathrm{id}_{X/c}$ ist $\mathrm{Im}\, s$ eine Transversale von X bzgl. c.

Beweis.

(a) Dies folgt aus Aufgabe 5(b).

(b) Dies folgt aus Aufgabe 5(c). □

Partitionen

In diesem Abschnitt wollen wir den mengentheoretischen Aspekt von Quotientenmengen etwas genauer beleuchten: Jede Äquivalenzrelation c auf einer Menge X partitioniert (also unterteilt) via X/c die Menge X in Teilmengen, nämlich in die Elemente von X/c. Gehen wir umgekehrt von einer Unterteilung von X in Teilmengen aus, so liefert uns dies wiederum eine Äquivalenzrelation, indem wir zwei Elemente als äquivalent betrachten, wenn sie im gleichen Teil der Unterteilung liegen. Der Hauptsatz über Äquivalenzrelationen besagt, dass sich diese Konstruktionen gegenseitig umkehren.
Wir beschränken uns auf den Beweis der ersten Aussage, also dass jede Äquivalenzrelation auf einer Menge diese Menge partitioniert. Zunächst präzisieren wir, was wir unter einer Unterteilung einer Menge verstehen wollen:

(1.19) Definition (Partition)**.** Es sei eine Menge X gegeben. Eine *Partition* von X ist eine Teilmenge $\mathcal{P}$ von $\mathrm{Pot}(X)$ so, dass $\emptyset \notin \mathcal{P}$ und

$$X = \dot{\bigcup} \mathcal{P}.$$

Für $x \in X$ heißt das eindeutige $P \in \mathcal{P}$ mit $x \in P$ der *Teil* von x in X bzgl. $\mathcal{P}$; wir schreiben $[x] = [x]_{\mathcal{P}} := P$.

(1.20) Bemerkung. Es seien eine Menge X und eine Äquivalenzrelation c auf X gegeben. Dann ist X/c eine Partition von X und für alle $x \in X$ ist $[x]_{X/c} = [x]_c$.

Beweis. Es ist $X/c = \{[x]_c \mid x \in X\}$. Für alle $K \in X/c$ gibt es also ein $x \in X$ mit $K = [x]_c$, und mit Proposition (1.9)(a) folgt $x \in [x]_c = K$. Insbesondere ist $K \neq \emptyset$ für alle $K \in X/c$ und damit $\emptyset \notin X/c$. Für $x \in X$ gilt ferner

$$x \in [x]_c \subseteq \bigcup_{y \in X} [y]_c = \bigcup \{[y]_c \mid y \in X\} = \bigcup X/c.$$

Folglich ist $X = \bigcup X/c$. Um die Disjunktheit dieser Vereinigung zu zeigen, seien $K, L \in \bigcup X/c$ mit $K \cap L \neq \emptyset$ gegeben. Ferner seien $x, y, z \in X$ mit $K = [x]_c$, $L = [y]_c$ und $z \in K \cap L$ gegeben. Da $z \in K = [x]_c$ gilt $z \; c \; x$, und da $z \in L = [y]_c$ gilt $z \; c \; y$. Nun ist aber c nach Aufgabe 2 euklidisch, wir erhalten also $x \; c \; y$ und somit $K = [x]_c = [y]_c = L$ nach Proposition (1.9)(b). □

Aufgaben

Aufgabe 1 (Relationen)**.**

(a) Finden Sie eine Relation auf $\{1, 2, 3\}$, die transitiv, aber weder reflexiv noch symmetrisch ist.

(b) Finden Sie eine Relation auf $\{1, 2, 3\}$, die reflexiv, aber weder transitiv noch symmetrisch ist.

(c) Finden Sie eine Relation auf $\{1, 2, 3\}$, die symmetrisch, aber weder transitiv noch reflexiv ist.

Aufgabe 2 (Äquivalenzrelationen)**.** Es seien eine Menge X und eine Relation r auf X gegeben. Wir sagen, dass r *euklidisch* ist, falls für $x, y, z \in X$ aus $x\ r\ z$ und $y\ r\ z$ stets $x\ r\ y$ folgt. Zeigen Sie: Genau dann ist r eine Äquivalenzrelation auf X, wenn r reflexiv und euklidisch ist.

Aufgabe 3 (Ordnungsrelationen)**.** Es sei eine Menge X gegeben. Eine Relation r auf X heißt *antisymmetrisch*, falls für $x, y \in X$ aus $x\ r\ y$ und $y\ r\ x$ stets $x = y$ folgt. Eine (*partielle*) *Ordnungsrelation* auf X ist eine Relation auf X, welche transitiv, reflexiv und antisymmetrisch ist.

(a) Zeigen Sie, dass die Teilbarkeitsrelation $\mid$ aus Beispiel (1.2)(b) eine Ordnungsrelation auf $\mathbb{N}$ ist.

(b) Es sei eine Menge X gegeben. Zeigen Sie, dass die Teilmengenrelation $\subseteq$ eine Ordnungsrelation auf $\mathrm{Pot}(X)$ ist.

Aufgabe 4 (Ordnungsrelationen und Injektivität)**.** Es seien eine Abbildung $f\colon X \to Y$, eine Ordnungsrelation o auf X und eine Ordnungsrelation p auf Y gegeben. Zeigen Sie: Wenn für $x, x' \in X$ aus $f(x)\ p\ f(x')$ stets $x\ o\ x'$ folgt, dann ist f injektiv.

Aufgabe 5 (Transversalen)**.** Es seien eine Menge X und eine Äquivalenzrelation c auf X gegeben.

(a) Zeigen Sie: Eine Teilmenge T von X ist genau dann eine Transversale von X bzgl. c, wenn die Restriktion $\mathrm{quo}|_T\colon T \to X/c$ eine Bijektion ist.

(b) Es sei eine Transversale T von X bzgl. c gegeben. Finden Sie eine Abbildung $s\colon X/c \to X$ mit $\mathrm{Im}\, s = T$ und $\mathrm{quo} \circ s = \mathrm{id}_{X/c}$.

(c) Zeigen Sie: Für jede Abbildung $s\colon X/c \to X$ mit $\mathrm{quo} \circ s = \mathrm{id}_{X/c}$ ist $\mathrm{Im}\, s$ eine Transversale von X bzgl. c.

Aufgabe 6 (Kongruenz modulo 5)**.** Für $x, y \in \mathbb{Z}$ gelte genau dann $x \equiv_5 y$, wenn es ein $p \in \mathbb{Z}$ mit $x = 5p + y$ gibt.

(a) Zeigen Sie, dass $\equiv_5$ eine Äquivalenzrelation auf $\mathbb{Z}$ ist.

(b) Bestimmen Sie $\mathbb{Z}/\equiv_5$. Wieviele Elemente hat der Quotient?

(c) Geben Sie zwei Transversalen von $\mathbb{Z}$ bzgl. $\equiv_5$ an.

3 Verknüpfungen

Bisher haben wir Mengen und Abbildungen zwischen Mengen betrachtet. Die aus der Schule bekannten Mengen $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ haben jedoch neben der Zusammenfassung ihrer Elemente noch mehr Struktur – wir können etwa Elemente addieren, subtrahieren, etc. oder auch Elemente vergleichen (sagen, wann ein Element „größer“ als ein anderes sein soll).
Während der zweite Aspekt (Vergleich von Elementen) bereits kurz in Aufgabe 3 angesprochen wurde, wollen wir in diesem und den folgenden Abschnitten den ersten Aspekt formalisieren. Was passiert also etwa bei der Addition auf der Menge der natürlichen Zahlen $\mathbb{N}$? Wir ordnen natürlichen Zahlen m und n deren Summe $m+n$ zu. Wie wir Zuordnungen mit Hilfe der Sprache der Mengenlehre formalisieren können, haben wir jedoch bereits in Abschnitt 1 gesehen: mit Hilfe von Abbildungen. Wir müssen also die Abbildung $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(m, n) \mapsto m+n$ betrachten.

Definition und Beispiele

(1.21) Definition (Verknüpfung)**.** Es sei eine Menge X gegeben. Eine *Verknüpfung* (oder *binäre algebraische Operation*) ist eine Abbildung $m\colon X \times X \to X$. Für $(x, y) \in X \times X$ schreiben wir $x\ m\ y := m(x, y)$.

Da zu einer gegebenen Menge X die Start- und die Zielmenge einer Verknüpfung auf X eindeutig festgelegt sind ($X \times X$ bzw. X), lassen wir diese Angaben im Folgenden meist weg.

(1.22) Beispiel.

(a) Auf $\mathbb{N}$ haben wir die Verknüpfungen $(x, y) \mapsto x + y$ und $(x, y) \mapsto x \cdot y$.

(b) Auf $\mathbb{Z}$ haben wir die Verknüpfungen $(x, y) \mapsto x + y$, $(x, y) \mapsto x - y$ und $(x, y) \mapsto x \cdot y$.

(c) Auf $\mathbb{Q}$ haben wir die Verknüpfungen $(x, y) \mapsto x + y$, $(x, y) \mapsto x - y$ und $(x, y) \mapsto x \cdot y$. Auf $\mathbb{Q} \setminus \{0\}$ haben wir die Verknüpfungen $(x, y) \mapsto x \cdot y$ und $(x, y) \mapsto x : y$.

(d) Es sei eine Menge X gegeben. Auf $\mathrm{Map}(X, X)$ haben wir die Verknüpfung $(g, f) \mapsto g \circ f$.

Assoziativität und Kommutativität

Als nächstes wollen wir grundlegende Eigenschaften von Verknüpfungen studieren, die entweder erfüllt sein können oder nicht. Hierbei orientieren wir uns an den Eigenschaften von Addition und Multiplikation auf den uns bekannten Zahlbereichen, sowie an der Verknüpfung $(g, f) \mapsto g \circ f$ auf $\mathrm{Map}(X, X)$ für eine Menge X.

(1.23) Definition (Assoziativität, Kommutativität)**.** Es seien eine Menge X und eine Verknüpfung m auf X gegeben.

(a) Wir sagen, dass m *assoziativ* ist, wenn für $x, y, z \in X$ stets

$$x\, m\, (y\, m\, z) = (x\, m\, y)\, m\, z$$

gilt.

(b) Wir sagen, dass m *kommutativ* ist, wenn für $x, y \in X$ stets

$$x\, m\, y = y\, m\, x$$

gilt.

(1.24) Beispiel.

(a) Die Verknüpfung $(x, y) \mapsto x + y$ auf $\mathbb{N}$ ist assoziativ und kommutativ.

(b) Es sei eine Menge X gegeben. Die Verknüpfung $(g, f) \mapsto g \circ f$ auf $\mathrm{Map}(X, X)$ ist assoziativ, aber im Allgemeinen nicht kommutativ.

Neutrale und inverse Elemente

(1.25) Definition (neutrales Element)**.** Es seien eine Menge X und eine Verknüpfung m auf X gegeben.

(a) Ein *linksneutrales Element* bzgl. m ist ein Element $e \in X$, welches $e\, m\, x = x$ für alle $x \in X$ erfüllt.

(b) Ein *rechtsneutrales Element* bzgl. m ist ein Element $e \in X$, welches $x\, m\, e = x$ für alle $x \in X$ erfüllt.

(c) Ein *neutrales Element* bzgl. m ist ein Element $e \in X$, welches links- und rechtsneutral bzgl. m ist.

(1.26) Beispiel.

(a) Es ist 0 ein neutrales Element bzgl. der Verknüpfung $(x, y) \mapsto x + y$ auf $\mathbb{Z}$.

(b) Für jede Menge X ist id_X ein neutrales Element bzgl. der Verknüpfung $(g, f) \mapsto g \circ f$ auf $\mathrm{Map}(X, X)$.

(1.27) Bemerkung. Es seien eine Menge X, eine Verknüpfung m auf X, ein linksneutrales Element e und ein rechtsneutrales Element e' bzgl. m gegeben. Dann gilt

$$e = e'.$$

Beweis. Da e linksneutral ist, gilt $e\, m\, x = x$ für alle $x \in X$, also insbesondere $e\, m\, e' = e'$. Da e' rechtsneutral ist, gilt $x\, m\, e' = x$ für alle $x \in X$, also insbesondere $e\, m\, e' = e$. Insgesamt haben wir

$$e = e\, m\, e' = e'.$$ □

(1.28) Korollar. Es seien eine Menge X und eine Verknüpfung m auf X gegeben. Dann gibt es höchstens ein neutrales Element bzgl. m.

Beweis. Siehe Aufgabe 9(a). □

(1.29) Bemerkung. Es seien eine Menge X, eine kommutative Verknüpfung m auf X und ein $e \in M$ gegeben. Die folgenden Bedingungen sind äquivalent.

(a) Es ist e linksneutral bzgl. m.

(b) Es ist e rechtsneutral bzgl. m.

(c) Es ist e neutral bzgl. m.

(1.30) Definition (inverse Elemente)**.** Es seien eine Menge X, eine Verknüpfung m auf X sowie $e, x \in X$ gegeben.

(a) Ein *linksinverses Element* zu x bzgl. m und e ist ein Element $y \in X$, welches $y\, m\, x = e$ erfüllt. Ist e ein neutrales Element bzgl. m, so nennen wir ein linksinverses Element zu x bzgl. m und e auch einfach ein *linksinverses Element* zu x bzgl. m.

(b) Ein *rechtsinverses Element* zu x bzgl. m und e ist ein Element $y \in X$, welches $x\, m\, y = e$ erfüllt. Ist e ein neutrales Element bzgl. m, so nennen wir ein rechtsinverses Element zu x bzgl. m und e auch einfach ein *rechtsinverses Element* zu x bzgl. m.

(c) Ein *inverses Element* zu x bzgl. m und e ist ein Element $y \in X$, welches links- und rechtsinvers zu x bzgl. m und e ist. Ist e ein neutrales Element bzgl. m, so nennen wir ein inverses Element zu x bzgl. m und e auch einfach ein *inverses Element* zu x bzgl. m.

(1.31) Beispiel.

(a) Für jedes Element $x \in \mathbb{Z}$ ist $-x$ ein inverses Element zu x bzgl. der Verknüpfung $(x, y) \mapsto x + y$ auf $\mathbb{Z}$.

(b) Es seien eine Menge X eine Menge und eine invertierbare Abbildung $f\colon X \to X$ gegeben. Dann ist die inverse Abbildung $f^{-1}\colon X \to X$ ein inverses Element zu f bzgl. der Verknüpfung $(g, f) \mapsto g \circ f$ auf $\mathrm{Map}(X, X)$.

(1.32) Bemerkung. Es seien eine Menge X, eine assoziative Verknüpfung m auf X und ein neutrales Element e bzgl. m gegeben. Ferner seien $x \in X$, ein linksinverses Element y und ein rechtsinverses Element y' zu x bzgl. m gegeben. Dann gilt

$$y = y'.$$

Beweis. Da e neutral bzgl. m ist, gilt $y\, m\, e = y$ und $e\, m\, y' = y'$. Da y linksinvers zu x bzgl. m ist, gilt $y\, m\, x = e$. Da y' rechtsinvers zu x bzgl. m ist, gilt $x\, m\, y = e$. Unter Ausnutzung der Assoziativität erhalten wir

$$y = y\, m\, e = y\, m\, (x\, m\, y') = (y\, m\, x)\, m\, y' = e\, m\, y' = y'.$$ □

(1.33) Korollar. Es seien eine Menge X, eine assoziative Verknüpfung m auf X und ein neutrales Element e bzgl. m gegeben. Dann gibt es zu jedem $x \in X$ höchstens ein inverses Element bzgl. m.

Beweis. Siehe Aufgabe 9(b). □

(1.34) Bemerkung. Es seien eine Menge X, eine kommutative Verknüpfung m auf X sowie $e, x, y \in X$ gegeben. Die folgenden Bedingungen sind äquivalent.

(a) Es ist y linksinvers zu x bzgl. m und e.

(b) Es ist y rechtsinvers zu x bzgl. m und e.

(c) Es ist y invers zu x bzgl. m und e.

(1.35) Definition (Invertierbarkeit)**.** Es seien eine Menge X, eine Verknüpfung m auf X und ein neutrales Element e bzgl. m gegeben. Ein $x \in X$ heißt *invertierbar* bzgl. m, falls es ein inverses Element zu x bzgl. m gibt.

(1.36) Beispiel.

(a) Es ist nur 0 bzgl. der Verknüpfung $(x, y) \mapsto x + y$ auf $\mathbb{N}_0$ invertierbar.

(b) Jedes $x \in \mathbb{Z}$ ist bzgl. der Verknüpfung $(x, y) \mapsto x + y$ auf $\mathbb{Z}$ invertierbar.

(c) Es sei eine Menge X gegeben. Ein $f \in \mathrm{Map}(X, X)$ ist bzgl. der Verknüpfung $(g, f) \mapsto g \circ f$ genau dann invertierbar, wenn es eine invertierbare Abbildung ist.

Aufgaben

Aufgabe 7 (Verknüpfungen)**.**

(a) Geben Sie vier Verknüpfungen auf $\mathbb{N}$ an.

(b) Untersuchen Sie auf $\mathbb{Z}$ die Verknüpfungen $(x, y) \mapsto x + y$, $(x, y) \mapsto x - y$, $(x, y) \mapsto x \cdot y$ auf Assoziativität, Kommutativität, links-/rechtsneutrale Elemente und links-/rechtsinverse Elemente.

(c) Untersuchen Sie auf $\mathbb{Q} \setminus \{0\}$ die Verknüpfungen $(x, y) \mapsto x \cdot y$ und $(x, y) \mapsto x : y$ auf Assoziativität, Kommutativität, links-/rechtsneutrale Elemente und links-/rechtsinverse Elemente.

Aufgabe 8 (Verknüpfungen)**.**

(a) Untersuchen Sie auf $\mathbb{N}$ die Verknüpfung $(m, n) \mapsto m^n$ auf Assoziativität, Kommutativität, links-/rechtsneutrale Elemente und links-/rechtsinverse Elemente.

(b) Untersuchen Sie auf $\mathbb{Z}$ die Verknüpfung $(x, y) \mapsto x + y - 1$ auf Assoziativität, Kommutativität, links-/rechtsneutrale Elemente und links-/rechtsinverse Elemente.

Aufgabe 9 (neutrale und inverse Elemente)**.** Es seien eine Menge X und eine Verknüpfung m auf X gegeben.

(a) Zeigen Sie, dass es höchstens ein neutrales Element bzgl. m gibt.

(b) Es sei m assoziativ und es sei e ein neutrales Element bzgl. m. Zeigen Sie, dass es zu jedem $x \in X$ höchstens ein inverses Element bzgl. m gibt.

Aufgabe 10 (links-/rechtsinverse Elemente)**.** Bestimmen Sie eine Menge X und ein Element in $\mathrm{Map}(X, X)$, welches ein links-, aber kein rechtsinverses Element bzgl. der Verknüpfung $(g, f) \mapsto g \circ f$ hat.

4 Gruppen und verwandte algebraische Strukturen

Als nächstes wollen wir uns davon lösen, Verknüpfungen als eigenständige Objekte zu betrachten. Wir wollen den Standpunkt einnehmen, dass Verknüpfungen „fest“ zu einer Menge dazugehören, und wollen die Menge zusammen mit den Verknüpfungen als eine gemeinsame „algebraische Struktur“ ansehen.
Obwohl wir etwa auf $\mathbb{Q}$ mehrere uns vertraute Verknüpfungen haben, siehe Beispiel (1.22)(c), begnügen wir uns in diesem Abschnitt zunächst mit „einfacheren“ Strukturen und studieren Mengen, die mit einer Verknüpfung versehen sind und einige der in Abschnitt 3 definierten Eigenschaften erfüllen. Mengen, welche mit zwei miteinander verträglichen Verknüpfungen ausgestattet sind, werden dann in Abschnitt 6 eingeführt.

Magmas

(1.37) Definition (Magma)**.** Ein *Magma* besteht aus einer Menge M zusammen mit einer Verknüpfung m auf M. Unter Missbrauch der Notation bezeichnen wir sowohl das besagte Magma als auch die unterliegende Menge mit M. Die Verknüpfung m wird *Multiplikation* (oder *Magmaverknüpfung*) von M genannt.
Für ein Magma M mit Multiplikation m schreiben wir $\cdot = \cdot^M := m$ und $xy = x \cdot y = x \cdot^M y := xmy$ für $x, y \in M$.

Bei der Festlegung „$\cdot = \cdot^M := m$“ in Definition (1.37) für die Multiplikation eines Magmas handelt es sich um eine Notation, um in einem abstrakt gegebenen Magma (d.h. ein nicht in einem konkreten Beispiel gegebenes Magma) einfach von der Verknüpfung sprechen zu können und um diese nicht immer explizit erwähnen zu müssen. In der Regel werden wir also von einem „Magma M“ anstatt von einem „Magma M mit Multiplikation m“ sprechen, die Multiplikation als implizit gegeben ansehen und diese dann mit dem Symbol $\cdot$ bezeichnen. Die Bezeichnung $\cdot^M$ werden wir nur dann verwenden, wenn wir explizit darauf hinweisen möchten, dass diese Multiplikation zu M gehört (etwa, wenn wir mehrere Magmas auf einmal betrachten), in der Regel werden wir jedoch darauf verzichten.
Die Notation „$\cdot$“ (und auch die Bezeichnung „Multiplikation“) ist natürlich von Beispielen motiviert, siehe etwa Beispiel (1.41)(a), (b). Es gibt natürlich auch andere Beispiele, wo die Magmaverknüpfung keine Multiplikation im vertrauten Sinne ist; in diesen konkret gegebenen Beispielen verwenden wir natürlich weiterhin die jeweils vorliegende Notation, die durch das Beispiel mitgebracht wird; siehe insbesondere Beispiel (1.41)(e).

(1.38) Definition (assoziatives Magma, kommutatives Magma)**.**

(a) Ein Magma M heißt *assoziativ*, falls die Multiplikation von M assoziativ ist.

(b) Ein Magma M heißt *kommutativ*, falls die Multiplikation von M kommutativ ist.

Mit Hilfe der Standardnotation in einem Magma M lesen sich die in Definition (1.38) eingeführten (möglichen) Eigenschaften eines Magmas wie folgt:

- *Assoziativität.* Für $x, y, z \in M$ ist $x(yz) = (xy)z$.
- *Kommutativität.* Für $x, y \in M$ ist $xy = yx$.

Für kommutative Magmas hat sich noch eine andere Bezeichnung und eine andere Notation eingebürgert, die natürlich ebenfalls von den Beispielen motiviert ist, siehe etwa Beispiel (1.41)(c), (d).

(1.39) Definition (abelsches Magma)**.** Ein *abelsches Magma* ist ein kommutatives Magma A mit Magmaverknüpfung a. Die Verknüpfung a wird auch *Addition* von A genannt.
Für ein abelsches Magma A mit Addition a schreiben wir $+ = +^A := a$ und $x + y = x +^A y := a(x, y)$ für $x, y \in A$.

Ein abelsches Magma ist also strukturell gesehen das Gleiche wie ein kommutatives Magma; wir verwenden lediglich in abstrakten abelschen Magmas eine andere Standardnotation: Abstrakte Magmas (die ggf. auch mal kommutativ sein dürfen, aber im Allgemeinen nicht müssen) werden multiplikativ geschrieben, abstrakte abelsche Magmas werden additiv geschrieben.
Insbesondere gilt: Alle Aussagen über beliebige Magmas und über kommutative Magmas (in multiplikativer Notation geschrieben) bleiben auch für abelsche Magmas (in additiver Notation geschrieben) korrekt. Umgekehrt bleiben alle Aussagen über abelsche Magmas (in additiver Notation geschrieben) auch für kommutative Magmas (in multiplikativer Notation geschrieben) korrekt. Bei der Verwendung muss gegebenenfalls nur die jeweilige Notation angepasst werden – in der Regel werden wir getroffene Aussagen über Magmas bzw. kommutative Magmas nicht in additiver Notation wiederholen.

Halbgruppen

Für assoziative (abelsche) Magmas verwenden wir folgende alternative Terminologie.

(1.40) Definition ((abelsche) Halbgruppe)**.**

(a) Eine *Halbgruppe* ist ein Magma mit assoziativer Multiplikation. Die Magmaverknüpfung einer Halbgruppe M wird auch *Halbgruppenverknüpfung* von M genannt.

(b) Eine *abelsche Halbgruppe* ist ein abelsches Magma mit assoziativer Addition.

Wir werden in diesem Kurs keine Beispiele von Magmas betrachten, welche nicht assoziativ sind – alle unsere Magmas sind also de facto Halbgruppen, alle abelschen Magmas sind de facto abelsche Halbgruppen.

(1.41) Beispiel.

(a) Es wird $\mathbb{N}$ eine kommutative Halbgruppe mit Multiplikation $(x, y) \mapsto x \cdot y$ (die uns vertraute Multiplikation der natürlichen Zahlen).

(b) Es wird $\mathbb{Q}$ eine kommutative Halbgruppe mit Multiplikation $(x, y) \mapsto x \cdot y$.

(c) Es wird $\mathbb{N}$ eine abelsche Halbgruppe mit Addition $(x, y) \mapsto x+y$ (die uns vertraute Addition der natürlichen Zahlen).

(d) Es wird $\mathbb{Z}$ eine abelsche Halbgruppe mit Addition $(x, y) \mapsto x + y$.

(e) Es sei eine Menge X gegeben. Dann wird $\mathrm{Map}(X, X)$ eine im Allgemeinen nicht-kommutative Halbgruppe mit Halbgruppenverknüpfung $(g, f) \mapsto g \circ f$.

(1.42) Konvention. Wegen der Assoziativität der Multiplikation einer Halbgruppe bzw. der Addition einer abelschen Halbgruppe kommt es bei iterativer Bildung nicht auf die Klammerung an. Im Regelfall lassen wir daher die Klammern im Folgenden weg.

Monoide

(1.43) Definition ((abelsches) Monoid)**.**

(a) Ein *Monoid* ist eine Halbgruppe M, welche ein neutrales Element bzgl. $\cdot^M$ besitzt. Die Halbgruppenverknüpfung eines Monoids M wird auch *Monoidverknüpfung* von M genannt. Das neutrale Element bzgl. der Multiplikation wird auch *Einselement* (oder die *Eins*) von M genannt und als $1 = 1^M$ notiert.

(b) Ein *abelsches Monoid* ist eine abelsche Halbgruppe A, welche ein neutrales Element bzgl. $+^A$ besitzt. Das neutrale Element bzgl. der Addition wird auch *Nullelement* (oder die *Null*) von A genannt und als $0 = 0^A$ notiert.

Mit Hilfe der Standardnotation in einem Monoid M lesen sich die *Axiome* eines Monoids, d.h. dessen definierende Eigenschaften, wie folgt:

- *Assoziativität.* Für $x, y, z \in M$ ist $x(yz) = (xy)z$.
- *Existenz der Eins.* Es existiert ein $e \in M$ mit $ex = xe = x$ für alle $x \in M$. Dieses e ist nach Korollar (1.28) eindeutig bestimmt und wird mit 1 bezeichnet. Wir haben also $1x = x1 = x$ für alle $x \in M$.

Ist M kommutativ, so gilt zusätzlich noch:

- *Kommutativität.* Für $x, y \in M$ ist $xy = yx$.

Die Axiome eines abelschen Monoids A sind die eines kommutativen Monoids in additiver Notation.
Wir betrachten unsere Beispiele aus (1.41) noch einmal und wollen festhalten, welche davon Monoide bzw. abelsche Monoide bilden.

(1.44) Beispiel.

(a) Die Halbgruppe $\mathbb{N}$ mit der Multiplikation $(x, y) \mapsto x \cdot y$ ist ein kommutatives Monoid.

(b) Die Halbgruppe $\mathbb{Q}$ mit der Multiplikation $(x, y) \mapsto x \cdot y$ ist ein kommutatives Monoid.

(c) Die abelsche Halbgruppe $\mathbb{N}$ mit der Addition $(x, y) \mapsto x + y$ ist kein abelsches Monoid. Allerdings wird $\mathbb{N}_0$ ein abelsches Monoid mit Addition $(x, y) \mapsto x + y$.

(d) Die abelsche Halbgruppe $\mathbb{Z}$ mit der Addition $(x, y) \mapsto x + y$ ist ein abelsches Monoid.

(e) Für jede Menge X ist die Halbgruppe $\mathrm{Map}(X, X)$ mit der Halbgruppenverknüpfung $(g, f) \mapsto g \circ f$ ein Monoid. Das Einselement von $\mathrm{Map}(X, X)$ ist id_X.

In erster Linie haben wir die Begriffe Magma, Halbgruppe und Monoid eingeführt, um mit deren Hilfe andere, speziellere Strukturen einzuführen, wie etwa im Folgenden den Begriff der Gruppe, siehe Definition (1.50), oder auch den Begriff des Rings in Abschnitt 6.
Bevor wir Gruppen einführen, legen wir noch eine vereinfachte Sprechweise für den Begriff der Invertierbarkeit bzgl. der Monoidverknüpfung in einem gegebenen Monoid fest:

(1.45) Definition (Invertierbarkeit)**.**

(a) Es sei ein Monoid M gegeben. Ein Element $x \in M$ heißt *invertierbar* in M (oder eine *Einheit* von M), falls x invertierbar bzgl. $\cdot^M$ ist. Das zu einem invertierbaren Element $x \in M$ bzgl. $\cdot^M$ inverse Element y wird auch das *inverse Element* (oder das *Inverse*) zu x in M genannt und als $x^{-1} = (x^{-1})^M := y$ notiert.

Die *Menge aller invertierbaren Elemente* in M bezeichnen wir mit

$$M^\times = \{x \in M \mid x \text{ ist invertierbar}\}.$$

(b) Es sei ein abelsches Monoid A gegeben. Ein Element $x \in A$ heißt *negierbar* in A, falls x invertierbar bzgl. $+^A$ ist. Das zu einem negierbaren Element $x \in A$ bzgl. $+^A$ inverse Element y wird auch das *negative Element* (oder das *Negative*) zu x in A genannt und als $-x = (-x)^A := y$ notiert.

Die etwas ungewöhnlich aussehende Notation $(x^{-1})^M$ in Definition (1.45)(a) soll lediglich deutlich machen, in welchem Monoid wir das Inverse zu x bilden – nämlich gerade im Monoid M. Wir werden diese Notation nur dann verwenden, wenn wir explizit darauf hinweisen wollen, in welchem Monoid das Inverse gebildet wird, vgl. etwa Definition (1.69)(a).

(1.46) Beispiel.

(a) Es wird $\mathbb{Z}$ ein Monoid mit Multiplikation $(x, y) \mapsto xy$. Die invertierbaren Elemente in $\mathbb{Z}$ sind 1 und -1.

(b) Es wird $\mathbb{N}_0$ ein abelsches Monoid mit Addition $(x, y) \mapsto x + y$. Das einzige negierbare Element in $\mathbb{N}_0$ ist 0.

(c) Es wird $\mathbb{Z}$ ein abelsches Monoid mit Addition $(x, y) \mapsto x + y$. Jedes Element in $\mathbb{Z}$ ist negierbar.

Wir wollen einige einfache Eigenschaften von invertierbaren Elementen herleiten.

(1.47) Proposition. Es sei ein Monoid M gegeben.

(a) Für $x, y \in M^\times$ ist auch $xy \in M^\times$ mit $(xy)^{-1} = y^{-1}x^{-1}$.

(b) Es ist $1 \in M^\times$ mit $1^{-1} = 1$.

(c) Für $x \in M^\times$ ist auch $x^{-1} \in M^\times$ mit $(x^{-1})^{-1} = x$.

Beweis. Siehe Aufgabe 11. □

(1.48) Bemerkung. Es seien ein Monoid M und $a \in M^\times$, $b, x \in M$ gegeben.

(a) Genau dann gilt $ax = b$, wenn $x = a^{-1}b$ ist.

(b) Genau dann gilt $xa = b$, wenn $x = ba^{-1}$ ist.

Beweis.

(a) Wenn $ax = b$ gilt, dann auch

$$x = 1x = a^{-1}ax = a^{-1}b.$$

Umgekehrt, wenn $x = a^{-1}b$ ist, dann haben wir nach Proposition (1.47)(c) auch

$$b = (a^{-1})^{-1}x = ax.$$

(b) Dies lässt sich analog zu (a) beweisen. □

(1.49) Korollar. Es sei ein Monoid M gegeben.

(a) Es seien $a \in M^\times$, $x, y \in M$ gegeben. Wenn $ax = ay$ oder $xa = ya$ gilt, dann ist $x = y$.

(b) Es seien $a \in M^\times$, $x \in M$ gegeben. Wenn $ax = a$ oder $xa = a$ gilt, dann ist $x = 1$.

Beweis.

(a) Es gelte $ax = ay$; der andere Fall wird analog bewiesen. Nach Bemerkung (1.48)(a) ist dann

$$x = a^{-1}ay = 1y = y.$$

(b) Es gelte $ax = a$; der andere Fall wird analog bewiesen. Dann haben wir $ax = a1$ und also $x = 1$ nach (a). □

Gruppen und abelsche Gruppen

(1.50) Definition ((abelsche) Gruppe)**.**

(a) Eine *Gruppe* ist ein Monoid G, in welchem jedes Element von G invertierbar ist. Die Monoidverknüpfung einer Gruppe G wird auch *Gruppenverknüpfung* von G genannt.

(b) Eine *abelsche Gruppe* ist ein abelsches Monoid A, in welchem jedes Element von A negierbar ist.

Die Axiome einer Gruppe G in Standardnotation lesen sich also wie folgt:

- *Assoziativität.* Für $x, y, z \in G$ ist $x(yz) = (xy)z$.

- *Existenz der Eins.* Es existiert ein $e \in G$ mit $ex = xe = x$ für alle $x \in G$. Dieses e ist nach Korollar (1.28) eindeutig bestimmt und wird mit 1 bezeichnet. Wir haben also $1x = x1 = x$ für alle $x \in G$.

- *Existenz der Inversen.* Für jedes $x \in G$ existiert ein $y \in G$ mit $yx = xy = 1$. Dieses y ist nach Korollar (1.33) eindeutig bestimmt und wird mit x^{-1} bezeichnet. Wir haben also $x^{-1}x = xx^{-1} = 1$.

Ist G kommutativ, so gilt zusätzlich noch:

- *Kommutativität.* Für $x, y \in G$ ist $xy = yx$.

Die Axiome einer abelschen Gruppe A sind die einer kommutativen Gruppe, jedoch mit anderer Notation. Es ist eine gute Übung, alle in diesem Abschnitt vorkommenden Aussagen in die additive Notation umzuschreiben, vgl. Aufgabe 17.
Wir betonen noch einmal: Jede kommutative Gruppe lässt sich als abelsche Gruppe auffassen und umgekehrt – strukturell gesehen sind es die gleichen Objekte, wir bringen durch die unterschiedlichen Terminologien lediglich zum Ausdruck, welche Notation wir verwenden. Insbesondere bleiben alle Aussagen über Gruppen auch für abelsche Gruppen gültig, sie müssen nur in der Notation angepasst werden.
Wie von der Menge der ganzen Zahlen $\mathbb{Z}$ bekannt, liefert die Existenz von negativen Elementen in einer abelschen Gruppe eine neue Verknüpfung:

(1.51) Definition (Subtraktion)**.** Es sei eine abelsche Gruppe A gegeben. Die Verknüpfung $(x, y) \mapsto x + (-y)$ auf A wird *Subtraktion* von A genannt und mit $-$ bezeichnet. Wir schreiben $x - y := x + (-y)$ für $x, y \in A$.

Wir betonen, dass die Addition einer abelschen Gruppe A ein Teil der Daten von A ist (d.h. A besteht aus der unterliegenden Menge, die unter Missbrauch der Notation ebenfalls mit A bezeichnet wird, und der Addition). Hingegen wird die Subtraktion mit Hilfe der Addition und den inversen Elementen definiert und ist insbesondere somit durch die Daten (unterliegende Menge und Addition) eindeutig festgelegt.
Da Gruppen (multiplikativ geschrieben) im Allgemeinen nicht kommutativ sind, können wir die analoge Verknüpfung $(x, y) \mapsto \frac{x}{y}$, wie etwa aus dem Beispiel $\mathbb{Q} \setminus \{0\}$ bekannt, nicht immer bilden, da im Allgemeinen $xy^{-1} \neq y^{-1}x$ ist. Genauer gesagt erhalten wir zwei Verknüpfungen, welche im Allgemeinen nicht übereinstimmen und für welche sich keine neue Notation eingebürgert hat. Lediglich bei Körpern, siehe Definition (1.108), wird die Bruchnotation manchmal verwandt.
Wir betrachten unsere Beispiele aus (1.41) und (1.44) noch einmal und wollen festhalten, welche davon Gruppen bzw. abelsche Gruppen bilden.

(1.52) Beispiel.

(a) Das Monoid $\mathbb{N}$ mit der Multiplikation $(x, y) \mapsto x \cdot y$ ist keine Gruppe.

(b) Das Monoid $\mathbb{Q}$ mit der Multiplikation $(x, y) \mapsto x \cdot y$ ist keine Gruppe. Allerdings wird $\mathbb{Q} \setminus \{0\}$ eine kommutative Gruppe mit Multiplikation $(x, y) \mapsto x \cdot y$.

(c) Die abelsche Halbgruppe $\mathbb{N}$ mit der Addition $(x, y) \mapsto x + y$ ist keine abelsche Gruppe. Das abelsche Monoid $\mathbb{N}_0$ mit der Addition $(x, y) \mapsto x + y$ ist keine abelsche Gruppe.

(d) Das abelsche Monoid $\mathbb{Z}$ mit der Addition $(x, y) \mapsto x + y$ ist eine abelsche Gruppe.

(e) Das Monoid $\mathrm{Map}(X, X)$ für eine Menge X mit der Monoidverknüpfung $(g, f) \mapsto g \circ f$ ist im Allgemeinen keine Gruppe.

Zu Beispiel (1.52)(e) vergleiche man auch Aufgabe 12 und Abschnitt 5.

(1.53) Konvention. Wenn wir in Zukunft von der abelschen Gruppe $\mathbb{Z}$ sprechen, so meinen wir damit stets $\mathbb{Z}$ mit der gewöhnlichen Addition. Wenn wir vom kommutativen Monoid $\mathbb{Z}$ sprechen, so meinen wir damit stets $\mathbb{Z}$ mit der gewöhnlichen Multiplikation. Ähnlich für $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{Q}$, $\mathbb{R}$.

Redundanz der Gruppenaxiome

Um zu zeigen, dass eine kommutative Halbgruppe eine Gruppe ist, genügt es natürlich, die definierende Eigenschaft eines links- oder eines rechtsneutrales Elements sowie die definierende Eigenschaft von links- oder rechtsinversen Element bzgl. der Magmaverknüpfung zu verifizieren, vgl. Bemerkung (1.29) und Bemerkung (1.34). Das folgende Lemma besagt, dass dies auch für nicht-kommutative Gruppen gilt, sodenn man sich auf eine Seite (jeweils links oder jeweils rechts) einigt.

(1.54) Lemma. Es sei eine Halbgruppe G gegeben.

(a) Wenn es ein linksneutrales Element e bzgl. $\cdot^G$ und für alle $x \in G$ ein linksinverses Element bzgl. $\cdot^G$ und e gibt, dann ist G eine Gruppe.

(b) Wenn es ein rechtsneutrales Element e bzgl. $\cdot^G$ und für alle $x \in G$ ein rechtsinverses Element bzgl. $\cdot^G$ und e gibt, dann ist G eine Gruppe.

Beweis.

(a) Es seien ein linksneutrales Element e in G bzgl. $\cdot^G$, ein beliebiges $x \in G$, ein linksinverses Element y zu x bzgl. $\cdot^G$ und e und ein linksinverses Element z zu y bzgl. $\cdot^G$ und e gegeben. Dann gilt $ex = x$, $ey = y$, $yx = e$ und $zy = e$. Es folgt

$$xy = (ex)y = ((zy)x)y = (z(yx))y = (ze)y = z(ey) = zy = e,$$

d.h. y ist auch ein rechtsinverses Element von x bzgl. m und e. Außerdem gilt

$$xe = x(yx) = (xy)x = ex = x.$$

Da $x \in G$ beliebig gewählt war, ist e somit auch ein rechtsneutrales Element in G bzgl. $\cdot^G$. Folglich ist e ein neutrales Element bzgl. $\cdot^G$ und zu jedem $x \in G$ existiert ein inverses Element bzgl. $\cdot^G$, d.h. G ist eine Gruppe.

(b) Dies lässt sich analog zu (a) beweisen. □

Die Einheitengruppe

Während in einer Gruppe jedes Element invertierbar ist, haben wir in einem beliebigen Monoid auch nicht-invertierbare Elemente. Wenn wir unsere Multiplikation auf einem Monoid jedoch auf die invertierbaren Elemente einschränken, erhalten wir eine Gruppe:

(1.55) Bemerkung. Für jedes Monoid M wird $M^\times$ eine Gruppe, wobei die Multiplikation auf $M^\times$ durch $x \cdot^{M^\times} y = x \cdot^M y$ für $x, y \in M$ gegeben ist.

Beweis. Siehe Aufgabe 13. □

(1.56) Definition (Einheitengruppe)**.** Es sei ein Monoid M gegeben. Die Gruppe $M^\times$ mit der Multiplikation aus Bemerkung (1.55) heißt *Einheitengruppe* von M.

Ein Monoid G ist also genau dann eine Gruppe, wenn $G^\times = G$ ist.

(1.57) Beispiel. Die Einheitengruppe von $\mathbb{Z}$, aufgefasst als Monoid bzgl. der uns vertrauten Multiplikation, ist gegeben durch

$$\mathbb{Z}^\times = \{1, -1\}.$$

Produkt- und Summennotation

Als nächstes führen wir die Produkt- bzw. Summenschreibweise ein:

(1.58) Notation. Es sei $n \in \mathbb{N}_0$ gegeben.

(a) Es seien ein Monoid M und $x_i \in M$ für $i \in [1,n]$ so gegeben, dass $x_i x_j = x_j x_i$ für $i,j \in [1,n]$. Für $k \in [0,n]$ definieren wir rekursiv

$$\prod_{i\in[1,k]} x_i := \begin{cases} 1, & \text{falls } k = 0, \\ \left(\prod_{i\in[1,k-1]} x_i\right) x_k, & \text{falls } k > 0. \end{cases}$$

(b) Es seien ein abelsches Monoid A und $x_i \in A$ für $i \in [1,n]$ gegeben. Für $k \in [0,n]$ definieren wir rekursiv

$$\sum_{i\in[1,k]} x_i := \begin{cases} 0, & \text{falls } k = 0, \\ \sum_{i\in[1,k-1]} x_i + x_k, & \text{falls } k > 0. \end{cases}$$

(1.59) Bemerkung. Es seien ein Monoid M, eine endliche Menge I und $x_i \in M$ für $i \in I$ so gegeben, dass $x_i x_j = x_j x_i$ für $i,j \in I$. Für Bijektionen $e, e' \colon [1,|I|] \to I$ gilt

$$\prod_{k\in[1,|I|]} x_{e(k)} = \prod_{k\in[1,|I|]} x_{e'(k)}.$$

Beweis. Dies folgt aus der Assoziativität von M. □

Bemerkung (1.59) erlaubt uns, die Produkt- und Summenschreibweise auf beliebige endliche Indexmengen zu verallgemeinern:

(1.60) Notation. Es sei eine endliche Menge I gegeben. Wir wählen eine Bijektion $e \colon [1,|I|] \to I$.

(a) Es seien ein Monoid M und $x_i \in M$ für $i \in I$ so gegeben, dass $x_i x_j = x_j x_i$ für $i,j \in I$. Wir setzen

$$\prod_{i\in I} x_i := \prod_{k\in[1,|I|]} x_{e(k)}.$$

(b) Es seien ein abelsches Monoid A und $x_i \in A$ für $i \in I$ gegeben. Wir setzen

$$\sum_{i\in I} x_i := \sum_{k\in[1,|I|]} x_{e(k)}.$$

Wir kommen zum Spezialfall, bei welchem alle indizierten Elemente gleich sind:

(1.61) Notation.

(a) Es seien ein Monoid M und ein $x \in M$ gegeben. Für $k \in \mathbb{N}_0$ setzen wir

$$x^k := \prod_{i\in[1,k]} x.$$

Wenn x invertierbar in M ist, so setzen wir

$$x^{-k} := (x^{-1})^k$$

für $k \in \mathbb{N}$.

(b) Es seien ein abelsches Monoid A und ein $x \in A$ gegeben. Für $k \in \mathbb{N}_0$ setzen wir

$$kx = k \cdot x := \sum_{i\in[1,k]} x.$$

Wenn x negierbar in A ist, so setzen wir

$$(-k)x := k(-x)$$

für $k \in \mathbb{N}$.

(1.62) Bemerkung. Es sei ein Monoid M gegeben. Dann ist

$$x^1 = x$$

für alle $x \in M$.

Nach Bemerkung (1.62) ist also die für den Fall $k = 1$ zunächst missbräuchliche Notation „$x^{-k} := (x^{-1})^k$“ in (1.61)(a) für ein invertierbares Element x in einem Monoid M gerechtfertigt.

(1.63) Proposition (Potenzgesetze)**.** Es sei ein Monoid M gegeben.

(a) Für $x \in M$, $k, l \in \mathbb{N}_0$ gilt

$$x^k x^l = x^{k+l}.$$

Für $x \in M^\times$, $k, l \in \mathbb{Z}$ gilt

$$x^k x^l = x^{k+l}.$$

(b) Für $x \in M$, $k, l \in \mathbb{N}_0$ gilt

$$(x^k)^l = x^{kl}.$$

Für $x \in M^\times$, $k, l \in \mathbb{Z}$ gilt

$$(x^k)^l = x^{kl}.$$

(c) Es sei M kommutativ. Für $x, y \in M$, $k \in \mathbb{N}_0$ gilt

$$x^k y^k = (xy)^k.$$

Für $x, y \in M^\times$, $k \in \mathbb{Z}$ gilt

$$x^k y^k = (xy)^k.$$

Beweis.

(a) Es seien $x \in M$, $k \in \mathbb{N}_0$. Um $x^k x^l = x^{k+l}$ für alle $l \in \mathbb{N}_0$ zu zeigen, führen wir Induktion nach l. Für $l = 0$ gilt

$$x^k x^l = x^k x^0 = x^k \cdot 1 = x^k = x^{k+0}.$$

Es sei also $l > 0$ und gelte $x^k x^{l-1} = x^{k+l-1}$. Dann ist auch $k + l \geq l > 0$ und somit

$$x^k x^l = x^k (x^{l-1} x) = (x^k x^{l-1}) x = x^{k+l-1} x = x^{k+l}.$$

Nach dem Induktionsprinzip haben wir $x^k x^l = x^{k+l}$ für alle $l \in \mathbb{N}_0$.

Um $x^k x^l = x^{k+l}$ für alle $x \in M^\times$, $k, l \in \mathbb{Z}$ zu zeigen, unterscheiden wir drei Fälle. Zuerst verifizieren wir die Gleichung für den Spezialfall $x \in M^\times$, $k \in \mathbb{Z}$, $l = 1$, danach für $x \in M^\times$, $k \in \mathbb{Z}$, $l \geq 0$ mittels Induktion nach l, und schließlich für $x \in M^\times$, $k \in \mathbb{Z}$, $l < 0$.

Zum ersten Fall. Es seien $x \in M^\times$, $k \in \mathbb{Z}$, $l = 1$. Für $k \geq 0$ ist $k+1 > 0$ und damit $x^{k+1} = x^{(k+1)-1} x = x^k x$ nach Definition. Für $k < 0$ gilt aber $-k > 0$ und damit ebenfalls

$$\begin{aligned} x^k x^1 = (x^{-1})^{-k} x = ((x^{-1})^{-k-1} x^{-1}) x = (x^{-1})^{-k-1} (x^{-1} x) = (x^{-1})^{-(k+1)} \cdot 1 = (x^{-1})^{-(k+1)} \\ = \begin{Bmatrix} (x^{-1})^0, & \text{falls } k = -1, \\ x^{-(-(k+1))}, & \text{falls } k < -1 \end{Bmatrix} = \begin{Bmatrix} 1, & \text{falls } k = -1, \\ x^{k+1}, & \text{falls } k < -1 \end{Bmatrix} = x^{k+1}. \end{aligned}$$

Zum zweiten Fall. Es seien $x \in M^\times$, $k \in \mathbb{Z}$. Um $x^k x^l = x^{k+l}$ für $l \in \mathbb{Z}$, $l \geq 0$ zu zeigen, führen wir Induktion nach l (wobei dies völlig analog zum Beweis für $x \in M$, $k, l \in \mathbb{N}_0$ geht): Für $l = 0$ gilt

$$x^k x^l = x^k x^0 = x^k \cdot 1 = x^k = x^{k+0}.$$

Es seien also $l > 0$ und es gelte $x^k x^{l-1} = x^{k+l-1}$. Unter Benutzung des ersten Falls erhalten wir dann auch

$$x^k x^l = x^k(x^{l-1}x) = (x^k x^{l-1})x = x^{k+l-1}x = x^{k+l}.$$

Nach dem Induktionsprinzip haben wir $x^k x^l = x^{k+l}$ für alle $l \geq 0$.

Zum dritten Fall. Schließlich seien $x \in M^\times$, $k, l \in \mathbb{Z}$, $l < 0$. Dann ist $-l > 0$, also

$$x^{k+l}x^{-l} = x^{k+l+(-l)} = x^k$$

nach dem zweiten Fall und damit $x^{k+l} = x^k(x^{-l})^{-1}$. Nun haben wir aber

$$x^{-l}x^l = ((x^{-1})^{-1})^{-l}(x^{-1})^{-l} = (x^{-1})^{-(-l)}(x^{-1})^{-l} = (x^{-1})^l(x^{-1})^{-l} = (x^{-1})^{l+(-l)} = (x^{-1})^0 = 1$$

unter Benutzung des zweiten Falls, also $(x^{-l})^{-1} = x^l$ nach Bemerkung (1.32) und damit auch in diesem Fall

$$x^k x^l = x^k(x^{-l})^{-1} = x^{k+l}.$$

(b) Es seien $x \in M$, $k \in \mathbb{N}_0$. Um $(x^k)^l = x^{kl}$ für alle $l \in \mathbb{N}_0$ zu zeigen, führen wir Induktion nach l. Für $l = 0$ gilt

$$(x^k)^0 = 1 = x^0 = x^{k\cdot 0}.$$

Es sei also $l > 0$ und gelte $(x^k)^{l-1} = x^{k(l-1)}$. Mit (a) folgt

$$(x^k)^l = (x^k)^{l-1}x^k = x^{k(l-1)}x^k = x^{k(l-1)+k} = x^{kl}$$

Nach dem Induktionsprinzip haben wir $(x^k)^l = x^{kl}$ für alle $l \in \mathbb{N}_0$.

Um $(x^k)^l = x^{kl}$ für alle $x \in M^\times$, $k, l \in \mathbb{Z}$, unterscheiden wir drei Fälle. Zuerst verifizieren wir die Gleichung für $k \geq 0$, $l \geq 0$, danach für $k < 0$, $l \geq 0$, und schließlich für $k \in \mathbb{Z}$, $l < 0$.

Zum ersten Fall. Wir haben bereits bewiesen, dass $(x^k)^l = x^{kl}$ für alle $x \in M$, $k, l \in \mathbb{N}_0$ gilt, also insbesondere für $x \in M^\times$, $k, l \in \mathbb{Z}$, $k \geq 0$, $l \geq 0$.

Zum zweiten Fall. Es seien $x \in M^\times$, $k, l \in \mathbb{Z}$, $k < 0$, $l \geq 0$. Dann ist $-k > 0$ und $-kl > 0$, also

$$(x^k)^l = ((x^{-1})^{-k})^l = (x^{-1})^{(-k)l} = (x^{-1})^{-kl} = x^{kl}$$

nach dem ersten Fall.

Zum dritten Fall. Es seien $x \in M^\times$, $k, l \in \mathbb{Z}$, $k \in \mathbb{Z}$, $l < 0$. Dann ist $-l > 0$, also

$$(x^k)^{-l} = x^{k(-l)}$$

nach dem ersten oder zweiten Fall. Nun ist aber $(x^k)^l\,(x^k)^{-l} = (x^k)^0 = 1$ und $x^{k(-l)}x^{kl} = x^0 = 1$ nach (a), also $((x^k)^{-l})^{-1} = (x^k)^l$ und $(x^{k(-l)})^{-1} = x^{kl}$ nach Bemerkung (1.32). Wir erhalten also auch in diesem Fall

$$(x^k)^l = ((x^k)^{-l})^{-1} = (x^{k(-l)})^{-1} = x^{kl}.$$

(c) Es seien $x, y \in M$. Um $x^k y^k = (xy)^k$ für alle $k \in \mathbb{N}_0$ zu zeigen, führen wir Induktion nach k. Für $k = 0$ gilt

$$x^k y^k = x^0 y^0 = 1 \cdot 1 = 1 = (xy)^0.$$

Es sei also $k > 0$ und gelte $x^{k-1}y^{k-1} = (xy)^{k-1}$. Dann ist auch

$$x^k y^k = (x^{k-1}x)(y^{k-1}y) = (x^{k-1}y^{k-1})(xy) = (xy)^{k-1}\,(xy) = (xy)^k.$$

Nach dem Induktionsprinzip haben wir $x^k y^k = (xy)^k$ für alle $k \in \mathbb{N}_0$.

Nun seien $x, y \in M^\times$, $k \in \mathbb{Z}$, $k < 0$. Dann ist $-k > 0$, also

$$x^k y^k = (x^{-1})^{-k}(y^{-1})^{-k} = (x^{-1}y^{-1})^{-k} = (y^{-1}x^{-1})^{-k} = ((xy)^{-1})^{-k} = (xy)^k$$

nach Proposition (1.47)(a). □

Homomorphismen

In der Mathematik ist es üblich, algebraische Strukturen (und auch andere), wie etwa die in diesem Abschnitt betrachteten (Magma, Halbgruppe, Monoid, Gruppe sowie deren abelsche Varianten), zusammen mit ihren strukturerhaltenden Abbildungen, sogenannte *Homomorphismen*, zu studieren. Strukturerhaltend bedeutet hierbei, dass diese Abbildungen verträglich mit allen relevanten Daten sind. Wir begnügen uns hier mit der Variante für Monoide und Gruppen.

(1.64) Definition (Homomorphismus von (abelschen) Monoiden und (abelschen) Gruppen)**.**

(a) (i) Es seien Monoide M und N gegeben. Ein *Monoidhomomorphismus* (oder *Homomorphismus von Monoiden* oder *Homomorphismus*) von M nach N ist eine Abbildung $\varphi\colon M \to N$ so, dass folgende Axiome gelten.

- *Verträglichkeit mit den Multiplikationen.* Für alle $x, x' \in M$ gilt
$$\varphi(x \cdot^M x') = \varphi(x) \cdot^N \varphi(x').$$
- *Verträglichkeit der Einselemente.* Es ist
$$\varphi(1^M) = 1^N.$$

(ii) Es seien abelsche Monoide A und B gegeben. Ein *Homomorphismus abelscher Monoide* (oder *Homomorphismus von abelschen Monoiden* oder *Homomorphismus*) von A nach B ist ein Monoidhomomorphismus $\varphi\colon A \to B$.

(b) (i) Es seien Gruppen G und H gegeben. Ein *Gruppenhomomorphismus* (oder *Homomorphismus von Gruppen* oder *Homomorphismus*) von G nach H ist ein Monoidhomomorphismus $\varphi\colon G \to H$ so, dass folgendes Axiom gilt.

- *Verträglichkeit der inversen Elemente.* Für alle $x \in G$ ist
$$\varphi((x^{-1})^G) = (\varphi(x)^{-1})^H.$$

(ii) Es seien abelsche Gruppen A und B gegeben. Ein *Homomorphismus abelscher Gruppen* (oder *Homomorphismus von abelschen Gruppen* oder *Homomorphismus*) von A nach B ist ein Gruppenhomomorphismus $\varphi\colon A \to B$.
Die *Menge aller Homomorphismen abelscher Gruppen* von A nach B bezeichnen wir mit
$$\begin{aligned}\mathrm{Hom}(A,B) &= \mathrm{Hom}_{\mathbf{AbGrp}}(A,B)\\ &:= \{\varphi \in \mathrm{Map}(A,B) \mid \varphi \text{ ist ein Homomorphismus abelscher Gruppen}\}.\end{aligned}$$

Die Verträglichkeit mit den Multiplikationen eines Monoidhomomorphismus $M \to N$ besagt, dass es egal ist, ob wir zuerst zwei Elemente von M miteinander in M multiplizieren und das Produkt nach N abbilden oder ob wir zunächst die beiden Faktoren von M nach N abbilden und erst deren Bilder in N multiplizieren.
Die Axiome eines Homomorphismus abelscher Gruppen $\varphi\colon A \to B$ in additiver (Kurz-)Notation lesen sich wie folgt:

- *Verträglichkeit mit den Additionen.* Für alle $x, x' \in A$ ist $\varphi(x + x') = \varphi(x) + \varphi(x')$.
- *Verträglichkeit der Nullelemente.* Es ist $\varphi(0) = 0$.
- *Verträglichkeit der negativen Elemente.* Für alle $x \in A$ ist $\varphi(-x) = -\varphi(x)$.

Es kommt auch vor, dass wir Homomorphismen von einer additiv geschriebenen (also abelschen) Struktur in eine multiplikativ geschriebene Struktur, oder umgekehrt, betrachten, siehe etwa Beispiel (1.65)(b).
Genauso wie Start- und Zielmenge Bestandteil einer Abbildung sein sollen, möchten wir, dass ein Monoidhomomorphismus $\varphi\colon M \to N$ von einem Monoid M zu einem Monoid N aus der unterliegenden Abbildung $\varphi\colon M \to N$ sowie den Monoiden M und N besteht, auch wenn wir das nicht explizit dazu sagen. Ähnlich für Gruppen und andere Strukturen, welche im Laufe der Vorlesung noch auftauchen werden.
Sind also Monoidhomorphismen $\varphi\colon M \to N$ und $\varphi\colon M' \to N'$ gegeben, so gilt genau dann $\varphi = \varphi'$ als Monoidhomomorphismen, wenn $M = M'$ und $N = N'$ als Monoide und $\varphi = \varphi'$ als Abbildungen gilt.

(1.65) Beispiel.

(a) Die Inklusion $\mathrm{inc}\colon \mathbb{N}_0 \to \mathbb{Z}$ ist ein Homomorphismus abelscher Monoide (wobei wir beide Mengen als abelsche Monoide bzgl. der uns vertrauten Additionen auffassen). Die Inklusion $\mathrm{inc}\colon \mathbb{Z} \to \mathbb{Q}$ ist ein Homomorphismus abelscher Gruppen (wobei wir beide Mengen als abelsche Gruppen bzgl. der uns vertrauten Additionen auffassen).

(b) Es wird $\mathbb{R}$ eine abelsche Gruppe mit Addition $(x, y) \mapsto x + y$ (die uns vertraute Addition der reellen Zahlen). Es wird $\mathbb{R}_{>0} = \{x \in \mathbb{R} \mid x > 0\}$ eine (kommutative) Gruppe mit Multiplikation $(x, y) \mapsto x \cdot y$ (die uns vertraute Multiplikation der reellen Zahlen). Bzgl. diesen Strukturen sind die Exponentialfunktion $\exp\colon \mathbb{R} \to \mathbb{R}_{>0}$ und die (natürliche) Logarithmusfunktion $\log\colon \mathbb{R}_{>0} \to \mathbb{R}$ sich gegenseitig invertierende Gruppenhomomorphismen.

(1.66) Bemerkung. Es sei ein Monoidhomomorphismus $\varphi\colon M \to N$ gegeben. Für jedes invertierbare Element $x \in M$ ist $\varphi(x)$ invertierbar in N mit

$$\varphi(x)^{-1} = \varphi(x^{-1}).$$

Beweis. Es sei ein invertierbares Element $x \in M$ gegeben. Dann ist

$$\varphi(x^{-1})\,\varphi(x) = \varphi(x^{-1}x) = \varphi(1) = 1,$$
$$\varphi(x)\,\varphi(x^{-1}) = \varphi(xx^{-1}) = \varphi(1) = 1.$$

Folglich ist $\varphi(x)$ invertierbar in N mit $\varphi(x)^{-1} = \varphi(x^{-1})$. □

(1.67) Lemma. Es seien Gruppen G und H und eine Abbildung $\varphi\colon G \to H$ gegeben. Genau dann ist φ ein Gruppenhomomorphismus, wenn

$$\varphi(xx') = \varphi(x)\,\varphi(x')$$

für alle $x, x' \in G$ gilt.

Beweis. Wenn φ ein Gruppenhomomorphismus ist, dann gilt insbesondere $\varphi(xx') = \varphi(x)\,\varphi(x')$ für alle $x, x' \in G$. Es gelte also umgekehrt $\varphi(xx') = \varphi(x)\,\varphi(x')$ für alle $x, x' \in G$. Dann ist insbesondere

$$\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\,\varphi(1).$$

Nun ist aber H eine Gruppe und damit insbesondere $\varphi(1)$ invertierbar in H, so dass

$$\varphi(1) = 1$$

folgt. Damit ist φ ein Monoidhomomorphismus. Nach Bemerkung (1.66) gilt nun aber $\varphi(x)^{-1} = \varphi(x^{-1})$ für alle $x \in G^\times = G$, d.h. φ ist sogar ein Gruppenhomomorphismus. □

Wir betonen, dass Lemma (1.67) nur für Abbildungen zwischen Gruppen gültig ist, nicht jedoch für beliebige Abbildungen zwischen Monoiden.

(1.68) Beispiel.

(a) Es sei ein Monoid M gegeben. Für alle $x \in M$ ist

$$\mathbb{N}_0 \to M,\ k \mapsto x^k$$

ein Monoidhomomorphismus.

(b) Es sei eine Gruppe G gegeben. Für alle $x \in G$ ist

$$\mathbb{Z} \to G,\ k \mapsto x^k$$

ein Gruppenhomomorphismus.

Beweis.

(a) Dies folgt aus dem Potenzgesetz (1.63)(a).

(b) Dies folgt aus dem Potenzgesetz (1.63)(a) und Lemma (1.67). □

Untergruppen

Zum Abschluss dieses Abschnitts betrachten wir noch das Konzept der Unterstrukturen: dies sind algebraische Strukturen, die elementweise innerhalb einer umgebenden algebraischen Struktur enthalten sind und deren Struktur (etwa die Verknüpfungen) sich durch Restriktion der umgebenden Struktur ergibt. Wir begnügen uns mit der Variante für Gruppen.

(1.69) Definition ((abelsche) Untergruppe)**.**

(a) Es sei eine Gruppe G gegeben. Eine *Untergruppe* von G ist eine Gruppe U so, dass die unterliegende Menge von U eine Teilmenge von G ist und so, dass folgende Axiome gelten.

- *Verträglichkeit der Multiplikationen.* Für alle $x, x' \in U$ gilt
$$x \cdot^U x' = x \cdot^G x'.$$
- *Verträglichkeit der Einselemente.* Es ist
$$1^U = 1^G.$$
- *Verträglichkeit der inversen Elemente.* Für alle $x \in U$ ist
$$(x^{-1})^U = (x^{-1})^G.$$

Eine Untergruppe U von G heißt *echt* (oder *strikt*), falls $U \neq G$ gilt.

Ist U eine Untergruppe von G, so schreiben wir $U \leq G$. Ist U keine Untergruppe von G, so schreiben wir $U \not\leq G$. Ist U eine echte Untergruppe von G, so schreiben wir $U < G$.

(b) Es sei eine abelsche Gruppe A gegeben. Eine *abelsche Untergruppe* von A ist eine Untergruppe von A.

Die Axiome einer abelschen Untergruppe U einer abelschen Gruppe A in additiver Notation lesen sich wie folgt:

- *Verträglichkeit der Additionen.* Für alle $x, x' \in U$ gilt $x +^U x' = x +^A x'$.
- *Verträglichkeit der Nullelemente.* Es ist $0^U = 0^A$.
- *Verträglichkeit der negativen Elemente.* Für alle $x \in A$ ist $(-x)^U = (-x)^A$.

(1.70) Beispiel.

(a) Es wird $\mathbb{Z}$ eine abelsche Gruppe mit Addition $(x, y) \mapsto x + y$ (die uns vertraute Addition der ganzen Zahlen). Es wird $\mathbb{Q}$ eine abelsche Gruppe mit Addition $(x, y) \mapsto x + y$ (die uns vertraute Addition der rationalen Zahlen). Mit diesen Strukturen ist $\mathbb{Z}$ eine abelsche Untergruppe von $\mathbb{Q}$.

(b) Es wird $\mathbb{Z}^\times = \{1, -1\}$ eine Gruppe mit Multiplikation $(x, y) \mapsto x \cdot y$ (die uns vertraute Multiplikation der ganzen Zahlen). Es wird $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$ eine Gruppe mit Multiplikation $(x, y) \mapsto x \cdot y$ (die uns vertraute Multiplikation der rationalen Zahlen). Bzgl. dieser Struktur ist $\mathbb{Z}^\times$ eine Untergruppe von $\mathbb{Q}^\times$.

(1.71) Bemerkung. Es seien Gruppen G und U so gegeben, dass die unterliegende Menge von U eine Teilmenge von G ist. Genau dann ist U eine Untergruppe von G, wenn die Inklusion $\mathrm{inc}\colon U \to G$ ein Gruppenhomomorphismus ist.

(1.72) Korollar. Es seien Gruppen G und U so gegeben, dass die unterliegende Menge von U eine Teilmenge von G ist. Genau dann ist U eine Untergruppe von G, wenn
$$x \cdot^U x' = x \cdot^G x'$$
für alle $x, x' \in U$ gilt.

Beweis. Dies folgt aus Bemerkung (1.71) und Lemma (1.67). □

(1.73) Konvention. Es seien eine Gruppe G und eine Teilmenge U von G gegeben. Da die Gruppenverknüpfung jeder Untergruppe von G vollständig durch die Gruppenverknüpfung von G bestimmt ist, gibt es höchstens eine Gruppenstruktur auf U so, dass U mit dieser Gruppenstruktur eine Untergruppe von G wird. Wir sagen daher auch, dass U eine Untergruppe von G *ist*, falls so eine Gruppenstruktur auf U existiert.

(1.74) Lemma (Untergruppenkriterium)**.** Es seien eine Gruppe G und eine Teilmenge U von G gegeben. Die folgenden Bedingungen sind äquivalent.

(a) Es ist U eine Untergruppe von G.

(b) Es gilt:

- *Abgeschlossenheit unter Multiplikation.* Für alle $x, x' \in U$ ist
$$xx' \in U.$$
- *Abgeschlossenheit unter der Eins.* Es ist
$$1 \in U.$$
- *Abgeschlossenheit unter Inversenbildung.* Für alle $x \in U$ ist
$$x^{-1} \in U.$$

(c) Es gilt:

- Es ist
$$U \neq \emptyset.$$
- Für alle $x, x' \in U$ ist
$$x^{-1}x' \in U.$$

Beweis. Wir zeigen zuerst die Äquivalenz von Bedingung (a) und Bedingung (b), danach die Äquivalenz von Bedingung (b) und Bedingung (c).
Es gelte zunächst Bedingung (a), d.h. es sei U eine Untergruppe von G. Für $x, x' \in U$ ist dann $x \cdot^G x' = x \cdot^U x' \in U$, es ist $1^G = 1^U \in U$, und für $x \in U$ ist $(x^{-1})^G = (x^{-1})^U \in U$. Folglich gilt Bedingung (b).
Nun gelte umgekehrt Bedingung (b). Da für $x, x' \in U$ stets $x \cdot^G x' \in U$ ist, können wir U als Magma mit der Multiplikation $(x, x') \mapsto x \cdot^G x'$ auffassen, so dass also $x \cdot^U x' = x \cdot^G x'$ gilt. Wir wollen zeigen, dass das Magma U eine Gruppe ist. Für $x, x', x'' \in U$ gilt

$$x \cdot^U (x' \cdot^U x'') = x \cdot^G (x' \cdot^G x'') = (x \cdot^G x') \cdot^G x'' = (x \cdot^U x') \cdot^U x'',$$

d.h. $\cdot^U$ ist assoziativ und damit U eine Halbgruppe. Ferner ist $1^G \in U$ und für $x \in U$ gilt

$$1^G \cdot^U x = 1^G \cdot^G x = x,$$

d.h. 1^G ist linksneutrales Element in U bzgl. $\cdot^U$. Schließlich ist für $x \in U$ auch $(x^{-1})^G \in U$ und es gilt

$$(x^{-1})^G \cdot^U x = (x^{-1})^G \cdot^G x = 1^G,$$

d.h. $(x^{-1})^G$ ist linksinvers zu x bzgl. $\cdot^U$ und 1^G. Nach Lemma (1.54) ist U also in der Tat eine Gruppe. Nach Definition der Multiplikation von U und Korollar (1.72) ist U dann aber sogar eine Untergruppe von G, d.h. es gilt Bedingung (a).
Folglich sind Bedingung (a) und Bedingung (b) äquivalent.
Als nächstes gelte Bedingung (b). Da U abgeschlossen unter der Eins ist, gilt $1^G \in U$, also insbesondere $U \neq \emptyset$. Sind $x, x' \in U$ gegeben, so ist ferner $(x^{-1})^G \in U$, da U abgeschlossen unter Inversenbildung ist, und folglich $(x^{-1})^G \cdot^G x' \in U$, da U abgeschlossen unter der Multiplikation ist. Wir haben somit Bedingung (c) gezeigt.
Schließlich gelte Bedingung (c). Da $U \neq \emptyset$ ist, gibt es ein Element $x_0 \in U$, und somit folgt $1 = x_0^{-1}x_0 \in U$. Für $x \in U$ ist außerdem $x^{-1} = x^{-1} \cdot 1 \in U$. Schließlich folgt für $x, x' \in U$, dass $xx' = (x^{-1})^{-1}x' \in U$ ist. Insgesamt gilt Bedingung (b).
Folglich sind Bedingung (b) und Bedingung (c) äquivalent.
Insgesamt sind Bedingung (a), Bedingung (b) und Bedingung (c) äquivalent. □

(1.75) Beispiel. Es wird $\mathbb{Z}$ eine abelsche Gruppe mit Addition $(x, y) \mapsto x + y$ (die uns vertraute Addition der ganzen Zahlen). Bzgl. dieser Struktur ist $2\mathbb{Z} := \{2x \mid x \in \mathbb{Z}\}$ eine Untergruppe von $\mathbb{Z}$.

Beweis. Zunächst ist $0 = 2 \cdot 0 \in 2\mathbb{Z}$ und damit $2\mathbb{Z} \neq \emptyset$. Es seien $y, y' \in 2\mathbb{Z}$ gegeben. Dann gibt es $x, x' \in \mathbb{Z}$ mit $y = 2x$, $y' = 2x'$, und es folgt $-y + y' = -2x + 2x' = 2(-x + x') \in 2\mathbb{Z}$. Nach dem Untergruppenkriterium (1.74) ist somit $2\mathbb{Z}$ eine Untergruppe von $\mathbb{Z}$. □

Aufgaben

Aufgabe 11 (Inversionsregeln)**.** Es sei ein Monoid M gegeben. Zeigen Sie:

(a) Für $x, y \in M^\times$ ist auch $xy \in M^\times$ mit $(xy)^{-1} = y^{-1}x^{-1}$.

(b) Es ist $1 \in M^\times$ mit $1^{-1} = 1$.

(c) Für $x \in M^\times$ ist auch $x^{-1} \in M^\times$ mit $(x^{-1})^{-1} = x$.

Aufgabe 12 (symmetrische Gruppe)**.** Nach Beispiel (1.52)(e) ist $\mathrm{Map}(X, X)$ zusammen mit der Verknüpfung $(g, f) \mapsto g \circ f$ im Allgemeinen keine Gruppe. Finden Sie eine geeignete Teilmenge S von $\mathrm{Map}(X, X)$ so, dass S mit der auf S *eingeschränkten* Verknüpfung $S \times S \to S$, $(g, f) \mapsto g \circ f$ eine Gruppe wird.

Aufgabe 13 (Einheitengruppe)**.** Es sei ein Monoid M gegeben. Zeigen Sie, dass

$$M^\times := \{x \in M \mid x \text{ invertierbar in } M\}$$

zusammen mit der von M vererbten Multiplikation eine Gruppe ist.

Aufgabe 14 (Linksmultiplikation)**.** Es seien eine Gruppe G und ein $g \in G$ gegeben. Zeigen Sie, dass die Abbildung $G \to G$, $x \mapsto gx$ bijektiv ist.

Aufgabe 15 (kommutative Gruppen)**.** Es sei G eine Gruppe. Für $g \in G$ sei $g^2 := gg$. Zeigen Sie:

(a) Genau dann ist G kommutativ, wenn $(gh)^2 = g^2h^2$ für alle $g, h \in G$ gilt.

(b) Wenn $g^2 = 1$ für alle $g \in G$ gilt, dann ist G kommutativ.

(c) Wenn $g = g^{-1}$ für alle $g \in G$ gilt, dann ist G kommutativ.

Aufgabe 16 (direktes Produkt)**.** Es seien Gruppen G_1 und G_2 gegeben. Zeigen Sie, dass $G_1 \times G_2$ zu einer Gruppe mit Multiplikation $((x_1, x_2), (y_1, y_2)) \mapsto (x_1y_1, x_2y_2)$ wird. Zeigen Sie weiter, dass $G_1 \times G_2$ kommutativ ist, falls G_1 und G_2 kommutativ sind.

Aufgabe 17 (abelsche Gruppen)**.** Reformulieren Sie die Aussagen aus Abschnitt 4 für abelsche Gruppen (d.h. übersetzen Sie alles in die additive Schreibweise). Beginnen Sie mit den Axiomen.

Aufgabe 18 (Bild eines Gruppenhomomorphismus)**.** Es sei ein Gruppenhomomorphismus $\varphi\colon G \to H$ gegeben. Zeigen Sie, dass $\mathrm{Im}\,\varphi$ eine Untergruppe von H ist.

Aufgabe 19 (Gruppenhomomorphismen)**.** Wir betrachten $\mathbb{R} \setminus \{0\}$ als kommutative Gruppe bzgl. der gewöhnlichen Multiplikation. Zeigen Sie, dass Absolutbetrag

$$|-|\colon \mathbb{R} \setminus \{0\} \to \mathbb{R} \setminus \{0\},\ x \mapsto |x|$$

und Signum

$$\mathrm{sgn}\colon \mathbb{R} \setminus \{0\} \to \mathbb{R} \setminus \{0\},\ x \mapsto \mathrm{sgn}\, x$$

Gruppenhomomorphismen sind und bestimmen Sie jeweils das Bild.

Aufgabe 20 (algebraische Eigenschaften von Gruppenhomomorphismen)**.**

(a) Es seien Gruppenhomomorphismen $\varphi\colon G \to H$ und $\psi\colon H \to K$ gegeben. Zeigen Sie, dass $\psi \circ \varphi\colon G \to K$ ebenfalls ein Gruppenhomomorphismus ist.

(b) Es sei eine Gruppe G gegeben. Zeigen Sie, dass $\mathrm{id}_G\colon G \to G$ ein Gruppenhomomorphismus ist.

(c) Es sei ein Gruppenhomomorphismus $\varphi\colon G \to H$ so gegeben, dass φ als Abbildung invertierbar ist. Zeigen Sie, dass $\varphi^{-1}\colon B \to A$ ebenfalls ein Gruppenhomomorphismus ist.

Aufgabe 21 (Homomorphismenmenge als abelsche Gruppe)**.** Es seien abelsche Gruppen A und B gegeben. Zeigen Sie, dass $\mathrm{Hom}(A, B)$ eine abelsche Gruppe wird, mit Addition gegeben durch

$$(\varphi + \psi)(x) = \varphi(x) + \psi(x)$$

für $x \in A$, $\varphi, \psi \in \mathrm{Hom}(A, B)$.

Aufgabe 22 (Schnitt und Summe von abelschen Untergruppen)**.** Es seien eine abelsche Gruppe A und abelsche Untergruppen U und V von A gegeben.

(a) Zeigen Sie, dass $U \cap V$ eine Untergruppe von A ist.

(b) Zeigen Sie, dass

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

eine Untergruppe von A ist. Man nennt $U + V$ die *Summe* von U und V in A.

Aufgabe 23 (Endomorphismen von $\mathbb{Z}$)**.** Es sei $n \in \mathbb{Z}$ gegeben. Zeigen Sie:

(a) Es ist $\mathbb{Z} \to \mathbb{Z}$, $x \mapsto xn$ ein Homomorphismus abelscher Gruppen.

(b) Es ist $\mathbb{Z}n$ eine abelsche Untergruppe von $\mathbb{Z}$.

Aufgabe 24 (abelsche Untergruppen von $\mathbb{Z}$)**.** Es sei eine abelsche Gruppe A gegeben. Eine abelsche Untergruppe U von A heißt *maximal*, wenn U eine echte abelsche Untergruppe von A ist und es keine echte abelsche Untergruppe U' von A so gibt, dass U eine echte abelsche Untergruppe von U' ist.

(a) Bestimmen Sie alle abelschen Untergruppen von $\mathbb{Z}$.

(b) Welche abelschen Untergruppen von $\mathbb{Z}$ sind ineinander enthalten?

(c) Wieviele endliche abelsche Untergruppen hat $\mathbb{Z}$?

(d) Welche abelschen Untergruppen von $\mathbb{Z}$ sind maximal?

Aufgabe 25 (Lemma von Bézout)**.** Es seien $m, n \in \mathbb{Z}$ mit $(m, n) \neq (0, 0)$ gegeben. Ein *größter gemeinsamer Teiler* von m und n ist eine Zahl $g \in \mathbb{Z}$ so, dass $g \mid m$ und $g \mid n$ sowie $d \mid g$ für alle $d \in \mathbb{Z}$ mit $d \mid m$ und $d \mid n$ gilt. Man kann zeigen (etwa mit Hilfe der Primfaktorzerlegung), dass es stets einen größten gemeinsamen Teiler von m und n gibt und dass dieser bis auf Vorzeichen eindeutig bestimmt ist. Wir schreiben $\gcd(m, n)$ für den eindeutig bestimmten nicht-negativen größten gemeinsamen Teiler von m und n.
Zeigen Sie:

(a) Es ist $\mathbb{Z}m + \mathbb{Z}n = \gcd(m, n)\mathbb{Z}$.

(b) Es existieren $x, y \in \mathbb{Z}$ mit $\gcd(m, n) = xm + yn$.

5 Die symmetrische Gruppe

In diesem Abschnitt werden wir eine ganze Serie von Gruppen, die sogenannten symmetrischen Gruppen, etwas genauer studieren.

Definition der symmetrischen Gruppe

Für jede Menge X wird $\mathrm{Map}(X,X) = \{f \mid f \text{ ist eine Abbildung von } X \text{ nach } X\}$ ein im Allgemeinen nichtkommutatives Monoid mit Monoidverknüpfung $(g,f) \mapsto g \circ f$ und Einselement id_X, siehe Beispiel (1.41)(e) und Beispiel (1.44)(e).

(1.76) Definition (symmetrische Gruppe)**.**

(a) Es sei eine Menge X gegeben. Die Gruppe

$$\mathrm{S}_X := \mathrm{Map}(X,X)^\times$$

heißt *symmetrische Gruppe* auf X. Ihre Elemente werden *Permutationen* von X genannt.

(b) Es sei $n \in \mathbb{N}$ gegeben. Wir nennen

$$\mathrm{S}_n := \mathrm{S}_{[1,n]}$$

auch die *symmetrische Gruppe vom Grad n*. Für $\pi \in \mathrm{S}_n$ schreiben wir

$$\left(\begin{smallmatrix} 1 & 2 & 3 & \dots & n \\ \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n) \end{smallmatrix}\right) := \pi.$$

Es besteht S_X für eine Menge X also gerade aus allen invertierbaren Abbildungen $X \to X$.

(1.77) Beispiel.

(a) Es ist

$$\mathrm{S}_1 = \{\mathrm{id}_{\{1\}}\} = \{\left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right)\}.$$

(b) Es ist

$$\mathrm{S}_2 = \{\mathrm{id}_{\{1,2\}}, (1 \mapsto 2,\, 2 \mapsto 1)\} = \{\left(\begin{smallmatrix} 1 & 2 \\ 1 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 \\ 2 & 1 \end{smallmatrix}\right)\}.$$

(c) Es ist

$$\mathrm{S}_3 = \{\left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix}\right)\}.$$

Man beachte, dass wir beim Bilden von Komposita – wie immer – von rechts nach links lesen:

(1.78) Beispiel. In S_3 ist

$$\left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right) \circ \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix}\right),$$
$$\left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}\right) \circ \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right).$$

Zykelschreibweise

Die klassische Schreibweise für Permutationen ist für viele Zwecke noch etwas schwerfällig. Wir führen nun die Zykelschreibweise ein.

(1.79) Definition (Zykel)**.** Es sei $n \in \mathbb{N}$ gegeben.

(a) Es seien $l \in [1,n]$ und verschiedene Elemente $j_k \in [1,n]$ für $k \in [1,l]$ gegeben. Die Permutation $\zeta \in \mathrm{S}_n$ gegeben durch

$$\zeta(i) = \begin{cases} j_{k+1}, & \text{falls } i = j_k \text{ für ein } k \in [1,l-1], \\ j_1, & \text{falls } i = j_l, \\ i, & \text{falls } i \notin \{j_k \mid k \in [1,l]\}, \end{cases}$$

heißt *Zykel der Länge l* (oder *l-Zykel*) zu $(j_1,\dots,j_l)$ und wird unter Missbrauch der Notation mit

$$(j_1,\dots,j_l) := \zeta$$

bezeichnet. Ferner schreiben wir

$$\mathrm{lth}(j_1,\dots,j_l) := l$$

für die *Länge* von $(j_1,\dots,j_l)$.

(b) Für $l \in [1,n]$ ist ein *l-Zykel* in S_n ein l-Zykel zu $(j_1,\dots,j_l)$ für gewisse verschiedene $j_k \in [1,n]$ für $k \in [1,l]$. Ein *Zykel* in S_n ist ein l-Zykel in S_n für ein $l \in [1,n]$. Ein Zykel der Länge 1 heißt *trivial*, sonst *nicht-trivial*.

(1.80) Notation. Bei der Komposition von Zykeln wird das Kompositionssymbol meistens weggelassen.

(1.81) Beispiel.

(a) In S_3 ist

$$\left(\begin{smallmatrix}1&2&3\\2&1&3\end{smallmatrix}\right) = (1,2),$$
$$\left(\begin{smallmatrix}1&2&3\\2&3&1\end{smallmatrix}\right) = (1,2,3).$$

(b) Die Permutation $\left(\begin{smallmatrix}1&2&3&4&5\\2&1&3&5&4\end{smallmatrix}\right)$ in S_5 ist kein Zykel. Stattdessen haben wir

$$\left(\begin{smallmatrix}1&2&3&4&5\\2&1&3&5&4\end{smallmatrix}\right) = (1,2,3)(4,5).$$

Wir zitieren nun einen Satz, der erst später, etwa in einer Vorlesung über *Algebra*, formal bewiesen wird.

(1.82) Satz. Es sei $n \in \mathbb{N}$ gegeben. Jede Permutation $\pi \in \mathrm{S}_n$ lässt sich (bis auf die Reihenfolge) eindeutig als Kompositum von paarweise disjunkten nicht-trivialen Zykeln schreiben.

Ohne Beweis. □

Dabei heißen Zykel $(j_1,\dots,j_l)$ und $(j'_1,\dots,j'_l)$ *disjunkt*, falls $\{j_k \mid k \in [1,l]\}$ und $\{j'_k \mid k \in [1,l']\}$ disjunkt sind, d.h. falls $\{j_k \mid k \in [1,l]\} \cap \{j'_k \mid k \in [1,l']\} = \emptyset$ ist.

(1.83) Definition (Zykelzerlegung)**.** Es seien $n \in \mathbb{N}$ und $\pi \in \mathrm{S}_n$ gegeben. Die Menge $Z \subseteq \mathrm{S}_n$ der paarweise disjunkten nicht-trivialen Zykeln mit $\pi = \bigcirc_{\zeta \in Z} \zeta$ heißt *Zykelzerlegung* von π.

Transpositionen

Die Zykel der Länge 2 bilden die „Grundbausteine“ in der symmetrischen Gruppe S_n für $n \in \mathbb{N}$, wie wir im Folgenden sehen werden.

(1.84) Definition (Transposition, Nachbartransposition)**.** Es sei $n \in \mathbb{N}$ gegeben.

(a) Eine *Transposition* (oder *Vertauschung*) in S_n ist ein Zykel der Länge 2.

(b) Eine *Nachbartransposition* in S_n ist eine Transposition der Form $(j,j+1)$ für ein $j \in [1,n-1]$.

(1.85) Bemerkung. Es sei $n \in \mathbb{N}$ gegeben. Für jede Transposition (i,j) in S_n und alle $k \in [1,n]$ gilt

$$(i,j) = (j,k)(i,k)(k,j).$$

(1.86) Bemerkung. Es sei $n \in \mathbb{N}$ gegeben.

(a) Es sei $l \in \mathbb{N}_0$. Für jeden l-Zykel $(j_1,\dots,j_l)$ in S_n gilt

$$(j_1,\dots,j_l) = (j_1,j_l)\dots(j_1,j_2) = (j_1,j_2)\dots(j_{l-1},j_l).$$

(b) Für jede Transposition (i,j) in S_n mit $i<j$ gilt

$$(i,j) = (j,j-1)\dots(i+2,i+1)(i,i+1)(i+1,i+2)\dots(j-1,j).$$

Beweis.

(b) Wir führen Induktion nach $j-i$, wobei für $j-i=1$ nichts zu tun ist. Es sei also $j-i>1$ und gelte

$$(i,j-1) = (j-1,j-2)\dots(i+2,i+1)(i,i+1)(i+1,i+2)\dots(j-2,j-1).$$

Dann ist nach Bemerkung (1.85) aber auch

$$\begin{aligned}(i,j) &= (j,j-1)(i,j-1)(j-1,j)\\ &= (j,j-1)(j-1,j-2)\dots(i+2,i+1)(i,i+1)(i+1,i+2)\dots(j-2,j-1)(j-1,j).\end{aligned}$$ □

(1.87) Proposition. Es sei $n \in \mathbb{N}$ gegeben. Jedes $\pi \in \mathrm{S}_n$ ist ein Kompositum von Nachbartranspositionen.

Beweis. Dies folgt aus Satz (1.82) und Bemerkung (1.86). □

(1.88) Beispiel.

(a) In S_9 ist

$$(1,4,7,3,5)(2,8,6,9) = (1,4)(4,7)(7,3)(3,5)(2,8)(8,6)(6,9).$$

(b) In S_9 ist

$$(1,4) = (4,3)(3,2)(1,2)(2,3)(3,4).$$

Signum

Die Darstellung einer Permutation als ein Kompositum von Transpositionen ist nicht eindeutig, wie man bereits an Bemerkung (1.86) erkennt. Wir werden jedoch zeigen, dass zumindest die Parität der Anzahl der Transpositionen festgelegt ist, siehe Aufgabe 35: Lässt sich eine Permutation als ein Kompositum einer geraden Anzahl an Permutationen schreiben, dann nicht als ein Kompositum einer ungeraden Anzahl an Permutationen (und umgekehrt).
Um dies zu zeigen, zählen wir diejenigen Paare, bei welchen unter einer Permutation die Ordnungsbeziehung vertauscht wird.

(1.89) Definition (Fehlstand)**.** Es seien $n \in \mathbb{N}$ und $\pi \in \mathrm{S}_n$ gegeben. Ein Paar $(i,j) \in [1,n] \times [1,n]$ heißt *Fehlstand* (oder *Inversionspaar*) von π, falls $i < j$ und $\pi(i) > \pi(j)$ ist.
Die *Menge aller Fehlstände* von π bezeichnen wir mit

$$\mathrm{Inv}(\pi) := \{(i,j) \in [1,n] \times [1,n] \mid i < j,\ \pi(i) > \pi(j)\}.$$

(1.90) Beispiel. Es ist

$$\mathrm{Inv}(\left(\begin{smallmatrix}1&2&3&4\\3&4&1&2\end{smallmatrix}\right)) = \{(1,3),(1,4),(2,3),(2,4)\}.$$

(1.91) Bemerkung. Es seien $n \in \mathbb{N}$ und $j \in [1, n-1]$ gegeben.

(a) Es ist

$$\mathrm{Inv}((j,j+1)) = \{(j,j+1)\}.$$

(b) Für $\pi \in \mathrm{S}_n$ ist

$$\begin{aligned}\mathrm{Inv}(\pi \circ (j,j+1)) = {} & \{(i,i') \mid (i,i') \in \mathrm{Inv}(\pi),\ i,i' \notin \{j,j+1\}\} \,\dot\cup\, \{(i,j+1) \mid (i,j) \in \mathrm{Inv}(\pi)\} \\ & \dot\cup\, \{(j+1,i) \mid (j,i) \in \mathrm{Inv}(\pi)\} \,\dot\cup\, \{(i,j) \mid (i,j+1) \in \mathrm{Inv}(\pi)\} \\ & \dot\cup\, \{(j,i) \mid (j+1,i) \in \mathrm{Inv}(\pi)\} \,\dot\cup\, S,\end{aligned}$$

wobei

$$S = \begin{cases}\{(j,j+1)\}, & \text{falls } (j,j+1) \notin \mathrm{Inv}(\pi), \\ \emptyset, & \text{falls } (j,j+1) \in \mathrm{Inv}(\pi).\end{cases}$$

Beweis.

(b) Es sei $\pi \in \mathrm{S}_n$ gegeben und es sei $\sigma := \pi \circ (j,j+1)$. Für $i \in [1,n]$ ist

$$\sigma(i) = \begin{cases}\pi(j+1), & \text{falls } i = j, \\ \pi(j), & \text{falls } i = j+1, \\ \pi(i), & \text{falls } i \notin \{j,j+1\}.\end{cases}$$

Folglich gilt: Für $i,i' \in [1,n]\backslash\{j,j+1\}$ ist genau dann $(i,i') \in \mathrm{Inv}(\sigma)$, wenn $(i,i') \in \mathrm{Inv}(\pi)$. Für $i \in [1,j-1]$ ist genau dann $(i,j+1) \in \mathrm{Inv}(\sigma)$, wenn $(i,j) \in \mathrm{Inv}(\pi)$. Für $i \in [j+2,n]$ ist genau dann $(j+1,i) \in \mathrm{Inv}(\sigma)$, wenn $(j,i) \in \mathrm{Inv}(\pi)$. Für $i \in [1,j-1]$ ist genau dann $(i,j) \in \mathrm{Inv}(\sigma)$, wenn $(i,j+1) \in \mathrm{Inv}(\pi)$. Für $i \in [j+2,n]$ ist genau dann $(j,i) \in \mathrm{Inv}(\sigma)$, wenn $(j+1,i) \in \mathrm{Inv}(\pi)$. Genau dann ist $(j,j+1) \in \mathrm{Inv}(\sigma)$, wenn $(j,j+1) \notin \mathrm{Inv}(\sigma)$. □

(1.92) Definition (Signum)**.** Es seien $n \in \mathbb{N}$ und $\pi \in \mathrm{S}_n$ gegeben. Das *Signum* (oder *Vorzeichen*) von π ist definiert als

$$\operatorname{sgn} \pi := (-1)^{|\operatorname{Inv}(\pi)|}.$$

(1.93) Beispiel. Es ist

$$\operatorname{sgn} \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{smallmatrix} \right) = 1.$$

Beweis. Nach Beispiel (1.90) ist

$$\operatorname{Inv}(\left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{smallmatrix} \right)) = \{(1,3), (1,4), (2,3), (2,4)\},$$

also

$$\operatorname{sgn} \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{smallmatrix} \right) = (-1)^4 = 1.$$ □

(1.94) Bemerkung. Es seien $n \in \mathbb{N}$ und $j \in [1, n-1]$ gegeben.

(a) Es ist

$$\operatorname{sgn} (j, j+1) = -1.$$

(b) Für $\pi \in \mathrm{S}_n$ ist

$$\operatorname{sgn}(\pi \circ (j, j+1)) = -\operatorname{sgn} \pi.$$

Beweis.

(a) Nach Bemerkung (1.91)(a) ist

$$\operatorname{Inv}((j, j+1)) = \{(j, j+1)\},$$

also

$$\operatorname{sgn} (j, j+1) = (-1)^{|\operatorname{Inv}((j,j+1))|} = (-1)^1 = -1.$$ □

(b) Nach Bemerkung (1.91)(b) ist

$$|\operatorname{Inv}(\pi \circ (j, j+1))| = \begin{cases} |\operatorname{Inv}(\pi)| + 1, & \text{falls } (j, j+1) \notin \operatorname{Inv}(\pi), \\ |\operatorname{Inv}(\pi)| - 1, & \text{falls } (j, j+1) \in \operatorname{Inv}(\pi), \end{cases}$$

also

$$\operatorname{sgn}(\pi \circ (j, j+1)) = (-1)^{|\operatorname{Inv}(\pi \circ (j,j+1))|} = (-1)^{|\operatorname{Inv}(\pi)|} \cdot (-1) = (\operatorname{sgn} \pi)(-1) = -\operatorname{sgn} \pi.$$

(1.95) Proposition. Für $n \in \mathbb{N}$ ist

$$\operatorname{sgn} \colon \mathrm{S}_n \to \mathbb{Z}^\times$$

ein Gruppenhomomorphismus.

Beweis. Es sei $n \in \mathbb{N}$ gegeben. Wir zeigen durch Induktion nach $l \in \mathbb{N}_0$: Für $\pi, \sigma \in \mathrm{S}_n$ so, dass σ ein Kompositum von l Nachbartranspositionen ist, gilt $\operatorname{sgn}(\pi \circ \sigma) = (\operatorname{sgn} \pi)(\operatorname{sgn} \sigma)$.
Für $l = 0$ gilt $\sigma = \mathrm{id}_{[1,n]}$, also

$$\operatorname{sgn}(\pi \circ \sigma) = \operatorname{sgn}(\pi \circ \mathrm{id}_{[1,n]}) = \operatorname{sgn} \pi = \operatorname{sgn} \pi \cdot 1 = (\operatorname{sgn} \pi)(\operatorname{sgn} \mathrm{id}_{[1,n]}) = (\operatorname{sgn} \pi)(\operatorname{sgn} \sigma)$$

für alle $\pi \in \mathrm{S}_n$.
Es sei also $l \in \mathbb{N}$ gegeben und es sei angenommen, dass $\operatorname{sgn}(\pi \circ \sigma') = (\operatorname{sgn} \pi)(\operatorname{sgn} \sigma')$ für $\pi, \sigma' \in \mathrm{S}_n$ so, dass σ' ein Kompositum von $l-1$ Nachbartransposition ist. Ferner seien $\pi, \sigma \in \mathrm{S}_n$ gegeben und es sei angenommen,

dass σ ein Kompositum von l Nachbartranspositionen ist. Dann ist $\sigma = \sigma' \circ \tau$ für ein $\sigma' \in \mathrm{S}_n$, welches ein Kompositum von $l-1$ Nachbartranspositionen ist, und eine Nachbartransposition $\tau \in \mathrm{S}_n$. Unter Ausnutzung von Bemerkung (1.94)(b) und der Induktionsvoraussetzung erhalten wir

$$\begin{aligned}\operatorname{sgn}(\pi \circ \sigma) &= \operatorname{sgn}(\pi \circ \sigma' \circ \tau) = -\operatorname{sgn}(\pi \circ \sigma') = -\operatorname{sgn}(\pi)\operatorname{sgn}(\sigma') = \operatorname{sgn}(\pi)(-\operatorname{sgn}(\sigma')) = \operatorname{sgn}(\pi)\operatorname{sgn}(\sigma' \circ \tau) \\ &= \operatorname{sgn}(\pi)\operatorname{sgn}(\sigma).\end{aligned}$$

Nach dem Induktionsprinzip und Proposition (1.87) folgt nun, dass $\operatorname{sgn}(\pi\circ\sigma) = (\operatorname{sgn}\pi)(\operatorname{sgn}\sigma)$ für alle $\pi, \sigma \in \mathrm{S}_n$. Dies bedeutet nach Lemma (1.67) aber, dass $\operatorname{sgn}\colon \mathrm{S}_n \to \mathbb{Z}^\times$ ein Gruppenhomomorphismus ist. □

(1.96) Korollar. Es sei $n \in \mathbb{N}$ gegeben. Für alle $\pi \in \mathrm{S}_n$ ist

$$\operatorname{sgn}\pi^{-1} = \operatorname{sgn}\pi.$$

Beweis. Es sei $\pi \in \mathrm{S}_n$ gegeben. Da sgn nach Proposition (1.95) ein Gruppenhomomorphismus und $x^{-1} = x$ für alle $x \in \mathbb{Z}^\times = \{1, -1\}$ gilt, haben wir

$$\operatorname{sgn}\pi^{-1} = (\operatorname{sgn}\pi)^{-1} = \operatorname{sgn}\pi.$$ □

(1.97) Satz. Es seien $n \in \mathbb{N}$ und $\pi \in \mathrm{S}_n$ gegeben. Ferner sei Z die Zykelzerlegung von π. Dann ist

$$\operatorname{sgn}\pi = (-1)^{\sum_{\zeta\in Z} \operatorname{lth}\zeta - |Z|}.$$

Beweis. Wir unterscheiden drei Fälle: Zuerst nehmen wir an, dass π eine Transposition ist, danach ein beliebiger Zykel und schließlich eine beliebige Permutation.
Zum ersten Fall. Es sei π eine Transposition, also $\pi = (i, j)$ für $i, j \in [1, n]$ mit $i < j$ und $Z = \{\pi\}$. Nach Bemerkung (1.86)(b) ist dann

$$\pi = (i, j) = (j, j-1)\dots(i+2, i+1)(i, i+1)(i+1, i+2)\dots(j-1, j).$$

Mit Proposition (1.95) und Bemerkung (1.94) erhalten wir

$$\begin{aligned}\operatorname{sgn}\pi &= \operatorname{sgn}((j, j-1)\dots(i+2, i+1)(i, i+1)(i+1, i+2)\dots(j-1, j)) \\ &= \operatorname{sgn}(j, j-1) \dots \operatorname{sgn}(i+2, i+1) \operatorname{sgn}(i, i+1) \operatorname{sgn}(i+1, i+2)\dots \operatorname{sgn}(j-1, j) \\ &= (-1)^{j-i-1}(-1)^{j-i} = -1 = (-1)^{2-1} = (-1)^{\sum_{\zeta\in Z} \operatorname{lth}\zeta - |Z|}.\end{aligned}$$

Zum zweiten Fall. Es sei π ein Zykel der Länge $l \in \mathbb{N}_0$, also $\pi = (j_1, \dots, j_l)$ für verschiedene $j_k \in [1, n]$ für $k \in [1, l]$. Nach Bemerkung (1.86)(a) ist dann

$$\pi = (j_1, \dots, j_l) = (j_1, j_2)\dots(j_{l-1}, j_l),$$

nach Proposition (1.95) und dem ersten Fall also

$$\operatorname{sgn}\pi = \operatorname{sgn}((j_1, j_2)\dots(j_{l-1}, j_l)) = \operatorname{sgn}(j_1, j_2) \dots \operatorname{sgn}(j_{l-1}, j_l) = (-1)^{l-1} = (-1)^{\sum_{\zeta\in Z} \operatorname{lth}\zeta - |Z|}.$$

Zum dritten Fall. Es sei π eine beliebige Permutation. Nach Proposition (1.95) und dem zweiten Fall gilt dann

$$\begin{aligned}\operatorname{sgn}\pi &= \operatorname{sgn}(\bigcirc_{\zeta\in Z} \zeta) = \prod_{\zeta\in Z} \operatorname{sgn}(\zeta) = \prod_{\zeta\in Z} (-1)^{\operatorname{lth}\zeta - 1} = (-1)^{\sum_{\zeta\in Z}(\operatorname{lth}\zeta - 1)} = (-1)^{\sum_{\zeta\in Z}\operatorname{lth}\zeta - \sum_{\zeta\in Z} 1} \\ &= (-1)^{\sum_{\zeta\in Z} \operatorname{lth}\zeta - |Z|}.\end{aligned}$$ □

(1.98) Beispiel. Für $(1, 4, 6)(3, 8, 5)(7, 9) \in \mathrm{S}_9$ gilt

$$\operatorname{sgn}((1, 4, 6)(3, 8, 5)(7, 9)) = (-1)^{3+3+2-3} = (-1)^5 = -1.$$

Aufgaben

Aufgabe 26 (Ordnung der symmetrischen Gruppe)**.** Bestimmen Sie $|\mathrm{S}_n|$ für $n \in \mathbb{N}$.

Aufgabe 27 (isomorphe symmetrische Gruppen)**.** Es sei eine invertierbare Abbildung $f\colon X \to Y$ gegeben. Zeigen Sie, dass es einen invertierbaren Gruppenhomomorphismus $\varphi\colon \mathrm{S}_X \to \mathrm{S}_Y$ so gibt, dass $\varphi^{-1}\colon \mathrm{S}_Y \to \mathrm{S}_X$ ebenfalls ein Gruppenhomomorphismus ist.

Aufgabe 28 (symmetrische Gruppe vom Grad 3)**.**

(a) Bestimmen Sie alle Elemente der S_3 in Zykeldarstellung (vgl. Beispiel (1.77)(c)). Berechnen Sie alle (binären) Komposita in einer Tafel aus $6 \cdot 6$ Feldern. Was sind die Inversen der einzelnen Elemente?

(b) Zeigen Sie, dass $\{\mathrm{id}, (1,2,3), (1,3,2)\}$ eine Untergruppe von S_3 ist.

Aufgabe 29 (Konjugation in der symmetrischen Gruppe)**.** Es sei $n \in \mathbb{N}$ gegeben. Für $\pi, \sigma \in \mathrm{S}_n$ sei ${}^{\pi}\sigma \in \mathrm{S}_n$ definiert durch

$$ {}^{\pi}\sigma := \pi\sigma\pi^{-1}. $$

(a) Zeigen Sie: Für alle $\pi \in \mathrm{S}_n$ ist die Abbildung ${}^{\pi}(-)\colon \mathrm{S}_n \to \mathrm{S}_n, \sigma \mapsto {}^{\pi}\sigma$ ein bijektiver Gruppenhomomorphismus.

(b) Es sei $n \in \mathbb{N}$ und $\pi \in \mathrm{S}_n$ eine Permutation. Zeigen Sie, dass ${}^{\pi}(-)$ Zykel auf Zykel abbildet und dabei die Zykellänge erhält. Geben Sie eine Formel für ${}^{\pi}\zeta$ für einen beliebigen Zykel $\zeta \in \mathrm{S}_n$ an.

Aufgabe 30 (Permutationen)**.** Es seien $\pi_1, \pi_2, \pi_3, \pi_4 \in \mathrm{S}_6$ definiert durch

$$ \pi_1 := \left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 1&5&3&6&4&2 \end{smallmatrix}\right),\ \pi_2 := \left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 3&2&4&1&6&5 \end{smallmatrix}\right),\ \pi_3 := (1,3,6)(2,4),\ \pi_4 := (1,2,3,4,5,6). $$

(a) Geben Sie π_1 und π_2 mittels Zykelzerlegung sowie π_3 und π_4 mittels klassischer Darstellung an.

(b) Berechnen Sie $\pi_1 \circ \pi_2$, $\pi_3 \circ \pi_4$, π_3^{-1} und $\pi_4 \circ \pi_3 \circ \pi_4^{-1}$.

(c) Berechnen Sie $\operatorname{sgn}\pi_2$, $\operatorname{sgn}\pi_3$ und $\operatorname{sgn}(\pi_2 \circ \pi_3)$.

(d) Zeigen Sie, dass $\{1, (1,2,3), (1,3,2)\}$ eine Untergruppe von S_3 ist.

Aufgabe 31 (Permutationen)**.** Es seien $\pi_1, \pi_2, \pi_3, \pi_4 \in \mathrm{S}_9$ definiert durch

$$ \pi_1 := \left(\begin{smallmatrix} 1&2&3&4&5&6&7&8&9 \\ 3&4&5&6&7&8&9&2&1 \end{smallmatrix}\right),\ \pi_2 := \left(\begin{smallmatrix} 1&2&3&4&5&6&7&8&9 \\ 2&1&4&3&5&7&6&9&8 \end{smallmatrix}\right),\ \pi_3 := (1,2,8,6)(3,9,4)(5,7),\ \pi_4 := (1,4)(6,7,8). $$

(a) Geben Sie π_1 und π_2 mittels Zykelzerlegung sowie π_3 und π_4 mittels klassischer Darstellung an.

(b) Berechnen Sie $\pi_1 \circ \pi_2$, $\pi_3 \circ \pi_4$, π_3^{-1} und $\pi_4 \circ \pi_3 \circ \pi_4^{-1}$.

(c) Berechnen Sie $\operatorname{sgn}\pi_2$, $\operatorname{sgn}\pi_3$, $\operatorname{sgn}(\pi_2 \circ \pi_3)$ und $\operatorname{sgn}((\pi_3 \circ \pi_2)^{-1})$.

(d) Schreiben Sie π_1 als ein Kompositum von Transpositionen.

Aufgabe 32 (Permutationen)**.** Es seien $\pi_1, \pi_2, \pi_3, \pi_4 \in \mathrm{S}_9$ definiert durch

$$ \pi_1 := \left(\begin{smallmatrix} 1&2&3&4&5&6&7&8&9 \\ 7&9&4&3&1&6&8&2&5 \end{smallmatrix}\right),\ \pi_2 := \left(\begin{smallmatrix} 1&2&3&4&5&6&7&8&9 \\ 4&6&8&9&2&3&5&7&1 \end{smallmatrix}\right),\ \pi_3 := \left(\begin{smallmatrix} 1&2&3&4&5&6&7&8&9 \\ 9&8&7&6&5&4&3&2&1 \end{smallmatrix}\right),\ \pi_4 := \left(\begin{smallmatrix} 1&2&3&4&5&6&7&8&9 \\ 9&8&7&6&1&2&3&4&5 \end{smallmatrix}\right). $$

(a) Geben Sie π_i für $i \in [1,4]$ mittels Zykelzerlegung an.

(b) Bestimmen Sie $\min\{k \in \mathbb{N} \mid \pi_i^k = \mathrm{id}_{[1,9]}\}$ für $i \in [1,4]$.

(c) Bestimmen Sie $\pi_1 \circ \pi_2$, $\pi_2 \circ \pi_1$, π_3^{-1}, π_4^{-1}.

(d) Berechnen Sie π_2^{1234} und π_4^{876}.

Aufgabe 33 (Kleinsche Vierergruppe)**.** Bestimmen Sie die kleinste Untergruppe von S_4, welche $(1,2)(3,4)$ und $(1,3)(2,4)$ enthält.

Aufgabe 34 (Inklusion von symmetrischen Gruppen)**.** Es sei $n \in \mathbb{N}$ mit $n \geq 2$ gegeben. Zeigen Sie, dass

$$U := \{\pi \in \mathrm{S}_n \mid \pi(n) = n\}$$

eine Untergruppe von S_n ist und finden Sie einen bijektiven Gruppenhomomorphismus $\mathrm{S}_{n-1} \to U$.

Aufgabe 35 (gerade Permutationen)**.** Es sei $n \in \mathbb{N}$ gegeben. Eine Permutation $\pi \in \mathrm{S}_n$ heißt *gerade*, falls $|\mathrm{Inv}(\pi)|$ gerade ist, sonst *ungerade*.

(a) Es sei $\pi \in \mathrm{S}_n$ gegeben. Ferner bezeichne Z die Zykelzerlegung von π. Zeigen Sie die Äquivalenz der folgenden Aussagen.

(i) Es ist π gerade.

(ii) Es ist $\operatorname{sgn} \pi = 1$.

(iii) Es ist $|\{\zeta \in Z \mid \operatorname{lth} \zeta \text{ ist gerade}\}|$ gerade.

(iv) Es ist π ein Kompositum einer geraden Anzahl von Transpositionen.

(b) Zeigen Sie, dass

$$\mathrm{A}_n := \{\pi \in \mathrm{S}_n \mid \pi \text{ gerade}\}$$

eine Untergruppe von S_n ist.

6 Ringe und Körper

Als nächstes wollen wir algebraische Strukturen betrachten, deren unterliegende Mengen mit zwei Verknüpfungen versehen sind.

Ringe

(1.99) Definition (Ring)**.**

(a) Ein *Ring* (genauer *unitärer Ring* oder *Ring mit Einselement* oder *Ring mit Eins*) besteht aus einer abelschen Gruppe R zusammen mit einer Verknüpfung m auf R so, dass die unterliegende Menge von R ein Monoid mit Multiplikation m wird und so, dass folgendes Axiom gilt.

- *Distributivität.* Für alle $x, y, z \in R$ ist

$$x\, m\, (y + z) = (x\, m\, y) + (x\, m\, z),$$
$$(x + y)\, m\, z = (x\, m\, z) + (y\, m\, z).$$

Die Verknüpfung m wird *Multiplikation* von R genannt.

(b) Es seien Ringe R und S gegeben. Ein *Ringhomomorphismus* (oder *Homomorphismus von Ringen* oder *Homomorphismus*) von R nach S ist ein Homomorphismus abelscher Gruppen $\varphi\colon R \to S$ so, dass φ ein Monoidhomomorphismus (bzgl. der Multiplikation in R uns S) ist.

Die Distributivgesetze eines Rings R mit Multiplikation m lassen sich alternativ auch kurz so formulieren: Für alle $x \in R$ sind $x\, m -\colon R \to R$ und $-\, m\, x\colon R \to R$ Homomorphismen abelscher Gruppen. Vgl. Lemma (1.67).

(1.100) Definition (kommutativer Ring)**.** Ein Ring R heißt *kommutativ*, falls die Multiplikation von R kommutativ ist.

Wir betonen, dass wir die in Definition (1.39) bzw. Definition (1.37) eingeführten Notationen für die Addition eines abelschen Magmas (und also insbesondere einer abelschen Gruppe) bzw. für die Multiplikation eines Magmas (und also insbesondere eines Monoids) auch für Ringe weiterhin verwenden, und ebenso für die neutralen und inversen Elemente bzgl. dieser Verknüpfungen. Die Axiome eines Rings R in Standardnotation lesen sich also wie folgt:

- *Assoziativität der Addition.* Für $x, y, z \in R$ ist $x + (y + z) = (x + y) + z$.

- *Existenz der Null.* Es existiert ein $n \in R$ mit $n + x = x + n = x$ für alle $x \in R$. Dieses n ist nach Korollar (1.28) eindeutig bestimmt und wird mit 0 bezeichnet. Wir haben also $0 + x = x + 0 = x$ für alle $x \in R$.
- *Existenz der Negativen.* Für jedes $x \in R$ existiert ein $y \in R$ mit $y + x = x + y = 0$. Dieses y ist nach Korollar (1.33) eindeutig bestimmt und wird mit $-x$ bezeichnet. Wir haben also $(-x)+x = x+(-x) = 0$.
- *Kommutativität der Addition.* Für $x, y \in R$ ist $x + y = y + x$.
- *Assoziativität der Multiplikation.* Für $x, y, z \in R$ ist $x(yz) = (xy)z$.
- *Existenz der Eins.* Es existiert ein $e \in R$ mit $ex = xe = x$ für alle $x \in R$. Dieses e ist nach Korollar (1.28) eindeutig bestimmt und wird mit 1 bezeichnet. Wir haben also $1x = x1 = x$ für alle $x \in R$.
- *Distributivität.* Für $x, y, z \in R$ ist $x(y + z) = (xy) + (xz)$ und $(x + y)z = (xz) + (yz)$.

Ist R kommutativ, so gilt zusätzlich noch:

- *Kommutativität der Multiplikation.* Für $x, y \in R$ ist $xy = yx$.

Ebenso verwenden wir die Notationen und Begriffe aus Definition (1.45)(a) und Definition (1.51). Ferner betonen wir, dass selbstverständlich alle Aussagen über (abelsche) Gruppen für die einem Ring unterliegende abelsche Gruppe, bestehend aus der unterliegenden Menge zusammen mit der Addition des Rings, sowie alle Aussagen über Monoide für das einem Ring unterliegende Monoid, bestehend aus der unterliegenden Menge zusammen mit der Multiplikation des Rings, gültig bleiben.

(1.101) Konvention. In Ringen lassen wir die Klammern um Produkte meistens weg, d.h. es gelte *Punkt- vor Strichrechnung.*

(1.102) Beispiel.

(a) (i) Es wird $\mathbb{N}$ kein Ring mit Addition $(x, y) \mapsto x + y$ und Multiplikation $(x, y) \mapsto xy$ (die uns vertraute Addition und die uns vertraute Multiplikation der natürlichen Zahlen).
(ii) Es wird $\mathbb{Z}$ ein kommutativer Ring mit Addition $(x, y) \mapsto x + y$ und Multiplikation $(x, y) \mapsto xy$.
(iii) Es wird $\mathbb{Q}$ ein kommutativer Ring mit Addition $(x, y) \mapsto x + y$ und Multiplikation $(x, y) \mapsto xy$.
(iv) Es wird $\mathbb{R}$ ein kommutativer Ring mit Addition $(x, y) \mapsto x + y$ und Multiplikation $(x, y) \mapsto xy$.

(b) (i) Es wird $\mathrm{inc}\colon \mathbb{Z} \to \mathbb{Q}$ ein Ringhomomorphismus.
(ii) Es wird $\mathrm{inc}\colon \mathbb{Q} \to \mathbb{R}$ ein Ringhomomorphismus.

(1.103) Bemerkung. Es seien Ringe R und S und eine Abbildung $\varphi\colon R \to S$ gegeben. Genau dann ist φ ein Ringhomomorphismus, wenn

$$\varphi(x + x') = \varphi(x) + \varphi(x'),$$
$$\varphi(xx') = \varphi(x)\,\varphi(x')$$

für alle $x, x' \in R$ und

$$\varphi(1) = 1$$

gilt.

Beweis. Wenn φ ein Ringhomomorphismus ist, dann gilt insbesondere für $x, x' \in R$ stets $\varphi(x+x') = \varphi(x)+\varphi(x')$ und $\varphi(xx') = \varphi(x)\,\varphi(x')$ sowie $\varphi(1) = 1$.
Wenn umgekehrt für $x, x' \in R$ stets $\varphi(x + x') = \varphi(x) + \varphi(x')$ und $\varphi(xx') = \varphi(x)\,\varphi(x')$ sowie $\varphi(1) = 1$ gilt, so ist φ ein Homomorphismus abelscher Gruppen nach Lemma (1.67) sowie ein Monoidhomomorphismus, also ein Ringhomomorphismus. □

Ein erstes Beispiel für einen nichtkommutativen Ring werden wir in Aufgabe 42 kennenlernen.

(1.104) Proposition. Es sei ein Ring R gegeben.

(a) Für $a \in R$ gilt $a \cdot 0 = 0 \cdot a = 0$.

(b) Für $a, b \in R$ gilt $a(-b) = (-a)b = -(ab)$.

(c) Für $a, b \in R$ gilt $(-a)(-b) = ab$.

Beweis. Siehe Aufgabe 36. □

Jeder Ring R hat eine unterliegende abelsche Gruppe. Folglich haben wir für jedes $x \in R$, $k \in \mathbb{Z}$ den Ausdruck $kx = k \cdot x \in R$ definiert, vgl. Notation (1.61)(b).

(1.105) Notation. Es sei ein Ring R gegeben. Für $k \in \mathbb{Z}$ schreiben wir auch

$$k = k^R := k1^R.$$

Wir betonen, dass die vorangegangene Vereinbarung konform mit unserer Notation für das Nullelement und das Einselement in einem Ring R ist. Sie besagt unter anderem, dass wir $2^R = 2 \cdot 1^R = 1^R + 1^R$, $3^R = 3 \cdot 1^R = 2 \cdot 1^R + 1^R = 2^R + 1^R$, etc., setzen. Genauer:

(1.106) Bemerkung. Es sei R ein Ring. Für $k \in \mathbb{Z}$ gilt

$$k^R = \begin{cases} 0^R, & \text{falls } k = 0, \\ (k-1)^R +^R 1^R, & \text{falls } k > 0, \\ (-|k|^R)^R, & \text{falls } k < 0. \end{cases}$$

Beweis. Es sei $k \in \mathbb{Z}$ gegeben. Für $k = 0$ ist $k^R = k1^R = 0 \cdot 1^R$ das Nullelement von R, siehe Notation (1.61)(b) und Notation (1.58)(b). Für $k > 0$ haben wir

$$k^R = k1^R = (k-1)1^R +^R 1^R = (k-1)^R +^R 1^R.$$

Für $k < 0$ gilt schließlich

$$k^R +^R |k|^R = (k1^R + |k|1^R) = (k + |k|)1^R = 0 \cdot 1^R = 0^R$$

nach Proposition (1.63)(a) und damit $k^R = (-|k|^R)^R$ auf Grund der Kommutativität der Addition von R. □

Wir werden häufig folgende Schreibweise antreffen:

(1.107) Notation (Kronecker-Delta)**.** Es seien ein Ring R, eine Menge I und Elemente $i, j \in I$ gegeben. Das *Kronecker-Delta* ist definiert als

$$\delta_{i,j} := \begin{cases} 1^R & \text{falls } i = j, \\ 0^R & \text{falls } i \neq j. \end{cases}$$

Körper

(1.108) Definition (Körper)**.** Ein *Körper* ist ein kommutativer Ring K, in welchem $0 \neq 1$ gilt und in welchem jedes Element von $K \setminus \{0\}$ invertierbar (bzgl. der Multiplikation $\cdot^K$) ist.

Wir fassen nun noch einmal alle Axiome, welche in einem Körper K gelten, zusammen.

- *Assoziativität der Addition.* Für alle $x, y, z \in K$ ist $x + (y + z) = (x + y) + z$.
- *Existenz der Null.* Es existiert ein $n \in K$ mit $n + x = x + n = x$ für alle $x \in K$. Dieses n ist nach Korollar (1.28) eindeutig bestimmt und wird mit 0 bezeichnet. Wir haben also $0 + x = x + 0 = x$ für alle $x \in K$.
- *Existenz der Negativen.* Für jedes $x \in K$ existiert ein $y \in K$ mit $y + x = x + y = 0$. Dieses y ist nach Korollar (1.33) eindeutig bestimmt und wird mit $-x$ bezeichnet. Wir haben also $(-x) + x = x + (-x) = 0$.
- *Kommutativität der Addition.* Für alle $x, y \in K$ ist $x + y = y + x$.

- *Assoziativität der Multiplikation.* Für alle $x, y, z \in K$ ist $x(yz) = (xy)z$.
- *Existenz der Eins.* Es existiert ein $e \in K$ mit $ex = xe = x$ für alle $x \in K$. Dieses e ist nach Korollar (1.28) eindeutig bestimmt und wird mit 1 bezeichnet. Wir haben also $1x = x1 = x$ für alle $x \in K$.
- *Existenz der Inversen.* Es ist $0 \neq 1$. Für jedes $x \in K \setminus \{0\}$ existiert ein $y \in K$ mit $yx = xy = 1$. Dieses y ist nach Korollar (1.33) eindeutig bestimmt und wird mit x^{-1} bezeichnet. Wir haben also $x^{-1}x = xx^{-1} = 1$.
- *Kommutativität der Multiplikation.* Für alle $x, y \in K$ ist $xy = yx$.
- *Distributivität.* Für alle $x, y, z \in K$ ist $x(y + z) = (xy) + (xz)$ und $(x + y)z = (xz) + (yz)$.

In Aufgabe 43 werden wir sehen, warum es plausibel ist, dass man die Invertierbarkeit der Null für einen Körper *nicht* fordert.

(1.109) Beispiel.

(a) Es wird $\mathbb{Z}$ kein Körper mit Addition $(x, y) \mapsto x + y$ und Multiplikation $(x, y) \mapsto xy$ (die uns vertraute Addition und die uns vertraute Multiplikation der ganzen Zahlen).

(b) Es wird $\mathbb{Q}$ ein Körper mit Addition $(x, y) \mapsto x + y$ und Multiplikation $(x, y) \mapsto xy$ (die uns vertraute Addition und die uns vertraute Multiplikation der rationalen Zahlen).

(1.110) Bemerkung. Ein kommutativer Ring K ist genau dann ein Körper, wenn

$$K^\times = K \setminus \{0\}$$

ist.

Beweis. Es sei zunächst K ein Körper, so dass $0 \neq 1$ und jedes Element von $K \setminus \{0\}$ ist invertierbar ist, d.h. $K \setminus \{0\} \subseteq K^\times$. Für alle $a \in K^\times$ gilt aber $aa^{-1} = 1 \neq 0$, also $a \neq 0$ nach Proposition (1.104)(a), d.h. es ist auch $K^\times \subseteq K \setminus \{0\}$. Insgesamt gilt $K^\times = K \setminus \{0\}$.
Es gelte umgekehrt $K^\times = K \setminus \{0\}$, so dass jedes Element von $K \setminus \{0\}$ invertierbar in K ist. Wegen $1 \in K^\times = K \setminus \{0\}$ nach Proposition (1.47)(b) ist ferner $0 \neq 1$ in K. Insgesamt ist K ein Körper. □

(1.111) Lemma. Es seien ein Körper K und $a, b \in K$ gegeben. Wenn $ab = 0$ gilt, dann ist $a = 0$ oder $b = 0$.

Beweis. Siehe Aufgabe 39. □

Aufgaben

Aufgabe 36 (Rechenregeln in Ringen)**.** Es sei ein Ring R gegeben. Zeigen Sie:

(a) Für $a \in R$ gilt $a \cdot 0 = 0 \cdot a = 0$.

(b) Für $a, b \in R$ gilt $a(-b) = (-a)b = -(ab)$.

(c) Für $a, b \in R$ gilt $(-a)(-b) = ab$.

Aufgabe 37 (Kürzungseigenschaft)**.** Es sei ein Ring R gegeben. Zeigen Sie die Äquivalenz der folgenden Bedingungen.

(a) Für $a, b \in R$ folgt aus $ab = 0$ stets $a = 0$ oder $b = 0$.

(b) Für $a, x, y \in R$ folgt aus $ax = ay$ stets $a = 0$ oder $x = y$.

(c) Für $a, x, y \in R$ folgt aus $xa = ya$ stets $a = 0$ oder $x = y$.

Aufgabe 38 (Ringhomomorphismus)**.** Zeigen Sie: Für jeden Ring R ist

$$\mathbb{Z} \to R,\ k \mapsto k^R$$

ein Ringhomomorphismus.

Aufgabe 39 (Nullteilerfreiheit)**.** Es seien ein Körper K und $a, b \in K$ gegeben. Zeigen Sie: Wenn $ab = 0$ gilt, dann ist $a = 0$ oder $b = 0$.

Aufgabe 40 (Ringstrukturen auf $\mathbb{R} \times \mathbb{R}$)**.**

(a) Zeigen Sie, dass $\mathbb{R} \times \mathbb{R}$ zu einem kommutativen Ring mit Addition $((a_1, a_2), (b_1, b_2)) \mapsto (a_1 + b_1, a_2 + b_2)$ und Multiplikation $((a_1, a_2), (b_1, b_2)) \mapsto (a_1 b_1, a_2 b_2)$ wird. Ist $\mathbb{R} \times \mathbb{R}$ mit dieser Struktur ein Körper?

(b) Zeigen Sie, dass $\mathbb{R} \times \mathbb{R}$ zu einem kommutativen Ring mit Addition $((a_1, a_2), (b_1, b_2)) \mapsto (a_1 + b_1, a_2 + b_2)$ und Multiplikation $((a_1, a_2), (b_1, b_2)) \mapsto (a_1 b_1 - a_2 b_2, a_1 b_2 + a_2 b_1)$ wird. Ist $\mathbb{R} \times \mathbb{R}$ mit dieser Struktur ein Körper?

Aufgabe 41 (Unterring)**.**

(a) Definieren Sie in Analogie zum Begriff der Untergruppe den Begriff des *Unterrings*.

(b) Zeigen Sie, dass

$$\mathbb{Z}[\sqrt{2}] := \{x + \sqrt{2} \cdot y \mid x, y \in \mathbb{Z}\}$$

ein Unterring von $\mathbb{R}$ ist. Ist $\mathbb{Z}[\sqrt{2}]$ ein Körper?

Aufgabe 42 (Endomorphismenring einer abelschen Gruppe)**.**

(a) Es sei eine abelsche Gruppe A gegeben. Nach Aufgabe 21 können wir $\mathrm{Hom}(A, A)$ als abelsche Gruppe auffassen. Zeigen Sie, dass $\mathrm{Hom}(A, A)$ zusammen mit der Komposition als Multiplikation ein Ring wird.

(b) Zeigen Sie, dass $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$, $(x_1, x_2) \mapsto (x_1 + x_2, x_2)$ und $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$, $(x_1, x_2) \mapsto (x_2, x_1)$ Homomorphismen abelscher Gruppen sind.

(c) Finden Sie eine abelsche Gruppe A so, dass $\mathrm{Hom}(A, A)$ versehen mit der Ringstruktur aus (a) nicht kommutativ ist.

Aufgabe 43 (Nullring)**.** Es sei ein Ring R gegeben. Zeigen Sie, dass folgende Aussagen äquivalent sind.

(a) Es ist 0 invertierbar in R.

(b) Es ist $0 = 1$ in R.

(c) Es ist $R = \{0\}$.

(d) Es ist $R^\times = \{0\}$.

Aufgabe 44 (Charakteristik)**.** Es sei ein Körper K gegeben.

(a) Es seien $n \in \mathbb{Z}$, $x \in K$ gegeben. Zeigen Sie, dass $nx = n^K \cdot^K x$ gilt.

(b) Es sei $n \in \mathbb{N}$ gegeben. Zeigen Sie: Wenn es ein $a \in K \setminus \{0\}$ mit $na = 0$ gibt, so gilt $nx = 0$ für alle $x \in K$.

(c) Es sei angenommen, dass ein $n \in \mathbb{N}$ mit $nx = 0$ für alle $x \in K$ existiert. Zeigen Sie, dass die kleinste natürliche Zahl mit dieser Eigenschaft eine Primzahl ist.

(d) Es sei K endlich mit $|K|$ gerade. Zeigen Sie, dass $x + x = 0$ für alle $x \in K$ gilt.

7 Restklassenringe der ganzen Zahlen

In diesem Abschnitt wollen wir eine ganze Serie von neuen Ringen und Körper konstruieren. Hierzu betrachten wir Äquivalenzrelation auf der Menge $\mathbb{Z}$ der ganzen Zahlen, welche verträglich mit der Ringstruktur auf $\mathbb{Z}$ sind.

Kongruenz von ganzen Zahlen

Wir führen zunächst eine Reihe von Äquivalenzrelationen auf $\mathbb{Z}$ ein.

(1.112) Definition (Kongruenz modulo n)**.** Es sei $n \in \mathbb{Z}$ gegeben. Für $x, y \in \mathbb{Z}$ sagen wir, dass x *kongruent* y *modulo* n ist, geschrieben $x \equiv_n y$, wenn es ein $p \in \mathbb{Z}$ mit $x = pn + y$ gibt.

(1.113) Beispiel. Es ist $1 \equiv_7 8$, $3 \equiv_7 10$, $2 \equiv_7 9$, $2 \equiv_7 16$, $2 \equiv_7 -5$, $16 \equiv_7 -5$.

(1.114) Bemerkung. Für $n \in \mathbb{Z}$ ist

$$\equiv_n = \equiv_{-n}.$$

Beweis. Es seien $n \in \mathbb{Z}$ und $x, y \in \mathbb{Z}$ gegeben. Genau dann $x \equiv_n y$ gilt, wenn es ein $p \in \mathbb{Z}$ mit $x = pn + y$ gibt. Wegen $pn + y = (-p)(-n) + y$ für alle $p \in \mathbb{Z}$ ist diese Bedingung jedoch äquivalent zu $x \equiv_{-n} y$. Folglich ist $\equiv_n = \equiv_{-n}$. □

Auf Grund von Bemerkung (1.114) werden wir uns im Folgenden auf $n \in \mathbb{N}_0$ beschränken.

(1.115) Proposition. Für $n \in \mathbb{N}_0$ ist $\equiv_n$ eine Äquivalenzrelation auf $\mathbb{Z}$.

Beweis. Es sei $n \in \mathbb{N}$ gegeben.
Es seien $x, y, z \in \mathbb{Z}$ mit $x \equiv_n y$ und $y \equiv_n z$ gegeben. Dann gibt es $p, q \in \mathbb{Z}$ mit $x = pn + y$ und $y = qn + z$. Es folgt

$$x = pn + y = pn + qn + z = (p + q)n + z,$$

also $x \equiv_n z$. Folglich ist $\equiv_n$ transitiv.
Für alle $x \in \mathbb{Z}$ ist $x = 0n + x$, also $x \equiv_n x$. Folglich ist $\equiv_n$ reflexiv.
Es seien $x, y \in \mathbb{Z}$ mit $x \equiv_n y$ gegeben. Dann gibt es ein $p \in \mathbb{Z}$ mit $x = pn + y$. Es folgt $y = (-p)n + x$, also $y \equiv_n x$. Folglich ist $\equiv_n$ symmetrisch.
Insgesamt ist $\equiv_n$ eine Äquivalenzrelation auf $\mathbb{Z}$. □

(1.116) Erinnerung. Für $x \in \mathbb{Z}$, $n \in \mathbb{N}$ gibt es eindeutig bestimmte $q \in \mathbb{Z}$, $r \in [0, n-1]$ mit $x = qn + r$. Man nennt q den *ganzzahligen Anteil* und r den *Rest* bei *Division mit Rest durch* n und schreibt $x \operatorname{div} n := q$ und $x \bmod n := r$. Genau dann gilt $n \mid x$, wenn $x \bmod n = 0$ ist (vgl. Aufgabe 3(a)).

(1.117) Proposition. Es sei $n \in \mathbb{N}$ gegeben.

(a) Für $x \in \mathbb{Z}$ ist $x \equiv_n x \bmod n$.

(b) Für $x, y \in \mathbb{Z}$ gilt genau dann $x \equiv_n y$, wenn $x \bmod n = y \bmod n$ ist.

Beweis.

(a) Für alle $x \in \mathbb{Z}$ gilt $x = (x \operatorname{div} n)\, n + (x \bmod n)$, also $x \equiv_n x \bmod n$.

(b) Es seien $x, y \in \mathbb{Z}$ gegeben. Nach (a) gilt $x \equiv_n x \bmod n$ und $y \equiv_n y \bmod n$. Folglich gilt genau dann $x \equiv_n y$, wenn $x \bmod n \equiv_n y \bmod n$ ist. Dies widerum ist äquivalent zu $n \mid (x \bmod n) - (y \bmod n)$. Da aber $x \bmod n \in [0, n-1]$ und $y \bmod n \in [0, n-1]$ gilt, ist $n \mid (x \bmod n) - (y \bmod n)$ gleichbedeutend mit $(x \bmod n) - (y \bmod n) = 0$, d.h. mit $x \bmod n = y \bmod n$. □

Konstruktion der Restklassenringe

Als nächstes werden wir auf den Quotientenmengen $\mathbb{Z}/\equiv_n$ für $n \in \mathbb{N}_0$ eine Ringstruktur konstruieren, und zwar so, dass wir repräsentantenweise rechnen können. Für die Addition wollen wir also etwa, dass in $\mathbb{Z}/\equiv_n$ die Gleichung $[x] + [y] = [x + y]$ für $x, y \in \mathbb{Z}$ gilt. Oder anders ausgedrückt: Wir wollen, dass die Quotientenabbildung $\mathrm{quo}\colon \mathbb{Z} \to \mathbb{Z}/\equiv_n$, $x \mapsto [x]$ ein Homomorphismus abelscher Gruppen wird. Analog für die Multiplikation, d.h. wir wollen, dass quo ein Ringhomomorphismus wird.
Um $[x] + [y] = [x + y]$ in $\mathbb{Z}/\equiv_n$ für $x, y \in \mathbb{Z}$ zu erreichen, muss für $(x, y), (\tilde{x}, \tilde{y}) \in \mathbb{Z} \times \mathbb{Z}$ mit $([x], [y]) = ([\tilde{x}], [\tilde{y}])$ in $\mathbb{Z}/\equiv_n \times \mathbb{Z}/\equiv_n$ stets $[x+y] = [\tilde{x}+\tilde{y}]$ in $\mathbb{Z}/\equiv_n$ gelten. Nun ist aber genau dann $[x] = [\tilde{x}]$ in $\mathbb{Z}/\equiv_n$, wenn $x \equiv_n \tilde{x}$ gilt, es ist genau dann $[y] = [\tilde{y}]$ in $\mathbb{Z}/\equiv_n$, wenn $y \equiv_n \tilde{y}$ gilt, und es ist genau dann $[x + y] = [\tilde{x} + \tilde{y}]$ in $\mathbb{Z}/\equiv_n$,

wenn $x + y \equiv_n \tilde{x} + \tilde{y}$ gilt. Folglich muss notwendigerweise aus $x \equiv_n \tilde{x}$ und $y \equiv_n \tilde{y}$ stets $x + y \equiv_n \tilde{x} + \tilde{y}$ folgen. Ähnlich für die Multiplikation.
Insgesamt müssen wir also zunächst zeigen, dass $\equiv_n$ verträglich mit den Verknüpfungen des kommutativen Rings $\mathbb{Z}$ ist. ([1])

(1.118) Proposition. Es sei $n \in \mathbb{N}_0$ gegeben. Für $x, \tilde{x}, y, \tilde{y} \in \mathbb{Z}$ mit $x \equiv_n \tilde{x}$ und $y \equiv_n \tilde{y}$ gilt auch $x+y \equiv_n \tilde{x}+\tilde{y}$ und $xy \equiv_n \tilde{x}\tilde{y}$.

Beweis. Es seien zunächst $x, y, \tilde{y} \in \mathbb{Z}$ mit $y \equiv_n \tilde{y}$ gegeben. Dann gibt es ein $p \in \mathbb{Z}$ mit $y = pn + \tilde{y}$. Es folgt $x + y = x + pn + \tilde{y} = pn + (x + \tilde{y})$ und $xy = x(pn + \tilde{y}) = (xp)n + (x\tilde{y})$, also $x + y \equiv_n x + \tilde{y}$ und $xy \equiv_n x\tilde{y}$.
Nun seien $x, \tilde{x}, y, \tilde{y} \in \mathbb{Z}$ mit $x \equiv_n \tilde{x}$ und $y \equiv_n \tilde{y}$ gegeben. Da Addition und Multiplikation in $\mathbb{Z}$ kommutativ sind, gilt dann in der Tat

$$x + y \equiv_n x + \tilde{y} = \tilde{y} + x \equiv_n \tilde{y} + \tilde{x} = \tilde{x} + \tilde{y},$$
$$xy \equiv_n x\tilde{y} = \tilde{y}x \equiv_n \tilde{y}\tilde{x} = \tilde{x}\tilde{y}.$$

□

(1.119) Proposition. Es sei $n \in \mathbb{N}_0$ gegeben.

(a) Die Menge $\mathbb{Z}/\equiv_n$ wird ein kommutativer Ring mit Addition und Multiplikation gegeben durch

$$[x] +^{\mathbb{Z}/\equiv_n} [y] = [x +^{\mathbb{Z}} y],$$
$$[x] \cdot^{\mathbb{Z}/\equiv_n} [y] = [x \cdot^{\mathbb{Z}} y]$$

für $x, y \in \mathbb{Z}$. Die Null und die Eins von $\mathbb{Z}/\equiv_n$ sind gegeben durch

$$0^{\mathbb{Z}/\equiv_n} = [0^{\mathbb{Z}}],$$
$$1^{\mathbb{Z}/\equiv_n} = [1^{\mathbb{Z}}].$$

Für $x \in \mathbb{Z}$ ist das Negative von $[x]$ in $\mathbb{Z}/\equiv_n$ gegeben durch

$$(-[x])^{\mathbb{Z}/\equiv_n} = [(-x)^{\mathbb{Z}}].$$

(b) Die Quotientenabbildung $\mathrm{quo}\colon \mathbb{Z} \to \mathbb{Z}/\equiv_n$ wird bzgl. der Struktur aus (a) ein Ringhomomorphismus.

Beweis.

(a) Um zu zeigen, dass die beschriebene Addition und die beschriebene Multiplikation wohldefiniert sind, seien $x, \tilde{x}, y, \tilde{y} \in \mathbb{Z}$ mit $[x] = [\tilde{x}]$ und $[y] = [\tilde{y}]$ gegeben. Dann gilt $x \equiv_n \tilde{x}$ und $y \equiv_n \tilde{y}$, also auch $x+y \equiv_n \tilde{x}+\tilde{y}$ und $xy \equiv_n \tilde{x}\tilde{y}$ nach Proprosition (1.118). Dies bedeutet aber $[x + y] = [\tilde{x} + \tilde{y}]$ und $[xy] = [\tilde{x}\tilde{y}]$ in $\mathbb{Z}/\equiv_n$ gilt.

Somit erhalten wir wohldefinierte Verknüpfungen

$$a\colon \mathbb{Z}/\equiv_n \times \mathbb{Z}/\equiv_n \to \mathbb{Z}/\equiv_n,\ ([x], [y]) \mapsto [x + y],$$
$$m\colon \mathbb{Z}/\equiv_n \times \mathbb{Z}/\equiv_n \to \mathbb{Z}/\equiv_n,\ ([x], [y]) \mapsto [xy].$$

Wir wollen zunächst zeigen, dass $\mathbb{Z}$ ein kommutativer Ring mit Addition a und Multiplikation m wird.

Für $x, y, z \in \mathbb{Z}$ gilt

$$[x]\ a\ ([y]\ a\ [z]) = [x]\ a\ [y + z] = [x + (y + z)] = [(x + y) + z] = [x + y]\ a\ [z] = ([x]\ a\ [y])\ a\ [z].$$

Folglich ist a assoziativ.

Für $x, y \in \mathbb{Z}$ gilt

$$[x]\ a\ [y] = [x + y] = [y + x] = [y]\ a\ [x].$$

Folglich ist $+$ kommutativ.

[1] Man könnte an dieser Stelle auch noch Verträglichkeit mit Null, Eins und den Negativen zu zeigen versuchen. In der Tat gelten diese Eigenschaften, sie sind jedoch redundant und folgen aus der Reflexivität und der Verträglichkeit mit der Addition.

Für $x \in \mathbb{Z}$ gilt

$$[0]\, a\, [x] = [0 + x] = [x].$$

Folglich ist [0] ein neutrales Element bzgl. a.

Für $x \in \mathbb{Z}$ gilt

$$[-x]\, a\, [x] = [(-x) + x] = [0].$$

Folglich ist $[-x]$ ein zu $[x]$ inverses Element bzgl. a.

Analog zeigt man, dass m assoziativ und multiplikativ und dass [1] ein neutrales Element bzgl. m ist.

Für $x, y, z \in \mathbb{Z}$ gilt

$$[x]\, m\, ([y]\, a\, [z]) = [x]\, m\, [y + z] = [x(y + z)] = [xy + xz] = [xy]\, a\, [xz] = ([x]\, m\, [y])\, a\, ([x]\, m\, [z]).$$

Folglich gelten die Distributivgesetze.

Insgesamt wird $\mathbb{Z}/\equiv_n$ ein kommutativer Ring mit Addition und Multiplikation gegeben durch $[x] + [y] = [x]\, a\, [y]$ und $[x] \cdot [y] = [x]\, m\, [y]$ für $x, y \in \mathbb{Z}$, Null $0 = [0]$, Eins $1 = [1]$ und Negativen $-[x] = [-x]$ für $x \in \mathbb{Z}$.

(b) Für $x, y \in R$ gilt

$$\operatorname{quo}(x + y) = [x + y] = [x] + [y] = \operatorname{quo}(x) + \operatorname{quo}(y),$$
$$\operatorname{quo}(xy) = [xy] = [x]\, [y] = \operatorname{quo}(x) \operatorname{quo}(y).$$

Ferner ist

$$\operatorname{quo}(1) = [1] = 1.$$

Nach Bemerkung (1.103) ist also quo ein Ringhomomorphismus. □

(1.120) Definition (Restklassenring)**.** Es sei $n \in \mathbb{N}_0$ gegeben. Der kommutative Ring $\mathbb{Z}/n := \mathbb{Z}/\equiv_n$ mit Addition und Multiplikation gegeben wie in Proposition (1.119) heißt *Restklassenring* von $\mathbb{Z}$ modulo n. Für $x \in \mathbb{Z}$ heißt die Äquivalenzklasse $[x]_n := [x]_{\equiv_n}$ auch die *Restklasse* von x modulo n.

Der Restklassenring $\mathbb{Z}/n$ wird in der Literatur oft auch als $\mathbb{Z}/n\mathbb{Z}$ (oder seltener $\mathbb{Z}/\mathbb{Z}n$) bezeichnet und leicht anders konstruiert; bei dieser alternativen Konstruktion spielt dann die Teilmenge $n\mathbb{Z} = \mathbb{Z}n = \{qn \mid q \in \mathbb{Z}\}$ eine Rolle.

Rechnen in Restklassenringen

(1.121) Konvention. Es sei $n \in \mathbb{N}_0$ gegeben. Für $x \in \mathbb{Z}$ schreiben wir unter Missbrauch der Notation meistens kurz x anstatt $[x]_n$ für die Restklasse von x modulo n, und sagen dann immer dazu, sobald x als Element von $\mathbb{Z}/n$ anzusehen ist. ([2])

Mit Konvention (1.121) gilt für $x, y \in \mathbb{Z}$ also $x = y$ in genau dann $\mathbb{Z}/n$, wenn $x \equiv_n y$ in $\mathbb{Z}$.

(1.122) Beispiel. In $\mathbb{Z}/7$ ist $1 = 8$, $3 = 10$, $2 = 5$. Es gilt $5 + 4 = 9 = 2$, $3 \cdot 4 = 12 = 5$, $13 \cdot 13 = (-1) \cdot (-1) = 1$.

Die Bezeichnung Restklasse bzw. Restklassenring kommt daher, dass jedes Element in $\mathbb{Z}/n$ für $n \in \mathbb{N}$, also jede Restklasse modulo n, durch den Rest eines beliebigen Repräsentanten bei Division mit Rest durch n repräsentiert wird:

(1.123) Bemerkung. Es sei $n \in \mathbb{Z} \setminus \{0\}$ gegeben. Für alle $x \in \mathbb{Z}$ ist $x = x \bmod n$ in $\mathbb{Z}/n$.

Beweis. Für alle $x \in \mathbb{Z}$ ist $x \equiv_n x \bmod n$ in $\mathbb{Z}$ nach Proposition (1.117)(a), also $x = x \bmod n$ in $\mathbb{Z}/n$ nach Proposition (1.9)(b). □

(1.124) Korollar. Für $n \in \mathbb{N}$ ist

$$\mathbb{Z}/n = \{0, \ldots, n - 1\}.$$

Beweis. Für $n \in \mathbb{N}$, $x \in \mathbb{Z}$ ist $x \bmod n \in [0, n - 1]$, vgl. Erinnerung (1.116), und es gilt $x = x \bmod n$ in $\mathbb{Z}/n$ nach Bemerkung (1.123). □

Manchmal nennt man $[0, n - 1]$ (aufgefasst als Teilmenge von $\mathbb{Z}$), wobei $n \in \mathbb{N}$, auch die *Standardtransversale* (oder das *Standardrepräsentantensystem*) für $\mathbb{Z}/n$.

[2] Da in $1^{\mathbb{Z}/n} = [1^{\mathbb{Z}}]$ ist, steht dies im Einklang mit Notation (1.105).

Algebraische Struktur

Per Konstruktion ist $\mathbb{Z}/n$ für $n \in \mathbb{Z}$ ein kommutativer Ring. Es stellt sich die Frage, für welche $n \in \mathbb{Z}$ dieser kommutative Ring ein Körper ist und, noch etwas allgemeiner, was im Allgemeinen die invertierbaren Elemente in $\mathbb{Z}/n$ sind.

(1.125) Proposition. Für $n \in \mathbb{N}$ ist

$$(\mathbb{Z}/n)^\times = \{[x] \mid x \in \mathbb{Z} \text{ mit } \gcd(x,n) = 1\}.$$

Beweis. Es seien $n \in \mathbb{N}$, $x \in \mathbb{Z}$ gegeben.
Zunächst sei x invertierbar in $\mathbb{Z}/n$. Dann gibt es ein $y \in \mathbb{Z}$ mit $yx = 1$ in $\mathbb{Z}/n$. Ferner gibt es $p \in \mathbb{Z}$, $q \in \mathbb{N}$ mit $x = p \gcd(x,n)$ und $n = q \gcd(x,n)$ in $\mathbb{Z}$. Wir erhalten

$$q = yxq = yp \gcd(x,n)\, q = ypn = 0$$

in $\mathbb{Z}/n$, also $n \mid q$ in $\mathbb{Z}$. Da aber $q \in \mathbb{N}$ und $q \mid n$ gilt, folgt $q = n$ und damit $\gcd(x,n) = 1$.
Nun gelte umgekehrt $\gcd(x,n) = 1$. Wir wollen zeigen, dass die Abbildung $l\colon \mathbb{Z}/n \to \mathbb{Z}/n$, $[y] \mapsto [xy]$ injektiv ist. Hierzu seien $y, y' \in \mathbb{Z}$ mit $l([y]) = l([y'])$ gegeben, d.h. es gelte $xy = xy'$ in $\mathbb{Z}/n$. Dann ist $x(y - y') = 0$ in $\mathbb{Z}/n$, also $n \mid x(y - y')$. Wegen $\gcd(x,n) = 1$ folgt $n \mid y - y'$, also $y - y' = 0$ in $\mathbb{Z}/n$ und damit $y = y'$ in $\mathbb{Z}/n$. Somit ist l in der Tat injektiv. Wegen der Endlichkeit von $\mathbb{Z}/n$ ist l dann aber auch surjektiv, es gibt also insbesondere ein $y \in \mathbb{Z}$ mit $xy = 1$ in $\mathbb{Z}/n$. Da $\mathbb{Z}/n$ kommutativ ist, impliziert dies aber bereits die Invertierbarkeit von x in $\mathbb{Z}/n$. □

Alternativer Beweis zu Proposition (1.125). Es sei $n \in \mathbb{N}$ gegeben. Die Inklusion $(\mathbb{Z}/n)^\times \subseteq \{[x] \mid x \in \mathbb{Z} \text{ mit } \gcd(x,n) = 1\}$ beweisen wir wie bisher.
Für die umgekehrte Inklusion sei $x \in \mathbb{Z}$ mit $\gcd(x,n) = 1$ gegeben. Nach Aufgabe 25(b) gibt es dann $a, b \in \mathbb{Z}$ mit $xa + nb = \gcd(x,n) = 1$ in $\mathbb{Z}$. Da $n = 0$ in $\mathbb{Z}/n$, erhalten wir $xa = xa + nb = 1$ in $\mathbb{Z}/n$, d.h. es ist x invertierbar in $\mathbb{Z}/n$ mit $x^{-1} = a$. □

(1.126) Satz. Für $n \in \mathbb{N}$ ist $\mathbb{Z}/n$ genau dann ein Körper, wenn n eine Primzahl ist.

Beweis. Es ist $\mathbb{Z}/n$ stets ein kommutativer Ring. Folglich ist $\mathbb{Z}/n$ genau dann ein Körper, wenn $0 \neq 1$ gilt und jedes $x \in [1, n-1]$ invertierbar in $\mathbb{Z}/n$ ist. In $\mathbb{Z}/n$ gilt genau dann $0 = 1$, wenn $n = 1$ ist, und es ist 1 keine Primzahl. Im Folgenden sei also $n > 1$. Nach Proposition (1.125) ist genau dann jedes $x \in [1, n-1]$ invertierbar in $\mathbb{Z}/n$, wenn $\gcd(x,n) = 1$ für alle $x \in [1, n-1]$ gilt. Wegen $n > 1$ ist dies aber äquivalent dazu, dass n eine Primzahl ist. □

(1.127) Definition (endliche Primkörper)**.** Für $p \in \mathbb{P}$ heißt $\mathbb{F}_p := \mathbb{Z}/p$ der *Primkörper* zur Primzahl p.

Aufgaben

Aufgabe 45 (Rechnen in $\mathbb{Z}/n$)**.**

(a) Berechnen Sie $17 + 23 + 40 - 8$ und $2 \cdot (-3) \cdot 15$ und $6^{1000000}$ in $\mathbb{Z}/7$.

(b) Berechnen Sie $(-8) + 13 - 2 + 5$ und $4 \cdot 3 \cdot 5$ und 9^{14} in $\mathbb{Z}/8$.

(c) Ist $3^{2016} = 3^{2012}$ in $\mathbb{Z}/80$?

Aufgabe 46 (Nullteiler in $\mathbb{Z}/n$)**.**

(a) Finden Sie $n \in \mathbb{N}$, $x, y \in \mathbb{Z}$ mit $x \neq 0$ und $y \neq 0$ in $\mathbb{Z}/n$, aber $xy = 0$ in $\mathbb{Z}/n$.

(b) Es seien $p, q \in \mathbb{N}$ mit $p > 1$ und $q > 1$. Zeigen Sie mit Hilfe von Lemma (1.111) noch einmal, dass $\mathbb{Z}/pq$ kein Körper ist.

Aufgabe 47 (Inverse in $\mathbb{Z}/n$)**.**

(a) Bestimmen Sie die invertierbaren Elemente in $\mathbb{Z}/11$ und geben Sie die jeweiligen Inversen an.

(b) Bestimmen Sie die invertierbaren Elemente in $\mathbb{Z}/15$ und geben Sie die jeweiligen Inversen an.

(c) Es sei $a \in \mathbb{Z}$ so, dass a^2 in $\mathbb{Z}/12$ invertierbar ist. Ist dann auch a in $\mathbb{Z}/12$ invertierbar?

Aufgabe 48 (chinesischer Restsatz)**.** Zeigen Sie, dass

$$\mathbb{Z}/6 \to \mathbb{Z}/2 \times \mathbb{Z}/3,\ [x]_6 \mapsto ([x]_2, [x]_3)$$

ein wohldefinierter bijektiver Ringhomomorphismus ist.

Kapitel II

Lineare Strukturen

1 Lineare Gleichungssysteme

Es seien $m, n \in \mathbb{N}_0$ und ein Körper K gegeben. Ein *lineares Gleichungssystem* aus m Gleichungen und n Unbekannten x_j für $j \in [1, n]$ über K ist durch

$$\begin{array}{ccccccccc} A_{1,1}x_1 & + & A_{1,2}x_2 & + & \dots & + & A_{1,n}x_n & = & b_1, \\ A_{2,1}x_1 & + & A_{2,2}x_2 & + & \dots & + & A_{2,n}x_n & = & b_2, \\ & & & & & & & \vdots & \\ A_{m,1}x_1 & + & A_{m,2}x_2 & + & \dots & + & A_{m,n}x_n & = & b_m \end{array}$$

für $A_{i,j}, b_i \in K$, wobei $i \in [1, m]$, $j \in [1, n]$, gegeben. Kurz können wir hierfür auch

$$\sum_{j \in [1,n]} A_{i,j}x_j = b_i$$

für $i \in [1, m]$ schreiben. Wir nennen das lineare Gleichungssystem *homogen*, falls $b_i = 0$ für $i \in \{1, \dots, m\}$, sonst *inhomogen*. Wenn wir ein solches lineares Gleichungssystem lösen wollen, so suchen wir also die Menge aller $x = (x_j)_{j \in [1,n]} \in K^n$, welche die m Gleichungen erfüllen.
Wir beginnen mit einem Beispiel:

(2.1) Beispiel. Es seien $x_1, x_2, x_3, x_4 \in \mathbb{R}$ gegeben. Genau dann gilt

$$\begin{array}{rcrcrcrcr} -2x_1 & + & 2x_2 & - & 6x_3 & - & 10x_4 & = & -24, \\ 2x_1 & + & 3x_2 & - & 9x_3 & - & 7x_4 & = & -15, \\ x_1 & + & x_2 & - & 3x_3 & - & 2x_4 & = & -4, \end{array}$$

wenn es ein $a \in \mathbb{R}$ mit

$$x_1 = 1,\ x_2 = -1 + 3a,\ x_3 = a,\ x_4 = 2$$

gibt.

Beweis. Zunächst gelte

$$\begin{aligned} -2x_1 + 2x_2 - 6x_3 - 10x_4 &= -24, \\ 2x_1 + 3x_2 - 9x_3 - 7x_4 &= -15, \\ x_1 + x_2 - 3x_3 - 2x_4 &= -4. \end{aligned}$$

Aus $-2x_1 + 2x_2 - 6x_3 - 10x_4 = -24$ und $2x_1 + 3x_2 - 9x_3 - 7x_4 = -15$ folgt

$$5x_2 - 15x_3 - 17x_4 = (-2x_1 + 2x_2 - 6x_3 - 10x_4) + (2x_1 + 3x_2 - 9x_3 - 7x_4) = -24 - 15 = -39.$$

Aus $2x_1 + 3x_2 - 9x_3 - 7x_4 = -15$ und $x_1 + x_2 - 3x_3 - 2x_4 = -4$ folgt

$$x_2 - 3x_3 - 3x_4 = (2x_1 + 3x_2 - 9x_3 - 7x_4) - 2(x_1 + x_2 - 3x_3 - 2x_4) = -15 - 2(-4) = -7.$$

Aus $5x_2 - 15x_3 - 17x_4 = -39$ und $x_2 - 3x_3 - 3x_4 = -7$ folgt

$$-2x_4 = (5x_2 - 15x_3 - 17x_4) - 5(x_2 - 3x_3 - 3x_4) = -39 - 5(-7) = -4$$

und damit

$$x_4 = -2.$$

Dies liefert

$$\begin{aligned} -2x_1 + 2x_2 - 6x_3 &= -24 + 10x_4 = -24 + 10 \cdot 2 = -4, \\ 2x_1 + 3x_2 - 9x_3 &= -15 + 7x_4 = -15 + 7 \cdot 2 = -1, \\ x_1 + x_2 - 3x_3 &= -4 + 2x_4 = -4 + 2 \cdot 2 = 0, \\ x_2 - 3x_3 &= -7 + 3x_4 = -7 + 3 \cdot 2 = -1. \end{aligned}$$

Aus $x_1 + x_2 - 3x_3 = 0$ und $x_2 - 3x_3 = -1$ folgt

$$x_1 = (x_1 + x_2 - 3x_3) - (x_2 - 3x_3) = 0 - (-1) = 1.$$

Dies liefert nun

$$x_2 - 3x_3 = 0 - x_1 = 0 - 1 = -1.$$

Wenn wir also $a := x_3$ setzen, so haben wir

$$\begin{aligned} x_3 &= a, \\ x_2 &= -1 + 3x_3 = -1 + 3a. \end{aligned}$$

Gibt es umgekehrt ein $a \in \mathbb{R}$ mit $x_1 = 1$, $x_2 = -1 + 3a$, $x_3 = a$, $x_4 = 2$, so gilt auch

$$\begin{aligned} -2x_1 + 2x_2 - 6x_3 - 10x_4 &= -2 \cdot 1 + 2(-1 + 3a) - 6a - 10 \cdot 2 = -24, \\ 2x_1 + 3x_2 - 9x_3 - 7x_4 &= 2 \cdot 1 + 3(-1 + 3a) - 9a - 7 \cdot 2 = -15, \\ x_1 + x_2 - 3x_3 - 2x_4 &= 1 + (-1 + 3a) - 3a - 2 \cdot 2 = -4. \end{aligned}$$

□

Man kann sich vorstellen, dass ein naives Vorgehen wie im Beweis von Beispiel (2.1) bei „großen“ linearen Gleichungssystemen (in Anwendungen können durchaus auch mal mehrere Hunderttausend Gleichungen und Unbekannte auftreten) sehr schnell zu Unübersichtlichkeiten führen kann. Da lineare Gleichungssysteme im Folgenden immer wieder auftauchen werden, wollen wir zu Beginn dieses Kapitels ein systematisches Verfahren zum Lösen linearer Gleichungssysteme erarbeiten.
Die Kernidee des Verfahrens ist wie folgt: Ähnlich wie im Beweis zu Beispiel (2.1) gewinnen wir zunächst aus den gegebenen Gleichungen neue Gleichungen. Hierbei ersetzen wir jedoch für jede neue Gleichung eine der vorherigen Gleichungen, ohne hierbei die Gesamtheit der Lösungen zu verändern. Wir erhalten also stets neue lineare Gleichungssysteme mit der gleichen Anzahl an Gleichungen und mit den gleichen Lösungen. Dies machen wir so lange, bis wir am Ende ein lineares Gleichungssystem haben, welches eine so einfache Gestalt hat, dass wir die Lösungen direkt bestimmen oder sogar ablesen können.

Matrizen

Zunächst wollen wir lineare Gleichungssysteme effizient formalisieren. Da ein lineares Gleichungssystem aus m Gleichungen und n Unbekannten wie oben nur von den gegebenen Koeffizienten $A_{i,j}$ und b_i für $i \in [1, m]$, $j \in [1, n]$ abhängt, werden wir lineare Gleichungssysteme im Folgenden in rechteckigen Schemata kodieren. Hierzu führen wir den nachfolgenden Begriff ein.

(2.2) Definition (Matrix)**.** Es seien $m, n \in \mathbb{N}_0$ und eine Menge X gegeben. Die *Menge der* $(m \times n)$*-Matrizen* über X ist definiert als

$$X^{m \times n} := X^{[1,m] \times [1,n]}.$$

Ein Element von $X^{m\times n}$ heißt $(m \times n)$-*Matrix über* X (oder $(m \times n)$-*Matrix mit Einträgen in* X). Für eine $(m \times n)$-Matrix A über X schreiben wir $A_{i,j} := A_{(i,j)}$ für den Eintrag an einer Stelle $(i, j) \in [1, m] \times [1, n]$ sowie

$$\begin{pmatrix} A_{1,1} & \dots & A_{1,n} \\ \vdots & & \vdots \\ A_{m,1} & \dots & A_{m,n} \end{pmatrix} := (A_{i,j})_{i\in[1,m],j\in[1,n]} := A.$$

Bei Matrizen, welche nur aus genau einer Zeile oder genau einer Spalte bestehen, lassen wir den jeweils zweiten Index für die Einträge weg:

(2.3) Notation. Es seien $n \in \mathbb{N}_0$ und eine Menge X gegeben.

(a) Für eine $(n \times 1)$-Matrix A über X schreiben wir $A_i := A_{i,1}$ für den Eintrag an der Stelle $(i, 1)$ für ein $i \in [1, n]$ sowie

$$\begin{pmatrix} A_1 \\ \vdots \\ A_n \end{pmatrix} := (A_i)_{i\in[1,n]} := A.$$

(b) Für eine $(1 \times n)$-Matrix A über X schreiben wir $A_i := A_{1,i}$ für den Eintrag an der Stelle $(1, i)$ für ein $i \in [1, n]$ sowie

$$\begin{pmatrix} A_1 & \dots & A_n \end{pmatrix} := (A_i)_{i\in[1,n]} := A.$$

(2.4) Definition (Zeile, Spalte)**.** Es seien $m, n \in \mathbb{N}_0$, eine Menge X und ein $A \in X^{m\times n}$ gegeben.

(a) Für $i \in [1, m]$ heißt $A_{i,-} \in K^{1\times n}$ gegeben durch

$$A_{i,-} = (A_{i,j})_{j\in[1,n]}$$

die *i-te Zeile* von A.

(b) Für $j \in [1, n]$ heißt $A_{-,j} \in K^{m\times 1}$ gegeben durch

$$A_{-,j} = (A_{i,j})_{i\in[1,m]}$$

die *j-te Spalte* von A.

Es seien $m, n \in \mathbb{N}_0$, eine Menge X und eine $(m \times n)$-Matrix

$$A = \begin{pmatrix} A_{1,1} & \dots & A_{1,n} \\ \vdots & & \vdots \\ A_{m,1} & \dots & A_{m,n} \end{pmatrix}$$

über X gegeben. Dann ist für $i \in [1, m]$ also die i-te Zeile gegeben durch

$$A_{i,-} = \begin{pmatrix} A_{i,1} & \dots & A_{i,n} \end{pmatrix},$$

während für $j \in [1, n]$ die j-te Spalte durch

$$A_{-,j} = \begin{pmatrix} A_{1,j} \\ \vdots \\ A_{m,j} \end{pmatrix}$$

gegeben ist. Mit anderen Worten, für $i \in [1, m]$, $j \in [1, n]$ ist

$$(A_{i,-})_j = A_{i,j} = (A_{-,j})_i.$$

Wir wollen im Folgenden noch eine einfache Notation für „aneinandergehängte“ Matrizen festlegen:

(2.5) Notation. Es seien $m, n, p, q \in \mathbb{N}_0$, eine Menge X sowie $A \in X^{m\times n}$, $B \in X^{m\times q}$, $C \in X^{p\times n}$, $D \in X^{p\times q}$ gegeben. Die Matrix $Z \in X^{(m+p)\times(n+q)}$ gegeben durch

$$Z_{i,j} = \begin{cases} A_{i,j}, & \text{falls } (i,j) \in [1,m] \times [1,n], \\ B_{i,j-n}, & \text{falls } (i,j) \in [1,m] \times [n+1,n+q], \\ C_{i-m,j}, & \text{falls } (i,j) \in [m+1,m+p] \times [1,n], \\ B_{i-m,j-n}, & \text{falls } (i,j) \in [m+1,m+p] \times [n+1,n+q], \end{cases}$$

für $(i,j) \in [1,m+p] \times [1,n+q]$ notieren wir als

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right) := Z.$$

Wir haben Matrizen eingeführt, um lineare Gleichungssysteme zu kodieren. Der präzise Zusammenhang wird in der nachfolgenden Definition festgehalten:

(2.6) Definition (Lösung eines linearen Gleichungssystems)**.** Es seien $m, n \in \mathbb{N}_0$ und ein Körper K gegeben.

(a) Es seien $A \in K^{m\times n}$ und $b \in K^{m\times 1}$ gegeben. Die *Lösungsmenge des linearen Gleichungssystem zur erweiterten Koeffizientenmatrix* $\left(A \mid b\right)$ ist definiert als

$$\mathrm{Sol}(A,b) := \{x \in K^{n\times 1} \mid \text{für } i \in [1,m] \text{ gilt } \sum_{j\in[1,n]} A_{i,j}x_j = b_i\}.$$

Die Elemente von $\mathrm{Sol}(A,b)$ heißen *Lösungen des linearen Gleichungssystem zur erweiterten Koeffizientenmatrix* $\left(A \mid b\right)$.

(b) Es sei $A \in K^{m\times n}$ gegeben. Die *Lösungsmenge des homogenen linearen Gleichungssystem zur Koeffizientenmatrix* A ist definiert also

$$\mathrm{Sol}_0(A) := \mathrm{Sol}(A, \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}).$$

Die Elemente von $\mathrm{Sol}_0(A)$ heißen *Lösungen des homogenen linearen Gleichungssystem zur Koeffizientenmatrix* A.

Dass wir die Lösungen x in Definition (2.6) aus $K^{n\times 1}$ und nicht aus K^n wählen, ist an dieser Stelle lediglich eine Konvention. Der Grund hierfür wird später deutlich werden.

(2.7) Beispiel. Es seien $A \in \mathbb{R}^{3\times 4}$ und $b \in \mathbb{R}^{3\times 1}$ gegeben durch

$$A := \begin{pmatrix} -2 & 2 & -6 & -10 \\ 2 & 3 & -9 & -7 \\ 1 & 1 & -3 & -2 \end{pmatrix}, \; b := \begin{pmatrix} -24 \\ -15 \\ -4 \end{pmatrix}.$$

Die Lösungsmenge des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix $\left(A \mid b\right)$ ist gegeben durch

$$\mathrm{Sol}(A,b) = \{\begin{pmatrix} 1 \\ -1+3a \\ a \\ 2 \end{pmatrix} \mid a \in \mathbb{R}\}.$$

Beweis. Dies folgt aus Beispiel (2.1). □

Zeilenstufenform

Als nächstes studieren wir Matrizen, bei denen sich die Lösungen der zugehörigen linearen Gleichungssysteme sofort rekursiv ermitteln lassen.

(2.8) Definition (Zeilenstufenindizes, Zeilenstufenanzahl)**.** Es seien $m, n \in \mathbb{N}_0$, ein Körper K und ein $A \in K^{m\times n}$ gegeben. Für $i \in [1, m]$ heißt

$$\mathrm{ech}_i = \mathrm{ech}_i(A) := \begin{cases} \min\{j \in [1,n] \mid A_{i,j} \neq 0\}, & \text{falls } A_{i,j} \neq 0 \text{ für ein } j \in [1,n], \\ n+i, & \text{falls } A_{i,j} = 0 \text{ für alle } j \in [1,n], \end{cases}$$

der *i-te Zeilenstufenindex* von A. Ferner heißt

$$|\{i \in [1,m] \mid \mathrm{ech}_i \in [1,n]\}|$$

die *Zeilenstufenanzahl* von A.

(2.9) Beispiel. Für $A \in \mathbb{R}^{3\times 4}$ gegeben durch

$$A = \begin{pmatrix} 0 & 3 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

ist

$$\mathrm{ech}_1 = 2,$$
$$\mathrm{ech}_2 = 6,$$
$$\mathrm{ech}_3 = 1.$$

(2.10) Definition ((reduzierte) Zeilenstufenform)**.** Es seien $m, n \in \mathbb{N}_0$, ein Körper K und ein $A \in K^{m\times n}$ gegeben.

(a) Wir sagen, dass A in *Zeilenstufenform* ist, falls

$$\mathrm{ech}_i < \mathrm{ech}_{i+1}$$

für alle $i \in [1, m-1]$ gilt.

(b) Wir sagen, dass A in *reduzierter Zeilenstufenform* ist, falls A in Zeilenstufenform ist und

$$A_{k,\mathrm{ech}_i} = \delta_{k,i}$$

für alle $k \in [1, i]$, $i \in [1, m]$ gilt.

Eine Matrix A in Zeilenstufenform ist von folgender Gestalt, wobei die mit $*$ markierten Einträge beliebig sind und $A_{i,\mathrm{ech}_i} \neq 0$ für $i \in [1, r]$ und für ein $r \in [0, m]$:

$$A = \left(\begin{array}{ccc|ccccccccccc} 0 & \dots & 0 & A_{1,\mathrm{ech}_1} & * & \dots & * & * & * & \dots & * & * & * & \dots & * \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & A_{2,\mathrm{ech}_2} & * & \dots & * & * & * & \dots & * \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & & \ddots & \ddots & \ddots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & \dots & 0 & \dots & 0 & A_{r,\mathrm{ech}_r} & * & \dots & * \\ \hline 0 & \dots & 0 & 0 & 0 & \dots & 0 & \dots & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & \dots & 0 & \dots & 0 & 0 & 0 & \dots & 0 \end{array}\right)$$

Eine Matrix A in reduzierter Zeilenstufenform ist von folgender Gestalt:

$$A = \left(\begin{array}{ccc|ccccccccccc} 0 & \dots & 0 & 1 & * & \dots & * & 0 & * & \dots & * & 0 & * & \dots & * \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & 1 & * & \dots & * & 0 & * & \dots & * \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & & \ddots & \ddots & \ddots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & \dots & 0 & \dots & 0 & 1 & * & \dots & * \\ \hline 0 & \dots & 0 & 0 & 0 & \dots & 0 & \dots & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & \dots & 0 & \dots & 0 & 0 & 0 & \dots & 0 \end{array}\right)$$

(2.11) Beispiel.

(a) Über $\mathbb{R}$ ist die Matrix

$$\begin{pmatrix} 1 & 1 & -1 & -3 \\ 0 & 0 & 2 & 4 \\ 2 & 2 & 0 & -2 \end{pmatrix}$$

nicht in Zeilenstufenform.

(b) Über $\mathbb{R}$ ist die Matrix

$$\begin{pmatrix} 1 & 1 & -1 & -3 \\ 0 & 0 & 2 & 4 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

in Zeilenstufenform, aber nicht in reduzierter Zeilenstufenform.

(c) Über $\mathbb{R}$ ist die Matrix

$$\begin{pmatrix} 1 & 1 & 0 & -1 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

in reduzierter Zeilenstufenform.

In folgender Proposition geben wir eine rekursive Formel für die Lösungmenge eines linearen Gleichungssystems zu einer Matrix in Zeilenstufenform an.

(2.12) Proposition. Es seien $m, n \in \mathbb{N}_0$, ein Körper K, ein $A \in K^{m\times n}$ in Zeilenstufenform und ein $b \in K^{m\times 1}$ gegeben. Ferner sei r die Zeilenstufenanzahl von A. Genau dann gibt es eine Lösung des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix $\left(A \mid b\right)$, wenn die Zeilenstufenanzahl von $\left(A \mid b\right)$ auch gleich r ist. In diesem Fall ist die Lösungsmenge des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix $\left(A \mid b\right)$ gegeben durch

$$\mathrm{Sol}(A,b) = \{x \in K^{n\times 1} \mid \text{für } i \in [1,r] \text{ ist } x_{\mathrm{ech}_i} = A_{i,\mathrm{ech}_i}^{-1}(b_i - \sum_{j\in[\mathrm{ech}_i+1,n]} A_{i,j}x_j)\}.$$

Beweis. Zunächst sei die Zeilenstufenanzahl von $\left(A \mid b\right)$ ungleich r, so dass es ein $i \in [r+1,m]$ mit $A_{i,j} = 0$ für alle $j \in [1,n]$ und $b_i \neq 0$ gibt.

$$\left(A \mid b\right) = \left(\begin{array}{cccccccccc|c} 0 & \dots & 0 & A_{1,\mathrm{ech}_1} & A_{1,\mathrm{ech}_1+1} & \dots & A_{1,\mathrm{ech}_r-1} & A_{1,\mathrm{ech}_r} & \dots & A_{1,n} & b_1 \\ \vdots & & \vdots & & \ddots & \ddots & \ddots & \vdots & & \vdots & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & A_{r,\mathrm{ech}_r} & \dots & A_{r,n} & b_r \\ \hline 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 & b_{r+1} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 & b_m \end{array}\right) \qquad b_i \neq 0$$

Dann ist aber

$$\sum_{j\in[1,n]} A_{i,j}x_j = \sum_{j\in[1,n]} 0x_j = 0 \neq b_i$$

für alle $x \in K^{n\times 1}$ und damit $\mathrm{Sol}(A,b) = \emptyset$.
Nun sei umgekehrt die Zeilenstufenanzahl von $\left(A \mid b\right)$ gleich r, so dass $A_{i,j} = 0$ für alle $i \in [r+1,m]$, $j \in [1,n]$ und $b_i = 0$ für alle $i \in [r+1,m]$ gilt.

$$\left(A \mid b\right) = \left(\begin{array}{cccccccccc|c} 0 & \dots & 0 & A_{1,\mathrm{ech}_1} & A_{1,\mathrm{ech}_1+1} & \dots & A_{1,\mathrm{ech}_r-1} & A_{1,\mathrm{ech}_r} & \dots & A_{1,n} & b_1 \\ \vdots & & \vdots & & \ddots & \ddots & \ddots & \vdots & & \vdots & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & A_{r,\mathrm{ech}_r} & \dots & A_{r,n} & b_r \\ \hline 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 \end{array}\right)$$

Dann ist $\left(A \mid b\right)$ in Zeilenstufenform und es gilt

$$\mathrm{ech}_i(\left(A \mid b\right)) = \mathrm{ech}_i(A).$$

für $i \in [1, r]$.
Nun sei ein $x \in K^{n\times 1}$ gegeben. Genau dann ist x eine Lösung des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix $\left(A \mid b\right)$, wenn

$$\sum_{j\in[1,n]} A_{i,j}x_j = b_i$$

für alle $i \in [1, m]$ gilt. Da A in Zeilenstufenform ist, gilt für alle $i \in [1, r]$ stets $A_{i,j} = 0$ für $j \in [1, \mathrm{ech}_i - 1]$ und damit

$$\sum_{j\in[1,n]} A_{i,j}x_j = \sum_{j\in[\mathrm{ech}_i,n]} A_{i,j}x_j = A_{i,\mathrm{ech}_i}x_{\mathrm{ech}_i} + \sum_{j\in[\mathrm{ech}_i+1,n]} A_{i,j}x_j.$$

Ferner gilt für $i \in [r + 1, m]$ ohnehin stets

$$\sum_{j\in[1,n]} A_{i,j}x_j = \sum_{j\in[1,n]} 0x_j = 0 = b_i.$$

Somit ist x genau dann eine Lösung des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix $\left(A \mid b\right)$, wenn

$$A_{i,\mathrm{ech}_i}x_{\mathrm{ech}_i} + \sum_{j\in[\mathrm{ech}_i+1,n]} A_{i,j}x_j = b_i$$

für alle $i \in [1, r]$ gilt. Diese Bedingung ist jedoch äquivalent dazu, dass

$$x_{\mathrm{ech}_i} = A^{-1}_{i,\mathrm{ech}_i}(b_i - \sum_{j\in[\mathrm{ech}_i+1,n]} A_{i,j}x_j)$$

für alle $i \in [1, r]$ gilt. Nun ist dies aber eine rekursive Beschreibung von x, folglich also $\mathrm{Sol}(A, b) \neq \emptyset$. □

Der konstruktive Beweis von Proposition (2.12) liefert folgenden Algorithmus zur Bestimmung der Lösungsmenge eines linearen Gleichungssystems in Zeilenstufenform.

(2.13) Algorithmus.

- Eingabe: $A \in K^{m\times n}$ in Zeilenstufenform, $b \in K^{m\times 1}$ für einen Körper K und $m, n \in \mathbb{N}_0$
- Ausgabe: $\mathrm{Sol}(A, b)$
- Verfahren:

```
function solref(A, b)
    ermittle die Zeilenstufenanzahl r von A;

    if b_i ≠ 0 für ein i ∈ [r + 1, m] then
        return ∅;
    end if;

    l := 1;
    for j from 1 to n do
        if j ≠ ech_i für alle i ∈ [1, r] then
            x_j := a_l;                          // a_l ist ein Symbol
            l := l + 1;
        end if;
    end for;
```

```
        for i from r to 1 do
            x_{ech_i} := A^{-1}_{i,ech_i}(b_i − Σ_{j∈[ech_i+1,n]} A_{i,j} x_j);
        end for;

        return {x | a_l ∈ K für l ∈ [1, n − r]};
    end function;
```

(2.14) Beispiel. Es seien $A \in \mathbb{R}^{3\times 4}$ und $b \in \mathbb{R}^{3\times 1}$ gegeben durch

$$A := \begin{pmatrix} 2 & 2 & -2 & -6 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \; b := \begin{pmatrix} 4 \\ 1 \\ 0 \end{pmatrix}.$$

Die Lösungsmenge des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix $\left(A \mid b\right)$ ist gegeben durch

$$\mathrm{Sol}(A,b) = \{ \begin{pmatrix} 3 - a_1 + a_2 \\ a_1 \\ 1 - 2a_2 \\ a_2 \end{pmatrix} \mid a_1, a_2 \in \mathbb{R} \}.$$

Beweis. Es ist

$$\left(A \mid b\right) = \left(\begin{array}{cccc|c} 2 & 2 & -2 & -6 & 4 \\ 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right).$$

Nach Proposition (2.12) gilt für $x \in \mathbb{R}^{4\times 1}$ genau dann $x \in \mathrm{Sol}(A,b)$, wenn es $a_1, a_2 \in \mathbb{R}$ gibt mit

$$\begin{aligned} x_2 &= a_1, \\ x_4 &= a_2, \\ x_3 &= 1 - 2x_4 = 1 - 2a_2, \\ x_1 &= \frac{1}{2}(4 - 2x_2 + 2x_3 + 6x_4) = 2 - x_2 + x_3 + 3x_4 = 2 - a_1 + (1 - 2a_2) + 3a_2 = 3 - a_1 + a_2. \end{aligned}$$

□

Elementare Zeilenoperationen

Da eine beliebige Matrix nicht in Zeilenstufenform ist, benötigen wir zum Lösen allgemeiner linearer Gleichungssystem eine Methode, um eine gegebene Matrix in eine geeignete Matrix in (reduzierter) Zeilenstufenform zu überführen. Hierbei bedeutet „geeignet“, dass die Lösungsmenge des linearen Gleichungssystems zur ursprünglichen Matrix gleich der Lösungsmenge des linearen Gleichungssystems zur Matrix in Zeilenstufenform sein sollte.
Um den Prozess des Überführens von Matrizen zu formalisieren, führen wir Operationen auf den Zeilen von Matrizen ein. Betrachten wir diese Zeilenoperationen simultan für alle $(m \times n)$-Matrizen über einem Körper K für gegebene $m, n \in \mathbb{N}_0$, so erhalten wir also eine Abbildung $K^{m\times n} \to K^{m\times n}$. Wir werden in Proposition (2.22) sehen, dass diese Operatoren die Lösungsmengen von linearen Gleichungssystemen invariant lassen.

(2.15) Definition (elementare Zeilenoperatoren)**.** Es seien $m, n \in \mathbb{N}_0$ und ein Körper K gegeben.

(a) Für $k, l \in [1, m]$ heißt $\mathrm{sw}_{k,l} \colon K^{m\times n} \to K^{m\times n}$ gegeben durch

$$\mathrm{sw}_{k,l}(A)_{i,j} = \begin{cases} A_{l,j}, & \text{falls } i = k, \\ A_{k,j}, & \text{falls } i = l, \\ A_{i,j}, & \text{falls } i \notin \{k, l\}, \end{cases}$$

für $i \in [1, m]$, $j \in [1, n]$, der *Vertauschungsoperator der k-ten und l-ten Zeile.*

(b) Für $k, l \in [1, m]$ mit $k \neq l$ und $c \in K$ heißt $\mathrm{add}_{k,l,c} \colon K^{m\times n} \to K^{m\times n}$ gegeben durch

$$\mathrm{add}_{k,l,c}(A)_{i,j} = \begin{cases} A_{k,j} + cA_{l,j}, & \text{falls } i = k, \\ A_{i,j}, & \text{falls } i \neq k, \end{cases}$$

für $i \in [1, m]$, $j \in [1, n]$, der *Additionsoperator des c-fachen der l-ten zur k-ten Zeile.*

(c) Für $k \in [1,m]$ und $c \in K^\times$ heißt $\mathrm{mul}_{k,c}\colon K^{m\times n} \to K^{m\times n}$ gegeben durch

$$\mathrm{mul}_{k,c}(A)_{i,j} = \begin{cases} cA_{k,j}, & \text{falls } i = k, \\ A_{i,j}, & \text{falls } i \neq k, \end{cases}$$

für $i \in [1,m]$, $j \in [1,n]$, der *Multiplikationsoperator der k-ten Zeile um das c-fache.*

Wir betonen, dass wir für die Definition des Additionsoperators in (2.15)(b) stets $k \neq l$ fordern, während dies für den Vertauschungsoperator in (2.15)(a) nicht zwingend vorgeschrieben wird: Im Fall $k = l$ gilt mit der dort verwendeten Notation $\mathrm{sw}_{k,l} = \mathrm{id}_{K^{m\times n}}$. Ebenso haben wir $\mathrm{add}_{k,l,c} = \mathrm{id}_{K^{m\times n}}$ im Fall $c = 0$ in Definition (2.15)(b) sowie $\mathrm{mul}_{k,c} = \mathrm{id}_{K^{m\times n}}$ im Fall $c = 1$ in Definition (2.15)(c).
Wenden wir den Vertauschungsoperator $\mathrm{sw}_{k,l}$ für $k,l \in [1,m]$ auf eine Matrix $A \in K^{m\times n}$ an, so bewirkt dies, dass die k-te und die l-te Zeile von A vertauscht werden. Steht die Matrix für ein lineares Gleichungssystem, so entspricht dies also gerade der Vertauschung der k-ten und l-ten Gleichung.
Wenden wir den Additionsoperator $\mathrm{add}_{k,l,c}$ für $k,l \in [1,m]$, $k \neq l$, $c \in K$ auf eine Matrix $A \in K^{m\times n}$ an, so bewirkt dies, dass das jeweilige c-fache der Komponenten der l-ten Zeile von A zu den Komponenten der k-ten Zeile von A addiert wird, Spalte für Spalte. Steht die Matrix für ein lineares Gleichungssystem, so entspricht dies also gerade der Addition des c-fachen der l-ten Gleichung zur k-ten Gleichung.
Wenden wir den Multiplikationsoperator $\mathrm{mul}_{k,c}$ für $k \in [1,m]$, $c \in K^\times$ auf eine Matrix $A \in K^{m\times n}$ an, so bewirkt dies, dass jede Komponente der k-ten Zeile von A mit c multipliziert wird. Steht die Matrix für ein lineares Gleichungssystem, so entspricht dies also gerade der Multiplikation der k-ten Gleichung mit c.

(2.16) Definition ((elementare) Zeilenoperatoren)**.** Es seien $m,n \in \mathbb{N}_0$ und ein Körper K gegeben.

(a) Ein *elementarer Zeilenoperator* auf $K^{m\times n}$ ist eine Abbildung $\rho\colon K^{m\times n} \to K^{m\times n}$ von der Form $\rho = \mathrm{sw}_{k,l}$ für gewisse $k,l \in [1,m]$ oder $\rho = \mathrm{add}_{k,l,c}$ für gewisse $k,l \in [1,m]$ mit $k \neq l$ und $c \in K$ oder $\rho = \mathrm{mul}_{k,c}$ für gewisse $k \in [1,m]$, $c \in K^\times$.

(b) Ein *Zeilenoperator* auf $K^{m\times n}$ ist eine Abbildung $\rho\colon K^{m\times n} \to K^{m\times n}$, welche sich als (endliches) Kompositum von elementaren Zeilenoperatoren schreiben lässt.

(2.17) Beispiel. Über $\mathbb{Q}$ gilt

$$\begin{pmatrix} 0 & 2 & 1 & -3 \\ 2 & 0 & -2 & 6 \\ 0 & 4 & 2 & -7 \end{pmatrix} \overset{\mathrm{sw}_{1,2}}{\longmapsto} \begin{pmatrix} 2 & 0 & -2 & 6 \\ 0 & 2 & 1 & -3 \\ 0 & 4 & 2 & -7 \end{pmatrix} \overset{\mathrm{add}_{3,2,-2}}{\longmapsto} \begin{pmatrix} 2 & 0 & -2 & 6 \\ 0 & 2 & 1 & -3 \\ 0 & 0 & 0 & -1 \end{pmatrix} \overset{\mathrm{mul}_{1,\frac{1}{2}}}{\longmapsto} \begin{pmatrix} 1 & 0 & -1 & 3 \\ 0 & 2 & 1 & -3 \\ 0 & 4 & 2 & -7 \end{pmatrix}.$$

Wirkt ein (elementarer) Zeilenoperator auf einer Matrix, so sprechen wir von einer (elementaren) Zeilenoperation.

(2.18) Bemerkung. Es seien $m,n \in \mathbb{N}_0$ und ein Körper K gegeben.

(a) Für $k,l \in [1,m]$ mit $k \neq l$ ist

$$\mathrm{add}_{k,l,-}\colon K \to \mathrm{Map}(K^{m\times n}, K^{m\times n}),\ c \mapsto \mathrm{add}_{k,l,c}$$

ein Monoidhomomorphismus, wobei wir K als Monoid bzgl. der Addition betrachten.

(b) Für $k \in [1,m]$ ist

$$\mathrm{mul}_{k,-}\colon K^\times \to \mathrm{Map}(K^{m\times n}, K^{m\times n}),\ c \mapsto \mathrm{mul}_{k,c}$$

ein Monoidhomomorphismus.

Beweis.

(a) Siehe Aufgabe 50(a).

(b) Siehe Aufgabe 50(b). □

Die wichtigste Eigenschaft einer elementaren Zeilenoperation ist ihre Fähigkeit, rückgängig gemacht zu werden:

(2.19) Bemerkung. Es seien $m, n \in \mathbb{N}_0$ und ein Körper K gegeben.

(a) Für $k, l \in [1, m]$ ist $\mathrm{sw}_{k,l} \colon K^{m\times n} \to K^{m\times n}$ eine invertierbare Abbildung mit

$$\mathrm{sw}_{k,l}^{-1} = \mathrm{sw}_{l,k} = \mathrm{sw}_{k,l}.$$

(b) Für $k, l \in [1, m]$ mit $k \neq l$ und $c \in K$ ist $\mathrm{add}_{k,l,c} \colon K^{m\times n} \to K^{m\times n}$ eine invertierbare Abbildung mit

$$\mathrm{add}_{k,l,c}^{-1} = \mathrm{add}_{k,l,-c}.$$

(c) Für $k \in [1, m]$, $c \in K^\times$ ist $\mathrm{mul}_{k,c} \colon K^{m\times n} \to K^{m\times n}$ eine invertierbare Abbildung mit

$$\mathrm{mul}_{k,c}^{-1} = \mathrm{mul}_{k,c^{-1}}.$$

Beweis.

(a) Für $k, l \in [1, m]$ gilt

$$\mathrm{sw}_{l,k}(\mathrm{sw}_{k,l}(A))_{i,j} = \left.\begin{cases} \mathrm{sw}_{k,l}(A)_{k,j}, & \text{falls } i = l, \\ \mathrm{sw}_{k,l}(A)_{l,j}, & \text{falls } i = k, \\ \mathrm{sw}_{k,l}(A)_{i,j}, & \text{falls } i \notin \{k, l\} \end{cases}\right\} = \left.\begin{cases} A_{l,j}, & \text{falls } i = l, \\ A_{k,j}, & \text{falls } i = k, \\ A_{i,j}, & \text{falls } i \notin \{k, l\} \end{cases}\right\} = A_{i,j}$$

für $i \in [1, m]$, $j \in [1, l]$, also $\mathrm{sw}_{l,k}(\mathrm{sw}_{k,l}(A)) = A$ für $A \in K^{m\times n}$ und damit

$$\mathrm{sw}_{l,k} \circ \mathrm{sw}_{k,l} = \mathrm{id}_{K^{m\times n}}.$$

Wegen $\mathrm{sw}_{l,k} = \mathrm{sw}_{k,l}$ impliziert dies aber auch

$$\mathrm{sw}_{k,l} \circ \mathrm{sw}_{l,k} = \mathrm{sw}_{l,k} \circ \mathrm{sw}_{k,l} = \mathrm{id}_{K^{m\times n}}$$

für $k, l \in [1, m]$, d.h. $\mathrm{sw}_{k,l}$ ist eine invertierbare Abbildung mit

$$\mathrm{sw}_{k,l}^{-1} = \mathrm{sw}_{l,k} = \mathrm{sw}_{k,l}.$$

(b) Es seien $k, l \in [1, m]$ mit $k \neq l$ gegeben. Nach Bemerkung (2.18)(a) ist $\mathrm{add}_{k,l,-} \colon K \to \mathrm{Map}(K^{m\times n}, K^{m\times n})$, $c \mapsto \mathrm{add}_{k,l,c}$ ein Monoidhomomorphismus. Nun ist aber K eine abelsche Gruppe und damit $\mathrm{add}_{k,l,c}$ für $c \in K$ nach Bemerkung (1.66) invertierbar mit

$$\mathrm{add}_{k,l,c}^{-1} = \mathrm{add}_{k,l,-c}.$$

(c) Es sei $k \in [1, m]$ gegeben. Nach Bemerkung (2.18)(b) ist $\mathrm{mul}_{k,-} \colon K^\times \to \mathrm{Map}(K^{m\times n}, K^{m\times n})$, $c \mapsto \mathrm{mul}_{k,c}$ ein Monoidhomomorphismus. Nun ist aber $K^\times$ eine Gruppe und damit $\mathrm{mul}_{k,c}$ für $c \in K$ nach Bemerkung (1.66) invertierbar mit

$$\mathrm{mul}_{k,c}^{-1} = \mathrm{mul}_{k,c^{-1}}.$$ □

(2.20) Korollar. Es seien $m, n \in \mathbb{N}_0$ und ein Körper K gegeben.

(a) Für $k, l \in [1, m]$ mit $k \neq l$ ist

$$\mathrm{add}_{k,l,-} \colon K \to \mathrm{S}_{K^{m\times n}},\ c \mapsto \mathrm{add}_{k,l,c}$$

ein Gruppenhomomorphismus, wobei wir K als Gruppe bzgl. der Addition betrachten.

(b) Für $k \in [1, m]$ ist

$$\mathrm{mul}_{k,-} \colon K^\times \to \mathrm{S}_{K^{m\times n}},\ c \mapsto \mathrm{mul}_{k,c}$$

ein Gruppenhomomorphismus.

Beweis.

(a) Dies folgt aus Bemerkung (2.18)(a) und Bemerkung (2.19)(b).

(b) Dies folgt aus Bemerkung (2.18)(b) und Bemerkung (2.19)(c). □

(2.21) Bemerkung. Es seien $m, n, p \in \mathbb{N}_0$, ein Körper K und $A \in K^{m\times n}$, $B \in K^{m\times p}$ gegeben.

(a) Für $k, l \in [1, m]$ gilt

$$\mathrm{sw}_{k,l}(\begin{pmatrix} A & B \end{pmatrix}) = \begin{pmatrix} \mathrm{sw}_{k,l}(A) & \mathrm{sw}_{k,l}(B) \end{pmatrix}.$$

(b) Für $k, l \in [1, m]$ mit $k \neq l$ und $c \in K$ gilt

$$\mathrm{add}_{k,l,c}(\begin{pmatrix} A & B \end{pmatrix}) = \begin{pmatrix} \mathrm{add}_{k,l,c}(A) & \mathrm{add}_{k,l,c}(B) \end{pmatrix}.$$

(c) Für $k \in [1, m]$, $c \in K^\times$ gilt

$$\mathrm{mul}_{k,c}(\begin{pmatrix} A & B \end{pmatrix}) = \begin{pmatrix} \mathrm{mul}_{k,c}(A) & \mathrm{mul}_{k,c}(B) \end{pmatrix}.$$

Beweis.

(a) Für $k, l \in [1, m]$ gilt

$$\begin{aligned}
\mathrm{sw}_{k,l}(\begin{pmatrix} A & B \end{pmatrix})_{i,j} &= \begin{cases} \begin{pmatrix} A & B \end{pmatrix}_{l,j}, & \text{falls } i = k, \\ \begin{pmatrix} A & B \end{pmatrix}_{k,j}, & \text{falls } i = l, \\ \begin{pmatrix} A & B \end{pmatrix}_{i,j}, & \text{falls } i \notin \{k, l\} \end{cases} \\
&= \begin{cases} A_{l,j}, & \text{falls } j \in [1, n],\ i = k, \\ A_{k,j}, & \text{falls } j \in [1, n],\ i = l, \\ A_{i,j}, & \text{falls } j \in [1, n],\ i \notin \{k, l\}, \\ B_{l,j-n}, & \text{falls } j \in [n+1, n+p],\ i = k, \\ B_{k,j-n}, & \text{falls } j \in [n+1, n+p],\ i = l, \\ B_{i,j-n}, & \text{falls } j \in [n+1, n+p],\ i \notin \{k, l\} \end{cases} \\
&= \begin{cases} \mathrm{sw}_{k,l}(A)_{i,j}, & \text{falls } j \in [1, n], \\ \mathrm{sw}_{k,l}(B)_{i,j-n}, & \text{falls } j \in [n+1, n+p] \end{cases} = \begin{pmatrix} \mathrm{sw}_{k,l}(A) & \mathrm{sw}_{k,l}(B) \end{pmatrix}_{i,j}
\end{aligned}$$

für $i \in [1, m]$, $j \in [1, n+p]$, also $\mathrm{sw}_{k,l}(\begin{pmatrix} A & B \end{pmatrix}) = \begin{pmatrix} \mathrm{sw}_{k,l}(A) & \mathrm{sw}_{k,l}(B) \end{pmatrix}$.

(b) Für $k, l \in [1, m]$ mit $k \neq l$ und $c \in K$ gilt

$$\begin{aligned}
\mathrm{add}_{k,l,c}(\begin{pmatrix} A & B \end{pmatrix})_{i,j} &= \begin{cases} \begin{pmatrix} A & B \end{pmatrix}_{k,j} + c \begin{pmatrix} A & B \end{pmatrix}_{l,j}, & \text{falls } i = k, \\ \begin{pmatrix} A & B \end{pmatrix}_{i,j}, & \text{falls } i \neq k \end{cases} \\
&= \begin{cases} A_{k,j} + cA_{l,j}, & \text{falls } j \in [1, n],\ i = k, \\ A_{i,j}, & \text{falls } j \in [1, n],\ i \neq k, \\ B_{k,j-n} + cB_{l,j-n}, & \text{falls } j \in [n+1, n+p],\ i = k, \\ B_{i,j-n}, & \text{falls } j \in [n+1, n+p],\ i \neq k \end{cases} \\
&= \begin{cases} \mathrm{add}_{k,l,c}(A)_{i,j}, & \text{falls } j \in [1, n], \\ \mathrm{add}_{k,l,c}(B)_{i,j-n}, & \text{falls } j \in [n+1, n+p] \end{cases} = \begin{pmatrix} \mathrm{add}_{k,l,c}(A) & \mathrm{add}_{k,l,c}(B) \end{pmatrix}_{i,j},
\end{aligned}$$

für $i \in [1, m]$, $j \in [1, n+p]$, also $\mathrm{add}_{k,l,c}(\begin{pmatrix} A & B \end{pmatrix}) = \begin{pmatrix} \mathrm{add}_{k,l,c}(A) & \mathrm{add}_{k,l,c}(B) \end{pmatrix}$.

(c) Für $k \in [1,m]$, $c \in K^\times$ gilt

$$\begin{aligned}\mathrm{mul}_{k,c}(\begin{pmatrix}A & B\end{pmatrix})_{i,j} &= \begin{cases} c\begin{pmatrix}A & B\end{pmatrix}_{k,j}, & \text{falls } i = k, \\ \begin{pmatrix}A & B\end{pmatrix}_{i,j}, & \text{falls } i \neq k \end{cases} \\ &= \begin{cases} cA_{k,j}, & \text{falls } j \in [1,n],\ i = k, \\ A_{i,j}, & \text{falls } j \in [1,n],\ i \neq k, \\ cB_{k,j-n}, & \text{falls } j \in [n+1,n+p],\ i = k, \\ B_{i,j-n}, & \text{falls } j \in [n+1,n+p],\ i \neq k \end{cases} \\ &= \begin{cases} \mathrm{mul}_{k,c}(A)_{i,j}, & \text{falls } j \in [1,n], \\ \mathrm{mul}_{k,c}(B)_{i,j-n}, & \text{falls } j \in [n+1,n+p] \end{cases} = \begin{pmatrix}\mathrm{mul}_{k,c}(A) & \mathrm{mul}_{k,c}(B)\end{pmatrix}_{i,j}\end{aligned}$$

für $i \in [1,m]$, $j \in [1,n+p]$, also $\mathrm{mul}_{k,c}(\begin{pmatrix}A & B\end{pmatrix}) = \begin{pmatrix}\mathrm{mul}_{k,c}(A) & \mathrm{mul}_{k,c}(B)\end{pmatrix}$. □

Wir betrachten elementare Zeilenoperatoren, weil sie die Lösungsmengen linearer Gleichungssysteme invariant lassen:

(2.22) Proposition. Es seien $m, n \in \mathbb{N}_0$, ein Körper K und ein Zeilenoperator ρ auf $K^{m\times n}$ gegeben. Ferner seien $A \in K^{m\times n}$, $b \in K^{m\times 1}$ und $x \in K^{n\times 1}$ gegeben. Genau dann ist x eine Lösung des linearen Gleichungssystem zur erweiterten Koeffizientenmatrix $\left(A \mid b\right)$, wenn x eine Lösung des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix $\rho(\left(A \mid b\right))$ ist.

Beweis. Wir halten zunächst fest, dass es genügt, die Aussage für einen elementaren Zeilenoperator ρ zu zeigen, der allgemeine Fall folgt dann durch Induktion unter Ausnutzung von Proposition (1.47)(a) und Bemerkung (2.19). Es sei im Folgenden also ρ ein elementarer Zeilenoperator auf $K^{m\times n}$, d.h. $\rho = \mathrm{sw}_{k,l}$ für gewisse $k, l \in [1,m]$ oder $\rho = \mathrm{add}_{k,l,c}$ für gewisse $k, l \in [1,m]$ mit $k \neq l$ oder $\rho = \mathrm{mul}_{k,c}$ für gewisse $k \in [1,m]$, $c \in K^\times$ und $c \in K$.
Es sei x eine Lösung des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix $\left(A \mid b\right)$, d.h. es gelte

$$\sum_{j\in[1,n]} A_{i,j}x_j = b_i$$

für $i \in [1,m]$.
Zuerst sei $\rho = \mathrm{sw}_{k,l}$ für gewisse $k, l \in [1,m]$. Dann gilt einerseits

$$\begin{aligned}\sum_{j\in[1,n]} \mathrm{sw}_{k,l}(A)_{k,j}x_j &= \sum_{j\in[1,n]} A_{l,j}x_j = b_l = \mathrm{sw}_{k,l}(b)_k, \\ \sum_{j\in[1,n]} \mathrm{sw}_{k,l}(A)_{l,j}x_j &= \sum_{j\in[1,n]} A_{k,j}x_j = b_k = \mathrm{sw}_{k,l}(b)_l,\end{aligned}$$

andererseits aber auch

$$\sum_{j\in[1,n]} \mathrm{sw}_{k,l}(A)_{i,j}x_j = \sum_{j\in[1,n]} A_{i,j}x_j = b_i = \mathrm{sw}_{k,l}(b)_i$$

für $i \in [1,m] \setminus \{k,l\}$. Insgesamt gilt also

$$\sum_{j\in[1,n]} \mathrm{sw}_{k,l}(A)_{i,j}x_j = \mathrm{sw}_{k,l}(b)_i$$

für alle $i \in [1,m]$, d.h. x ist eine Lösung des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix $\left(\mathrm{sw}_{k,l}(A) \mid \mathrm{sw}_{k,l}(b)\right) = \mathrm{sw}_{k,l}(\left(A \mid b\right)) = \rho(\left(A \mid b\right))$.
Als nächstes sei $\rho = \mathrm{add}_{k,l,c}$ für gewisse $k, l \in [1,m]$ mit $k \neq l$ und $c \in K$. Dann gilt einerseits

$$\sum_{j\in[1,n]} \mathrm{add}_{k,l,c}(A)_{k,j}x_j = \sum_{j\in[1,n]} (A_{k,j} + cA_{l,j})x_j = \sum_{j\in[1,n]} A_{k,j}x_j + c\sum_{j\in[1,n]} A_{l,j}x_j = b_k + cb_l = \mathrm{add}_{k,l,c}(b)_k,$$

andererseits aber auch

$$\sum_{j\in[1,n]} \mathrm{add}_{k,l,c}(A)_{i,j}x_j = \sum_{j\in[1,n]} A_{i,j}x_j = b_i = \mathrm{add}_{k,l,c}(b)_i$$

für $i \in [1,m] \setminus \{k\}$. Insgesamt gilt also

$$\sum_{j\in[1,n]} \mathrm{add}_{k,l,c}(A)_{i,j}x_j = \mathrm{add}_{k,l,c}(b)_i$$

für alle $i \in [1,m]$, d.h. x ist eine Lösung des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix $\big(\mathrm{add}_{k,l,c}(A) \mid \mathrm{add}_{k,l,c}(b)\big) = \mathrm{add}_{k,l,c}\big(\big(A \mid b\big)\big) = \rho(\big(A \mid b\big))$.
Schließlich sei $\rho = \mathrm{mul}_{k,c}$ für gewisse $k \in [1,m]$, $c \in K^\times$. Dann gilt einerseits

$$\sum_{j\in[1,n]} \mathrm{mul}_{k,c}(A)_{k,j}x_j = \sum_{j\in[1,n]} cA_{k,j}x_j = c\sum_{j\in[1,n]} A_{k,j}x_j = cb_k = \mathrm{mul}_{k,c}(b)_k,$$

andererseits aber auch

$$\sum_{j\in[1,n]} \mathrm{mul}_{k,c}(A)_{i,j}x_j = \sum_{j\in[1,n]} A_{i,j}x_j = b_i = \mathrm{mul}_{k,c}(b)_i$$

für $i \in [1,m] \setminus \{k\}$. Insgesamt gilt also

$$\sum_{j\in[1,n]} \mathrm{mul}_{k,c}(A)_{i,j}x_j = \mathrm{mul}_{k,c}(b)_i$$

für alle $i \in [1,m]$, d.h. x ist eine Lösung des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix $\big(\mathrm{mul}_{k,c}(A) \mid \mathrm{mul}_{k,c}(b)\big) = \mathrm{mul}_{k,c}\big(\big(A \mid b\big)\big) = \rho(\big(A \mid b\big))$.
Folglich ist in jedem Fall x auch eine Lösung des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix $\rho(\big(A \mid b\big))$.
Umgekehrt sei nun x eine Lösung des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix $\rho(\big(A \mid b\big))$. Nach Bemerkung (2.19) ist ρ invertierbar und ρ^{-1} ist ebenfalls ein elementarer Zeilenoperator auf $K^{m\times n}$. Folglich ist x auch eine Lösung des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix $\rho^{-1}(\rho(\big(A \mid b\big))) = \big(A \mid b\big)$. □

(2.23) Bemerkung. Es seien $m,n \in \mathbb{N}_0$, ein Körper K, ein $A \in K^{m\times n}$, ein Zeilenoperator ρ auf $K^{m\times n}$ und ein $j \in [1,n]$ gegeben. Genau dann gilt $A_{i,j} = 0$ für alle $i \in [1,m]$, wenn $\rho(A)_{i,j} = 0$ für alle $i \in [1,m]$.

Beweis. Wir halten zunächst fest, dass es genügt, die Aussage für einen elementaren Zeilenoperator ρ zu zeigen, der allgemeine Fall folgt dann durch Induktion unter Ausnutzung von Proposition (1.47)(a) und Bemerkung (2.19). Es sei im Folgenden also ρ ein elementarer Zeilenoperator auf $K^{m\times n}$, d.h. $\rho = \mathrm{sw}_{k,l}$ für gewisse $k,l \in [1,m]$ oder $\rho = \mathrm{add}_{k,l,c}$ für gewisse $k,l \in [1,m]$ mit $k \neq l$ oder $\rho = \mathrm{mul}_{k,c}$ für gewisse $k \in [1,m]$, $c \in K^\times$ und $c \in K$.
Es gelte zunächst $A_{i,j} = 0$ für alle $i \in [1,m]$. Wenn $\rho = \mathrm{sw}_{k,l}$ für gewisse $k,l \in [1,m]$ ist, so haben wir

$$\rho(A)_{i,j} = \mathrm{sw}_{k,l}(A)_{i,j} = \begin{cases} A_{l,j}, & \text{falls } i = k, \\ A_{k,j}, & \text{falls } i = l, \\ A_{i,j}, & \text{falls } i \notin \{k,l\} \end{cases} = 0$$

für alle $i \in [1,m]$. Ferner, wenn $\rho = \mathrm{add}_{k,l,c}$ für gewisse $k,l \in [1,m]$ mit $k \neq l$ und $c \in K$ ist, so haben wir

$$\rho(A)_{i,j} = \mathrm{add}_{k,l,c}(A)_{i,j} = \begin{cases} A_{k,j} + cA_{l,j}, & \text{falls } i = k, \\ A_{i,j}, & \text{falls } i \neq k \end{cases} = \begin{cases} 0 + c\cdot 0, & \text{falls } i = k, \\ 0, & \text{falls } i \neq k \end{cases} = 0$$

für alle $i \in [1,m]$. Schließlich, wenn $\rho = \mathrm{mul}_{k,c}$ für gewisse $k \in [1,m]$, $c \in K^\times$ ist, so haben wir

$$\rho(A)_{i,j} = \mathrm{mul}_{k,c}(A)_{i,j} = \begin{cases} cA_{k,j}, & \text{falls } i = k, \\ A_{i,j}, & \text{falls } i \neq k \end{cases} = \begin{cases} c\cdot 0, & \text{falls } i = k, \\ 0, & \text{falls } i \neq k \end{cases} = 0$$

für alle $i \in [1,m]$. Folglich ist in jedem Fall $\rho(A)_{i,j} = 0$ für alle $i \in [1,m]$.
Es gelte also umgekehrt $\rho(A)_{i,j} = 0$ für alle $i \in [1,m]$. Nach Bemerkung (2.19) ist ρ invertierbar und ρ^{-1} ist ebenfalls ein elementarer Zeilenoperator auf $K^{m\times n}$. Folglich ist auch $A_{i,j} = \rho^{-1}(\rho(A))_{i,j} = 0$ für alle $i \in [1,m]$. □

Im Allgemeinen kommutieren verschiedene (elementare) Zeilenoperatoren nicht. Es gilt jedoch folgende Aussage, welche wir im Beweis von Satz (2.25) benötigen werden.

(2.24) Bemerkung. Es seien $m, n \in \mathbb{N}_0$ und ein Körper K gegeben.

(a) Für alle $k, k', l \in [1, m]$ mit $k \neq l$, $k' \neq l$ und $c, c' \in K$ gilt

$$\mathrm{add}_{k,l,c} \circ \mathrm{add}_{k',l,c'} = \mathrm{add}_{k',l,c'} \circ \mathrm{add}_{k,l,c}.$$

(b) Für alle $k, k' \in [1, m]$, $c, c' \in K^\times$ gilt

$$\mathrm{mul}_{k,c} \circ \mathrm{mul}_{k',c'} = \mathrm{mul}_{k',c'} \circ \mathrm{mul}_{k,c}.$$

Beweis.

(a) Es seien $k, k', l \in [1, m]$ mit $k \neq l$, $k' \neq l$ und $c, c' \in K$ gegeben. Im Fall $k = k'$ haben wir

$$\begin{aligned}\mathrm{add}_{k,l,c} \circ \mathrm{add}_{k',l,c'} &= \mathrm{add}_{k,l,c} \circ \mathrm{add}_{k,l,c'} = \mathrm{add}_{k,l,c+c'} = \mathrm{add}_{k,l,c'+c} = \mathrm{add}_{k,l,c'} \circ \mathrm{add}_{k,l,c} \\ &= \mathrm{add}_{k',l,c'} \circ \mathrm{add}_{k,l,c}.\end{aligned}$$

Im Fall $k \neq k'$ erhalten wir hingegen

$$\begin{aligned}\mathrm{add}_{k,l,c}(\mathrm{add}_{k',l,c'}(A))_{i,j} &= \begin{Bmatrix}\mathrm{add}_{k',l,c'}(A)_{k,j} + c\,\mathrm{add}_{k',l,c'}(A)_{l,j}, & \text{falls } i = k, \\ \mathrm{add}_{k',l,c'}(A)_{i,j}, & \text{falls } i \neq k\end{Bmatrix} \\ &= \begin{Bmatrix}A_{k,j} + cA_{l,j}, & \text{falls } i = k, \\ A_{k',j} + c'A_{l,j}, & \text{falls } i = k', \\ A_{i,j}, & \text{falls } i \notin \{k, k'\}\end{Bmatrix} \\ &= \begin{Bmatrix}\mathrm{add}_{k,l,c}(A)_{k',j} + c'\mathrm{add}_{k,l,c}(A)_{l,j}, & \text{falls } i = k', \\ \mathrm{add}_{k,l,c}(A)_{i,j}, & \text{falls } i \neq k'\end{Bmatrix} \\ &= \mathrm{add}_{k',l,c'}(\mathrm{add}_{k,l,c}(A))_{i,j}\end{aligned}$$

für $i \in [1, m]$, $j \in [1, n]$, also $\mathrm{add}_{k,l,c}(\mathrm{add}_{k',l,c'}(A)) = \mathrm{add}_{k',l,c'}(\mathrm{add}_{k,l,c}(A))$ für $A \in K^{m \times n}$. In beiden Fällen gilt also

$$\mathrm{add}_{k,l,c} \circ \mathrm{add}_{k',l,c'} = \mathrm{add}_{k',l,c'} \circ \mathrm{add}_{k,l,c}.$$

(b) Es seien $k, k' \in [1, m]$, $c, c' \in K^\times$ gegeben. Im Fall $k = k'$ haben

$$\mathrm{mul}_{k,c} \circ \mathrm{mul}_{k',c'} = \mathrm{mul}_{k,c} \circ \mathrm{mul}_{k,c'} = \mathrm{mul}_{k,cc'} = \mathrm{mul}_{k,c'c} = \mathrm{mul}_{k,c'} \circ \mathrm{mul}_{k,c} = \mathrm{mul}_{k',c'} \circ \mathrm{mul}_{k,c}.$$

Im Fall $k \neq k'$ erhalten wir hingegen

$$\begin{aligned}\mathrm{mul}_{k,c}(\mathrm{mul}_{k',c'}(A))_{i,j} &= \begin{Bmatrix}c\,\mathrm{mul}_{k',c'}(A)_{k,j}, & \text{falls } i = k, \\ \mathrm{mul}_{k',c'}(A)_{i,j}, & \text{falls } i \neq k\end{Bmatrix} = \begin{Bmatrix}cA_{k,j}, & \text{falls } i = k, \\ c'A_{k',j}, & \text{falls } i = k', \\ A_{i,j}, & \text{falls } i \notin \{k, k'\}\end{Bmatrix} \\ &= \begin{Bmatrix}c'\mathrm{mul}_{k,c}(A)_{k',j}, & \text{falls } i = k', \\ \mathrm{mul}_{k,c}(A)_{i,j}, & \text{falls } i \neq k'\end{Bmatrix} = \mathrm{mul}_{k',c'}(\mathrm{mul}_{k,c}(A))_{i,j}\end{aligned}$$

für $i \in [1, m]$, $j \in [1, n]$, also $\mathrm{mul}_{k,c}(\mathrm{mul}_{k',c'}(A)) = \mathrm{mul}_{k',c'}(\mathrm{mul}_{k,c}(A))$ für $A \in K^{m \times n}$. In beiden Fällen gilt also

$$\mathrm{mul}_{k,c} \circ \mathrm{mul}_{k',c'} = \mathrm{mul}_{k',c'} \circ \mathrm{mul}_{k,c}.$$

□

Das Gaußsche Eliminationsverfahren

Wir stellen nun ein Verfahren vor, welches mittels Zeilenoperationen eine gegebene Matrix in eine Matrix in (reduzierter) Zeilenstufenform überführt.

(2.25) Satz. Es seien $m, n \in \mathbb{N}_0$ und ein Körper K gegeben.

(a) Für alle $A \in K^{m\times n}$ existiert ein Zeilenoperator ρ auf $K^{m\times n}$, welcher sich als Kompositum von Vertauschungs- und Additionsoperatoren schreiben lässt, so, dass $\rho(A)$ in Zeilenstufenform ist.

(b) Für alle $A \in K^{m\times n}$ in Zeilenstufenform existiert ein Zeilenoperator ρ auf $K^{m\times n}$, welcher sich als Kompositum von Multiplikations- und Additionsoperatoren schreiben lässt, so, dass $\rho(A)$ in reduzierter Zeilenstufenform und $\mathrm{ech}_i(\rho(A)) = \mathrm{ech}_i(A)$ für alle $i \in [1, m]$ ist.

(c) Für alle $A \in K^{m\times n}$ existiert ein Zeilenoperator ρ auf $K^{m\times n}$ so, dass $\rho(A)$ in reduzierter Zeilenstufenform ist.

Beweis.

(a) Wir führen vollständige Induktion nach m, wobei für $m = 0$ nichts zu tun ist.

Es sei also ein $m \in \mathbb{N}$ beliebig gegeben und es sei angenommen, dass es für alle $B \in K^{(m-1)\times n'}$, wobei $n' \in \mathbb{N}_0$, einen Zeilenoperator σ auf $K^{(m-1)\times n}$ so gibt, dass $\sigma(B)$ in Zeilenstufenform und σ ein Kompositum von Vertauschungs- und Additionsoperatoren ist. Ferner sei ein $A \in K^{m\times n}$ gegeben.

Wenn $A_{i,j} = 0$ für alle $(i, j) \in [1, m] \times [1, n]$ gilt, so ist A bereits in Zeilenstufenform. Folglich ist $\mathrm{id}_{K^{m\times n}}$ ein Zeilenoperator auf $K^{m\times n}$, welcher sich als Kompositum von Vertauschungs- und Additionsoperatoren schreiben lässt, mit $\mathrm{id}_{K^{m\times n}}(A) = A$ in Zeilenstufenform.

Es sei also im Folgenden angenommen, dass es ein $(i, j) \in [1, m] \times [1, n]$ mit $A_{i,j} \neq 0$ gibt. Wir setzen $l := \min\{\mathrm{ech}_i(A) \mid i \in [1, m]\}$ und wählen ein $k \in [1, m]$ mit $l = \mathrm{ech}_k(A)$.

$$A = \left(\begin{array}{ccc|c|ccc} 0 & \dots & 0 & A_{1,l} & A_{1,l+1} & \dots & A_{1,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & A_{k-1,l} & A_{k-1,l+1} & \dots & A_{k-1,n} \\ \hline 0 & \dots & 0 & A_{k,l} & A_{k,l+1} & \dots & A_{k,n} \\ \hline 0 & \dots & 0 & A_{k+1,l} & A_{k+1,l+1} & \dots & A_{k+1,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & A_{m,l} & A_{m,l+1} & \dots & A_{m,n} \end{array}\right) \qquad A_{k,l} \neq 0$$

Ferner setzen wir

$$A' := \mathrm{sw}_{1,k}(A).$$

Für $i \in [1, m]$, $j \in [1, n]$ ist dann

$$A'_{i,j} = \mathrm{sw}_{1,k}(A)_{i,j} = \begin{cases} A_{k,j}, & \text{falls } i = 1, \\ A_{1,j}, & \text{falls } i = k, \\ A_{i,j}, & \text{falls } i \notin \{1, k\}. \end{cases}$$

Somit folgt

$$\mathrm{ech}_i(A') = \left.\begin{cases} \mathrm{ech}_k(A), & \text{falls } i = 1, \\ \mathrm{ech}_1(A), & \text{falls } i = k, \\ \mathrm{ech}_i(A), & \text{falls } i \notin \{1, k\} \end{cases}\right\} = \begin{cases} l, & \text{falls } i = 1, \\ \mathrm{ech}_1(A), & \text{falls } i = k, \\ \mathrm{ech}_i(A), & \text{falls } i \notin \{1, k\} \end{cases}$$

für $i \in [1, m]$. Wir haben also

$$\mathrm{ech}_1(A') = l \leq \mathrm{ech}_i(A')$$

für $i \in [2,m]$.

$$A' = \left(\begin{array}{ccc|c|ccc} 0 & \dots & 0 & A'_{1,l} & A'_{1,l+1} & \dots & A'_{1,n} \\ \hline 0 & \dots & 0 & A'_{2,l} & A'_{2,l+1} & \dots & A'_{2,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & A'_{m,l} & A'_{m,l+1} & \dots & A'_{m,n} \end{array}\right) \qquad A'_{1,l} \neq 0$$

Nach Bemerkung (2.24)(a) gilt

$$\mathrm{add}_{h,1,-A'_{h,l}A'^{-1}_{1,l}} \circ \mathrm{add}_{h',1,-A'_{h',l}A'^{-1}_{1,l}} = \mathrm{add}_{h',1,-A'_{h',l}A'^{-1}_{1,l}} \circ \mathrm{add}_{h,1,-A'_{h,l}A'^{-1}_{1,l}}$$

für $h, h' \in [2,m]$. Wir setzen weiter

$$A'' := (\bigcirc_{h\in[2,m]} \mathrm{add}_{h,1,-A'_{h,l}A'^{-1}_{1,l}})(A').$$

Für $j \in [1,n]$ ist dann

$$A''_{1,j} = (\bigcirc_{h\in[2,m]} \mathrm{add}_{h,1,-A'_{h,l}A'^{-1}_{1,l}})(A')_{1,j} = A'_{1,j}$$

und damit $\mathrm{ech}_1(A'') = \mathrm{ech}_1(A') = l$. Für $i \in [2,m]$, $j \in [1,n]$ ist ferner

$$A''_{i,j} = (\bigcirc_{h\in[2,m]} \mathrm{add}_{h,1,-A'_{h,l}A'^{-1}_{1,l}})(A')_{i,j} = \mathrm{add}_{i,1,-A'_{i,l}A'^{-1}_{1,l}}(A')_{i,j} = A'_{i,j} - A'_{i,l}A'^{-1}_{1,l}A'_{1,j},$$

also für $j \in [1,l]$ insbesondere

$$A''_{i,j} = A'_{i,j} - A'_{i,l}A'^{-1}_{1,l}A'_{1,j} = \left.\begin{cases} 0 - A'_{i,l}A'^{-1}_{1,l} \cdot 0, & \text{falls } j \in [1,l-1], \\ A'_{i,l} - A'_{i,l}A'^{-1}_{1,l}A'_{1,l}, & \text{falls } j = l \end{cases}\right\} = 0$$

und damit $\mathrm{ech}_i(A'') > l$. Wir haben also

$$\mathrm{ech}_1(A'') = l < \mathrm{ech}_i(A'')$$

für $i \in [2,m]$.

$$A'' = \left(\begin{array}{ccc|c|ccc} 0 & \dots & 0 & A''_{1,l} & A''_{1,l+1} & \dots & A''_{1,n} \\ \hline 0 & \dots & 0 & 0 & A''_{2,l+1} & \dots & A''_{2,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & A''_{m,l+1} & \dots & A''_{m,n} \end{array}\right) \qquad A''_{1,l} \neq 0$$

Nun definieren wir $B \in K^{(m-1)\times(n-l)}$ durch

$$B_{i,j} := A''_{i+1,j+l}$$

für $i \in [1,m-1]$, $j \in [1,n-l]$.

$$A'' = \left(\begin{array}{ccc|c|ccc} 0 & \dots & 0 & A''_{1,l} & A''_{1,l+1} & \dots & A''_{1,n} \\ \hline 0 & \dots & 0 & 0 & & & \\ \vdots & & \vdots & & & B & \\ 0 & \dots & 0 & 0 & & & \end{array}\right) \qquad A''_{1,l} \neq 0$$

Nach Induktionsvoraussetzung gibt es einen Zeilenoperator σ auf $K^{(m-1)\times(n-l)}$ so, dass $\sigma(B)$ in Zeilenstufenform und σ ein Kompositum von Vertauschungs- und Additionsoperatoren ist. Wegen $\mathrm{ech}_1(A'') = l < \mathrm{ech}_i(A'')$ für $i \in [2,m]$ gibt es dann aber auch einen Zeilenoperator $\tilde{\sigma}$ auf $K^{m\times n}$ so, dass $A''' := \tilde{\sigma}(A'')$

in Zeilenstufenform und $\tilde{\sigma}$ ein Kompositum von Vertauschungs- und Additionsoperatoren ist (man nehme jeweils „dieselben“ elementaren Zeilenoperatoren und addiere 1 zu jedem Zeilenindex).

$$A''' = \left(\begin{array}{ccc|c|ccc} 0 & \dots & 0 & A''_{1,l} & A''_{1,l+1} & \dots & A''_{1,n} \\ \hline 0 & \dots & 0 & 0 & & & \\ \vdots & & \vdots & & & \sigma(B) & \\ 0 & \dots & 0 & 0 & & & \end{array}\right) \qquad A''_{1,l} \neq 0$$

Wir setzen

$$\rho := \tilde{\sigma} \circ \Big(\bigcirc_{h\in[2,m]} \mathrm{add}_{h,1,-\frac{A'_{h,l}}{A'_{1,l}}} \Big) \circ \mathrm{sw}_{1,k}.$$

Dann ist ρ ein Kompositum aus Vertauschungs- und Additionsoperatoren und es ist

$$\rho(A) = \tilde{\sigma}\Big(\big(\bigcirc_{h\in[2,m]} \mathrm{add}_{h,1,-\frac{A'_{h,l}}{A'_{1,l}}}\big)(\mathrm{sw}_{1,k}(A))\Big) = \tilde{\sigma}\Big(\big(\bigcirc_{h\in[2,m]} \mathrm{add}_{h,1,-\frac{A'_{h,l}}{A'_{1,l}}}\big)(A')\Big) = \tilde{\sigma}(A'') = A'''$$

in Zeilenstufenform.

(b) Wir führen vollständige Induktion nach m, wobei für $m = 0$ nichts zu tun ist.

Es sei also ein $m \in \mathbb{N}$ beliebig gegeben und es sei angenommen, dass es für alle $B \in K^{m'\times n'}$ in Zeilenstufenform, wobei $m', n' \in \mathbb{N}_0$ mit $m' < m$, einen Zeilenoperator σ auf $K^{m'\times n'}$ mit $\sigma(B)$ in reduzierter Zeilenstufenform und $\mathrm{ech}_i(\sigma(B)) = \mathrm{ech}_i(B)$ für alle $i \in [1, m']$ gibt. Ferner sei ein $A \in K^{m\times n}$ in Zeilenstufenform gegeben.

Wenn $A_{i,j} = 0$ für alle $(i, j) \in [1, m] \times [1, n]$ gilt, so ist A bereits in reduzierter Zeilenstufenform. Folglich ist $\mathrm{id}_{K^{m\times n}}$ ein Zeilenoperator auf $K^{m\times n}$ mit $\mathrm{id}_{K^{m\times n}}(A) = A$ in reduzierter Zeilenstufenform.

Es sei also im Folgenden angenommen, dass es ein $(i, j) \in [1, m] \times [1, n]$ mit $A_{i,j} \neq 0$ gibt. Wir bezeichnen mit $r = \max\{i \in [1, m] \mid \mathrm{ech}_i(A) \in [1, n]\}$ die Stufenanzahl von A und setzen $s := \mathrm{ech}_r(A)$.

$$A = \left(\begin{array}{ccc|c|ccc} A_{1,1} & \dots & A_{1,s-1} & A_{1,s} & A_{1,s+1} & \dots & A_{1,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ A_{r-1,1} & \dots & A_{r-1,s-1} & A_{r-1,s} & A_{r-1,s+1} & \dots & A_{r-1,n} \\ \hline 0 & \dots & 0 & A_{r,s} & A_{r,s+1} & \dots & A_{r,n} \\ \hline 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 \end{array}\right) \qquad A_{r,s} \neq 0$$

Ferner setzen wir

$$A' := \mathrm{mul}_{r,A_{r,s}^{-1}}(A).$$

Für $i \in [1, m]$, $j \in [1, n]$ gilt dann

$$A'_{i,j} = \mathrm{mul}_{r,A_{r,s}^{-1}}(A)_{i,j} = \begin{cases} A_{r,s}^{-1}A_{r,j}, & \text{falls } i = r, \\ A_{i,j}, & \text{falls } i \neq r, \end{cases}$$

also insbesondere $A'_{r,j} = A_{r,s}^{-1} \cdot 0 = 0$ für $j \in [1, s-1]$ und $A'_{r,s} = A_{r,s}^{-1}A_{r,s} = 1$, sowie $A'_{i,j} = A_{i,j} = 0$ für $i \in [r+1, m]$, $j \in [1, n]$.

$$A' = \left(\begin{array}{ccc|c|ccc} A_{1,1} & \dots & A_{1,s-1} & A_{1,s} & A_{1,s+1} & \dots & A_{1,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ A_{r-1,1} & \dots & A_{r-1,s-1} & A_{r-1,s} & A_{r-1,s+1} & \dots & A_{r-1,n} \\ \hline 0 & \dots & 0 & 1 & A'_{r,s+1} & \dots & A'_{r,n} \\ \hline 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 \end{array}\right)$$

Nach Bemerkung (2.24)(a) gilt

$$\mathrm{add}_{k,r,-A_{k,s}} \circ \mathrm{add}_{k',r,-A_{k',s}} = \mathrm{add}_{k',r,-A_{k',s}} \circ \mathrm{add}_{k,r,-A_{k,s}}$$

für $k, k' \in [1, r-1]$. Wir setzen weiter

$$A'' := (\bigcirc_{k\in[1,r-1]} \mathrm{add}_{k,r,-A_{k,s}})(A').$$

Für $i \in [1,m]$, $j \in [1,n]$ ist dann

$$A''_{i,j} := (\bigcirc_{k\in[1,r-1]} \mathrm{add}_{k,r,-A_{k,s}})(A')_{i,j} = \left\{\begin{matrix}\mathrm{add}_{i,r,-A_{i,s}}(A')_{i,j}, & \text{falls } i \in [1,r-1],\\ A'_{i,j}, & \text{falls } i \in [r,m]\end{matrix}\right\}$$
$$= \begin{cases} A'_{i,j} - A_{i,s}A'_{r,j}, & \text{falls } i \in [1,r-1],\\ A'_{i,j}, & \text{falls } i \in [r,m],\end{cases}$$

also insbesondere $A''_{i,j} = A_{i,j} - A_{i,s} \cdot 0 = A_{i,j}$ für $i \in [1,r-1]$, $j \in [1,s-1]$ und $A''_{i,s} = A_{i,s} - A_{i,s} \cdot 1 = 0$ für $i \in [1,r-1]$, sowie $A''_{r,j} = 0$ für $j \in [1,s-1]$ und $A''_{r,s} = 1$, sowie $A''_{i,j} = 0$ für $i \in [r+1,m]$, $j \in [1,n]$.

$$A'' = \left(\begin{array}{ccc|c|ccc} A_{1,1} & \dots & A_{1,s-1} & 0 & A''_{1,s+1} & \dots & A''_{1,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ A_{r-1,1} & \dots & A_{r-1,s-1} & 0 & A''_{r-1,s+1} & \dots & A''_{r-1,n} \\ \hline 0 & \dots & 0 & 1 & A'_{r,s+1} & \dots & A'_{r,n} \\ \hline 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 \end{array}\right)$$

Nun definieren wir $B \in K^{(r-1)\times(n-1)}$ durch

$$B_{i,j} := \begin{cases} A''_{i,j}, & \text{falls } j \in [1,s-1],\\ A''_{i,j+1}, & \text{falls } j \in [s,n-1],\end{cases}$$

für $i \in [1,r-1]$, $j \in [1,n-1]$, so dass insbesondere $B_{i,j} = A_{i,j}$ für $i \in [1,r-1]$, $j \in [1,s-l]$ gilt.

$$A'' = \left(\begin{array}{ccc|c|ccc} B_{1,1} & \dots & B_{1,s-1} & 0 & B_{1,s} & \dots & B_{1,n-1} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ B_{r-1,1} & \dots & B_{r-1,s-1} & 0 & B_{r-1,s} & \dots & B_{r-1,n-1} \\ \hline 0 & \dots & 0 & 1 & A'_{r,s+1} & \dots & A'_{r,n} \\ \hline 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 \end{array}\right)$$

Nach Induktionsvoraussetzung gibt es einen Zeilenoperator σ auf $K^{(r-1)\times(n-1)}$ so, dass $\sigma(B)$ in reduzierter Zeilenstufenform und $\mathrm{ech}_i(\sigma(B)) = \mathrm{ech}_i(B)$ für alle $i \in [1,m']$ ist. Wegen $\mathrm{ech}_i(A'') < s = \mathrm{ech}_r(A) = \mathrm{ech}_r(A'')$ für $i \in [1,r-1]$ gibt es dann aber auch einen Zeilenoperator $\tilde{\sigma}$ auf $K^{m\times n}$ so, dass $A''' = \tilde{\sigma}(A'')$ in reduzierter Zeilenstufenform und $\mathrm{ech}_i(\tilde{\sigma}(A'')) = \mathrm{ech}_i(A'') = \mathrm{ech}_i(A)$ für alle $i \in [1,m]$ ist (man nehme jeweils „dieselben“ elementaren Zeilenoperatoren).

$$A''' = \left(\begin{array}{ccc|c|ccc} \sigma(B)_{1,1} & \dots & \sigma(B)_{1,s-1} & 0 & \sigma(B)_{1,s} & \dots & \sigma(B)_{1,n-1} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ \sigma(B)_{r-1,1} & \dots & \sigma(B)_{r-1,s-1} & 0 & \sigma(B)_{r-1,s} & \dots & \sigma(B)_{r-1,n-1} \\ \hline 0 & \dots & 0 & 1 & A'_{r,s+1} & \dots & A'_{r,n} \\ \hline 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & 0 & \dots & 0 \end{array}\right)$$

Wir setzen

$$\rho := \tilde{\sigma} \circ (\bigcirc_{k\in[1,r-1]} \mathrm{add}_{k,r,-A_{k,s}}) \circ \mathrm{mul}_{r,A_{r,s}^{-1}}.$$

Dann ist

$$\begin{aligned}\rho(A) &= \tilde{\sigma}((\bigcirc_{k\in[1,r-1]} \mathrm{add}_{k,r,-A_{k,s}})(\mathrm{mul}_{r,A_{r,s}^{-1}}(\rho_0(A)))) = \tilde{\sigma}((\bigcirc_{k\in[1,r-1]} \mathrm{add}_{k,r,-A_{k,s}})(\mathrm{mul}_{r,A_{r,s}^{-1}}(A)))\\ &= \tilde{\sigma}((\bigcirc_{k\in[1,r-1]} \mathrm{add}_{k,r,-A_{k,s}})(A')) = \tilde{\sigma}(A'') = A'''\end{aligned}$$

in reduzierter Zeilenstufenform und es gilt $\mathrm{ech}_i(\rho(A)) = \mathrm{ech}_i(A)$ für $i \in [1,m]$.

(c) Dies folgt aus (a) und (b). □

(2.26) Algorithmus (Gaußsches Eliminationsverfahren)**.**

(a) Algorithmus zur Berechnung einer Zeilenstufenform:

- Eingabe: $A \in K^{m\times n}$ für einen Körper K und $m,n \in \mathbb{N}_0$
- Ausgabe: $\rho(A) \in K^{m\times n}$ in Zeilenstufenform für einen Zeilenoperator ρ auf $K^{m\times n}$
- Verfahren:

```
function rowechelonform(A)
    if A_{i,j} = 0 für alle i ∈ [1,m], j ∈ [1,n] then
        return A;
    end if;

    l := min {ech_i(A) | i ∈ [1,m]};
    wähle k ∈ [1,n] mit l = ech_k(A);
    A := sw_{1,k}(A);
    for h ∈ [2,m] do
        A := add_{h,1,-A'_{h,l}A'^{-1}_{1,l}}(A);
    end for;

    definiere B ∈ K^{(m-1)×n-l} durch B_{i,j} := A_{i+1,j+l} für i ∈ [1,m-1], j ∈ [1,n-l];
    B := rowechelonform(B);
    ersetze A_{i,j} für i ∈ [2,m], j ∈ [l+1,n] durch B_{i-1,j-l};

    return A;
end function;
```

(b) Algorithmus zur Berechnung einer reduzierten Zeilenstufenform:

- Eingabe: $A \in K^{m\times n}$ für einen Körper K und $m,n \in \mathbb{N}_0$
- Ausgabe: $\rho(A) \in K^{m\times n}$ in reduzierter Zeilenstufenform für einen Zeilenoperator ρ auf $K^{m\times n}$
- Verfahren:

```
function reducedrowechelonform(A)
    if A_{i,j} = 0 für alle i ∈ [1,m], j ∈ [1,n] then
        return A;
    end if;

    A := rowechelonform(A);

    r := max {i ∈ [1,m] | ech_i(A) ∈ [1,n]};
    s := ech_r(A);
    A := mul_{r,A_{r,s}^{-1}}(A);
    for k ∈ [1,r-1] do
```

```
            A := add_{k,r,-A_{k,s}}(A);
        end for;

        definiere B ∈ K^{(r-1)×(n-1)} durch B_{i,j} := A_{i,j} für i ∈ [1, r-1], j ∈ [1, s-1]
            und B_{i,j} := A_{i,j+1} für i ∈ [1, r-1], j ∈ [s, n-1];
        B := reducedrowechelonform(B);
        ersetze A_{i,j} für i ∈ [1, r-1], j ∈ [1, s-1] durch B_{i,j}
            und A_{i,j} für i ∈ [1, r-1], j ∈ [s+1, n] durch B_{i,j-1};

        return A;
    end function;
```

(2.27) Beispiel. Für $B \in \mathbb{R}^{3\times 5}$ gegeben durch

$$B = \begin{pmatrix} -2 & 2 & -6 & -10 & -24 \\ 2 & 3 & -9 & -7 & -15 \\ 1 & 1 & -3 & -2 & -4 \end{pmatrix}$$

gibt es Zeilenoperatoren ρ und ρ' auf $\mathbb{R}^{3\times 5}$ mit

$$\rho(B) = \begin{pmatrix} 1 & 1 & -3 & -2 & -4 \\ 0 & 1 & -3 & -3 & -7 \\ 0 & 0 & 0 & -2 & -4 \end{pmatrix},$$
$$\rho'(B) = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & -3 & 0 & -1 \\ 0 & 0 & 0 & 1 & 2 \end{pmatrix}.$$

Beweis. Wir benutzen das Gaußsche Eliminationsverfahren (2.26):

$$\begin{pmatrix} -2 & 2 & -6 & -10 & -24 \\ 2 & 3 & -9 & -7 & -15 \\ 1 & 1 & -3 & -2 & -4 \end{pmatrix} \overset{\mathrm{sw}_{1,3}}{\longmapsto} \begin{pmatrix} 1 & 1 & -3 & -2 & -4 \\ -2 & 2 & -6 & -10 & -24 \\ 2 & 3 & -9 & -7 & -15 \end{pmatrix}$$
$$\overset{\mathrm{add}_{3,1,-2}\circ\mathrm{add}_{2,1,2}}{\longmapsto} \begin{pmatrix} 1 & 1 & -3 & -2 & -4 \\ 0 & 4 & -12 & -14 & -32 \\ 0 & 1 & -3 & -3 & -7 \end{pmatrix} \overset{\mathrm{sw}_{2,3}}{\longmapsto} \begin{pmatrix} 1 & 1 & -3 & -2 & -4 \\ 0 & 1 & -3 & -3 & -7 \\ 0 & 4 & -12 & -14 & -32 \end{pmatrix}$$
$$\overset{\mathrm{add}_{3,2,-4}}{\longmapsto} \begin{pmatrix} 1 & 1 & -3 & -2 & -4 \\ 0 & 1 & -3 & -3 & -7 \\ 0 & 0 & 0 & -2 & -4 \end{pmatrix} \overset{\mathrm{mul}_{3,-\frac{1}{2}}}{\longmapsto} \begin{pmatrix} 1 & 1 & -3 & -2 & -4 \\ 0 & 1 & -3 & -3 & -7 \\ 0 & 0 & 0 & 1 & 2 \end{pmatrix}$$
$$\overset{\mathrm{add}_{2,3,3}\circ\mathrm{add}_{1,3,2}}{\longmapsto} \begin{pmatrix} 1 & 1 & -3 & 0 & 0 \\ 0 & 1 & -3 & 0 & -1 \\ 0 & 0 & 0 & 1 & 2 \end{pmatrix} \overset{\mathrm{add}_{1,2,-1}}{\longmapsto} \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & -3 & 0 & -1 \\ 0 & 0 & 0 & 1 & 2 \end{pmatrix}$$

□

Insgesamt haben wir uns nun folgende Methode zur Berechnung der Lösungen eines linearen Gleichungssystems erarbeitet:

(2.28) Algorithmus.

- Eingabe: $A \in K^{m\times n}$, $b \in K^{m\times 1}$ für einen Körper K und $m, n \in \mathbb{N}_0$
- Ausgabe: $\mathrm{Sol}(A, b)$
- Verfahren:

```
function sol(A, b)
    A := rowechelonform(A) oder A := reducedrowechelonform(A);
    return solref(A, b);
end function;
```

Alternativer Beweis zu Beispiel (2.7). Nach Beispiel (2.27) gibt es einen Zeilenoperator ρ auf $\mathbb{R}^{3\times 5}$ mit

$$\rho'(\left(A \mid b\right)) = \left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & -3 & 0 & -1 \\ 0 & 0 & 0 & 1 & 2 \end{array}\right).$$

Mit Proposition (2.22) und Proposition (2.12) erhalten wir

$$\mathrm{Sol}(A,b) = \{ \begin{pmatrix} 1 \\ -1+3a \\ a \\ 2 \end{pmatrix} \mid a \in \mathbb{R}\}. \qquad \square$$

Betrachten wir zum Schluss dieses Abschnitts noch ein weiteres Beispiel, an welchem wir sehen werden, dass das Gaußsche Eliminationsverfahren zwar prinzipiell immer funktioniert, jedoch aus praktischen Gründen manchmal besser in leicht abgewandelter Form verwendet werden sollte.

(2.29) Beispiel. Es seien $A \in \mathbb{Q}^{3\times 3}$ und $b \in \mathbb{Q}^{3\times 1}$ gegeben durch

$$A := \begin{pmatrix} 8 & 8 & 2 \\ 5 & 6 & -2 \\ 11 & 2 & -4 \end{pmatrix},\ b := \begin{pmatrix} 30 \\ 11 \\ 3 \end{pmatrix}.$$

Die Lösungsmenge des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix $\left(A \mid b\right)$ ist gegeben durch

$$\mathrm{Sol}(A,b) = \{ \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}\}.$$

Beweis. Wir wenden das Gaußsche Eliminationsverfahren (2.26) auf $\left(A \mid b\right)$ an:

$$\left(\begin{array}{ccc|c} 8 & 8 & 2 & 30 \\ 5 & 6 & -2 & 11 \\ 11 & 2 & -4 & 3 \end{array}\right) \xrightarrow{\mathrm{add}_{3,1,-\frac{11}{8}} \circ \mathrm{add}_{2,1,-\frac{5}{8}}} \left(\begin{array}{ccc|c} 8 & 8 & 2 & 30 \\ 0 & 1 & -\frac{13}{4} & -\frac{31}{4} \\ 0 & -9 & -\frac{27}{4} & -\frac{153}{4} \end{array}\right) \xrightarrow{\mathrm{add}_{3,2,9}} \left(\begin{array}{ccc|c} 8 & 8 & 2 & 30 \\ 0 & 1 & -\frac{13}{4} & -\frac{31}{4} \\ 0 & 0 & -36 & -108 \end{array}\right)$$

$$\xrightarrow{\mathrm{mul}_{3,-\frac{1}{36}}} \left(\begin{array}{ccc|c} 8 & 8 & 2 & 30 \\ 0 & 1 & -\frac{13}{4} & -\frac{31}{4} \\ 0 & 0 & 1 & 3 \end{array}\right) \xrightarrow{\mathrm{add}_{2,3,\frac{13}{4}} \circ \mathrm{add}_{1,3,-2}} \left(\begin{array}{ccc|c} 8 & 8 & 0 & 24 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 3 \end{array}\right) \xrightarrow{\mathrm{add}_{1,2,-8}} \left(\begin{array}{ccc|c} 8 & 0 & 0 & 8 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 3 \end{array}\right)$$

$$\xrightarrow{\mathrm{mul}_{1,\frac{1}{8}}} \left(\begin{array}{ccc|c} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 3 \end{array}\right)$$

Mit Proposition (2.22) erhalten wir

$$\mathrm{Sol}(A,b) = \{ \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}\}. \qquad \square$$

Im Beweis zu Beispiel (2.29) haben wir das Gaußsche Eliminationsverfahren angewandt. Hierdurch traten im Laufe des Verfahrens Brüche auf, was das Rechnen von Hand etwas unangenehm macht.
Dies hätten wir vermeiden können, wenn wir den Algorithmus leicht abgewandelt hätten. Im nachfolgenden Beweis werden wir etwa nicht direkt die erste Spalte „ausräumen“, sondern zunächst die Einträge durch Addition von ganzzahligen Vielfachen betragsmäßig verringern. Hierdurch benötigen wir zwar mehr Schritte, vermeiden jedoch die Bildung von Brüchen.

Alternativer Beweis zu Beispiel (2.29). Wir formen $\left(A \mid b\right)$ mittels elementarer Zeilenoperationen um:

$$\left(\begin{array}{ccc|c} 8 & 8 & 2 & 30 \\ 5 & 6 & -2 & 11 \\ 11 & 2 & -4 & 3 \end{array}\right) \xrightarrow{\mathrm{mul}_{1,\frac{1}{4}}} \left(\begin{array}{ccc|c} 4 & 4 & 1 & 15 \\ 5 & 6 & -2 & 11 \\ 11 & 2 & -4 & 3 \end{array}\right) \xrightarrow{\mathrm{add}_{3,1,-3} \circ \mathrm{add}_{2,1,-1}} \left(\begin{array}{ccc|c} 4 & 4 & 1 & 15 \\ 1 & 2 & -3 & -4 \\ -1 & -10 & -7 & -42 \end{array}\right)$$

$$\xmapsto{\mathrm{add}_{3,2,1}\circ\mathrm{add}_{1,2,-4}} \left(\begin{array}{ccc|c} 0 & -4 & 13 & 31 \\ 1 & 2 & -3 & -4 \\ 0 & -8 & -10 & -46 \end{array}\right) \xmapsto{\mathrm{add}_{3,1,-2}} \left(\begin{array}{ccc|c} 0 & -4 & 13 & 31 \\ 1 & 2 & -3 & -4 \\ 0 & 0 & -36 & -108 \end{array}\right)$$
$$\xmapsto{\mathrm{mul}_{3,-\frac{1}{36}}} \left(\begin{array}{ccc|c} 0 & -4 & 13 & 31 \\ 1 & 2 & -3 & -4 \\ 0 & 0 & 1 & 3 \end{array}\right) \xmapsto{\mathrm{add}_{2,3,3}\circ\mathrm{add}_{1,3,-13}} \left(\begin{array}{ccc|c} 0 & -4 & 0 & -8 \\ 1 & 2 & 0 & 5 \\ 0 & 0 & 1 & 3 \end{array}\right) \xmapsto{\mathrm{mul}_{1,-\frac{1}{4}}} \left(\begin{array}{ccc|c} 0 & 1 & 0 & 2 \\ 1 & 2 & 0 & 5 \\ 0 & 0 & 1 & 3 \end{array}\right)$$
$$\xmapsto{\mathrm{add}_{2,1,-2}} \left(\begin{array}{ccc|c} 0 & 1 & 0 & 2 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 3 \end{array}\right) \xmapsto{\mathrm{sw}_{1,2}} \left(\begin{array}{ccc|c} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 3 \end{array}\right)$$

Mit Proposition (2.22) erhalten wir

$$\mathrm{Sol}(A,b) = \{\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}\}.$$ □

Wir hätten noch etwas effizienter arbeiten können, wenn wir beim Ausräumen mit der dritten anstatt der ersten Spalte begonnen hätten:

Alternativer Beweis zu Beispiel (2.29). Wir formen $\left(A \mid b\right)$ mittels elementarer Zeilenoperationen um:

$$\left(\begin{array}{ccc|c} 8 & 8 & 2 & 30 \\ 5 & 6 & -2 & 11 \\ 11 & 2 & -4 & 3 \end{array}\right) \xmapsto{\mathrm{add}_{2,1,1}\circ\mathrm{add}_{3,1,2}} \left(\begin{array}{ccc|c} 8 & 8 & 2 & 30 \\ 13 & 14 & 0 & 41 \\ 27 & 18 & 0 & 63 \end{array}\right) \xmapsto{\mathrm{mul}_{1,\frac{1}{4}}\circ\mathrm{mul}_{3,\frac{1}{9}}} \left(\begin{array}{ccc|c} 4 & 4 & 1 & 15 \\ 13 & 14 & 0 & 41 \\ 3 & 2 & 0 & 7 \end{array}\right)$$
$$\xmapsto{\mathrm{add}_{1,3,-2}\circ\mathrm{add}_{2,3,-7}} \left(\begin{array}{ccc|c} -2 & 0 & 1 & 1 \\ -8 & 0 & 0 & -8 \\ 3 & 2 & 0 & 7 \end{array}\right) \xmapsto{\mathrm{mul}_{2,-\frac{1}{8}}} \left(\begin{array}{ccc|c} -2 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 3 & 2 & 0 & 7 \end{array}\right) \xmapsto{\mathrm{add}_{1,2,2}\circ\mathrm{add}_{3,2,-3}} \left(\begin{array}{ccc|c} 0 & 0 & 1 & 3 \\ 1 & 0 & 0 & 1 \\ 0 & 2 & 0 & 4 \end{array}\right)$$
$$\xmapsto{\mathrm{mul}_{3,\frac{1}{2}}} \left(\begin{array}{ccc|c} 0 & 0 & 1 & 3 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2 \end{array}\right)$$

Mit Proposition (2.22) erhalten wir

$$\mathrm{Sol}(A,b) = \{\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}\}.$$ □

Aufgaben

Aufgabe 49 (2 lineare Gleichungen in 2 Unbekannten)**.** Es seien ein Körper K und $a, b, c, d \in K$ gegeben. Zeigen Sie, dass folgende Bedingungen äquivalent sind.

(a) Für alle $e, f \in K$ gibt es genau ein $(x, y) \in K \times K$ mit

$$ax + by = e,$$
$$cx + dy = f.$$

(b) Für $(x, y) \in K \times K$ folgt aus

$$ax + by = 0,$$
$$cx + dy = 0$$

bereits $(x, y) = (0, 0)$.

(c) Es gilt

$$ad - bc \neq 0.$$

Aufgabe 50 (elementare Zeilenoperatoren)**.** Es seien $m, n \in \mathbb{N}_0$ und ein Körper K gegeben. Zeigen Sie:

(a) Für $k, l \in [1, m]$ mit $k \neq l$ ist

$$\mathrm{add}_{k,l,-} \colon K \to \mathrm{Map}(K^{m\times n}, K^{m\times n}),\ c \mapsto \mathrm{add}_{k,l,c}$$

ein Monoidhomomorphismus, wobei wir K als Monoid bzgl. der Addition betrachten.

(b) Für $k \in [1, m]$ ist

$$\mathrm{mul}_{k,-} \colon K^\times \to \mathrm{Map}(K^{m\times n}, K^{m\times n}),\ c \mapsto \mathrm{mul}_{k,c}$$

ein Monoidhomomorphismus.

Aufgabe 51 (lineares Gleichungssystem mit verschiedenen rechten Seiten)**.** Es seien $A \in \mathbb{R}^{4\times 5}$ und $b_i \in \mathbb{R}^{4\times 1}$ für $i \in [1, 3]$ gegeben durch

$$A := \begin{pmatrix} 1 & -1 & 5 & 3 & 2 \\ 1 & 2 & -1 & 3 & -1 \\ 0 & 1 & -2 & 2 & 1 \\ -1 & -7 & 11 & -1 & 8 \end{pmatrix},\ b_1 := \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix},\ b_2 := \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix},\ b_3 := \begin{pmatrix} 4 \\ 3 \\ 2 \\ 1 \end{pmatrix}.$$

Bestimmen Sie die Lösungsmenge des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix $\left(A \mid b_i\right)$ für $i \in [1, 3]$.

Aufgabe 52 (lineares Gleichungssystem mit Parameter)**.** Es sei $a \in \mathbb{Q}$ gegeben. Bestimmen Sie in Abhängigkeit von a die Menge aller $x \in \mathbb{Q}^{4\times 1}$ mit

$$\begin{array}{rcrcrcl} x_1 & + & ax_2 & & & + & x_4 = 1, \\ & & x_2 & + & ax_3 & & = 1, \\ x_1 & & & - & x_3 & + & a^2 x_4 = 2. \end{array}$$

Aufgabe 53 (lineares Gleichungssystem über verschiedenen Körpern)**.** Es seien ein Körper K und $A \in K^{4\times 4}$ gegeben durch

$$A := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 9 & 6 & 8 \\ 3 & 12 & 17 & 12 \\ 4 & 18 & 21 & 27 \end{pmatrix}.$$

Bestimmen Sie die Anzahl der Lösungen des homogenen linearen Gleichungssystems zur Koeffizientenmatrix A für

$$K \in \{\mathbb{Q}, \mathbb{R}, \mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5, \mathbb{F}_7, \mathbb{F}_{11}, \mathbb{F}_{13}\}.$$

Aufgabe 54 (lineares Gleichungssystem über $\mathbb{Z}$)**.**

(a) Bestimmen Sie die Menge aller $x \in \mathbb{Q}^{3\times 1}$ mit

$$\begin{array}{rcrcrcl} & & x_1 & + & 2x_2 & & = 0, \\ & & 2x_1 & + & 6x_2 & - & x_3 = 0, \\ - & & x_1 & - & 4x_2 & + & x_3 = 0. \end{array}$$

(b) Bestimmen Sie die Menge aller $x \in \mathbb{Z}^{3\times 1}$ mit

$$\begin{array}{rcrcrcl} & & x_1 & + & 2x_2 & & = 0, \\ & & 2x_1 & + & 6x_2 & - & x_3 = 0, \\ - & & x_1 & - & 4x_2 & + & x_3 = 0. \end{array}$$

Aufgabe 55 (homogene lineare Gleichungssysteme)**.** Es seien $m, n \in \mathbb{N}$, ein Körper K und ein $A \in K^{m\times n}$ gegeben. Unter einer *Lösung* wollen wir im Folgenden stets eine Lösung des homogenen linearen Gleichungssystems zur Koeffizientenmatrix A verstehen.
Zeigen oder widerlegen Sie:

(a) Wenn $m = n - 1$ ist, dann gibt es genau eine Lösung.

(b) Wenn $m > n$ ist, dann gibt es keine Lösung.

(c) Wenn $m = n$ ist, dann gibt es genau eine Lösung.

(d) Für $x, y \in K^{n\times 1}$ gilt: Wenn x und y Lösungen sind, dann ist auch $(x_i + y_i)_{i\in[1,n]}$ eine Lösung.

(e) Für $x \in K^{n\times 1}$ gilt: Wenn x eine Lösung ist, dann ist auch $(x_i + 1)_{i\in[1,n]}$ eine Lösung.

(f) Für $x, y \in K^{n\times 1}$ gilt: Wenn x und y Lösungen sind, dann ist auch $(x_i - y_i)_{i\in[1,n]}$ eine Lösung.

(g) Für $x \in K^{n\times 1}$ gilt: Wenn x eine Lösung ist, dann ist $(x_i - i)_{i\in[1,n]}$ keine Lösung.

(h) Für $a \in K$, $x \in K^{n\times 1}$ gilt: Wenn x eine Lösung ist, dann ist auch $(ax_i)_{i\in[1,n]}$ eine Lösung.

Aufgabe 56 (Datenerhebung)**.** In einer Umfrage wurden 10 Personen nach Haar- und Augenfarbe befragt. Auf die erste Frage antworteten 4 Personen „blond“ und 6 Personen „dunkel“. Auf die zweite Frage antworteten 8 Personen „braun“ und 2 Personen „blau“.
Ein Biologe möchte nun wissen, wie viele der Personen blonde Haare und blaue Augen (x_1), wie viele blonde Haare und braune Augen (x_2), wie viele dunkle Haare und blaue Augen (x_3) und wie viele dunkle Haare und braune Augen (x_4) haben.
Stellen Sie zur Ermittlung von x_1, x_2, x_3, x_4 ein lineares Gleichungssystem über $\mathbb{Q}$ mit vier Gleichungen in den vier Unbekannten auf und lösen Sie dieses. Finden Sie anschließend für den Biologen alle Möglichkeiten, wie die aufgeschlüsselten Umfrageergebnisse ausgesehen haben könnten.

2 Vektorräume

In diesem Abschnitt werden die zentralen Objekte der linearen Algebra, Vektorräume über Körpern sowie deren Homomorphismen, eingeführt.

Definition und Beispiele

(2.30) Definition (Vektorraum)**.** Es sei ein Körper K gegeben.

(a) Ein *Vektorraum über K* (oder *K-Vektorraum* oder *Vektorraum* oder *linearer Raum*) besteht aus einer abelschen Gruppe V zusammen mit einer Abbildung $s\colon K \times V \to V$ so, dass folgende Axiome gelten.

- *Assoziativität.* Für $a, b \in K$, $v \in V$ ist

$$s(a, s(b, v)) = s(ab, v).$$

- *Einselement.* Für $v \in V$ ist

$$s(1, v) = v.$$

- *Distributivität.* Für $a, b \in K$, $v \in V$ ist

$$s(a + b, v) = s(a, v) + s(b, v).$$

Für $a \in K$, $v, w \in V$ ist

$$s(a, v + w) = s(a, v) + s(a, w).$$

Unter Missbrauch der Notation bezeichnen wir sowohl den besagten K-Vektorraum als auch die unterliegende abelsche Gruppe mit V. Die Abbildung s wird *Skalarmultiplikation* von V genannt.

Für einen K-Vektorraum V mit Skalarmultiplikation s schreiben wir $\cdot = \cdot^V := s$ und $av = a \cdot v = a \cdot^V v := s(a, v)$ für $a \in K$, $v \in V$. Die Elemente von K werden *Skalare* von V genannt. Die Elemente von V werden auch *Vektoren* in V genannt. Das Nullelement von V wird auch *Nullvektor* in V genannt. Für einen Vektor v in V wird $-v$ auch der *negative Vektor* zu v genannt.

(b) Es seien K-Vektorräume V und W gegeben. Ein *Vektorraumhomomorphismus über K* (oder *K-Vektorraumhomomorphismus* oder *Homomorphismus von K-Vektorräumen* oder *K-Homomorphismus* oder *Homomorphismus* oder *K-lineare Abbildung* oder *lineare Abbildung*) von V nach W ist ein Homomorphismus abelscher Gruppen $\varphi\colon V \to W$ so, dass

$$\varphi(a \cdot^V v) = a \cdot^W \varphi(v)$$

für $a \in K$, $v \in V$ gilt.

Die *Menge aller K-Vektorraumhomomorphismen* von V nach W bezeichnen wir mit

$$\begin{aligned}\mathrm{Hom}(V,W) = \mathrm{Hom}_K(V,W) &= \mathrm{Hom}_{\mathbf{Vec}(K)}(V,W)\\ &:= \{\varphi \in \mathrm{Hom}_{\mathbf{AbGrp}}(V,W) \mid \varphi \text{ ist ein } K\text{-Vektorraumhomomorphismus}\}.\end{aligned}$$

(2.31) Konvention. In Vektorräumen lassen wir die Klammern um Produkte aus Skalaren und Vektoren meistens weg, d.h. es gelte *Punkt- vor Strichrechnung*.

Der Vollständigkeit halber wollen wir alle Axiome eines Vektorraums V über einem Körper K noch in Standardnotation auflisten:

- *Assoziativität der Addition.* Für $v, w, x \in V$ ist $v + (w + x) = (v + w) + x$.
- *Existenz des Nullvektors.* Es existiert ein $n \in V$ mit $n + v = v + n = v$ für alle $v \in V$. Dieses n ist nach Korollar (1.28) eindeutig bestimmt und wird mit $0 = 0^V$ bezeichnet. Wir haben also $0 + v = v + 0 = v$ für alle $v \in V$.
- *Existenz der negativen Vektoren.* Für jedes $v \in V$ existiert ein $w \in V$ mit $w + v = v + w = 0$. Dieses w ist nach Korollar (1.33) eindeutig bestimmt und wird mit $-v = (-v)^V$ bezeichnet. Wir haben also $(-v) + v = v + (-v) = 0$.
- *Kommutativität der Addition.* Für $v, w \in V$ ist $v + w = w + v$.
- *Assoziativität der Skalarmultiplikation.* Für $a, b \in K$, $v \in V$ ist $a(bv) = (ab)v$.
- *Einselement der Skalarmultiplikation.* Für $v \in V$ ist $1v = v$.
- *Distributivität.* Für $a, b \in K$, $v \in V$ ist $(a + b)v = av + bv$. Für $a \in K$, $v, w \in V$ ist $a(v + w) = av + aw$.

Wir verwenden außerdem die Notation und die Terminologie aus Definition (1.51). Ferner betonen wir, dass natürlich alle Aussagen über abelsche Gruppen für die einem Vektorraum unterliegende abelsche Gruppe gültig bleiben.

(2.32) Konvention. Es seien ein Körper K und ein K-Vektorraum V gegeben. Da für $a, b \in K$, $v \in V$ stets $(ab)v = a(bv)$ gilt, schreiben wir im Folgenden meist kurz $abv := (ab)v = a(bv)$.

Die Axiome eines Vektorraumhomomorphismus $\varphi\colon V \to W$ über einem Körper K in Standardnotation lesen sich wie folgt:

- *Verträglichkeit mit den Additionen.* Für $v, v' \in V$ ist $\varphi(v + v') = \varphi(v) + \varphi(v')$.
- *Verträglichkeit der Nullvektoren.* Es ist $\varphi(0) = 0$.
- *Verträglichkeit der negativen Vektoren.* Für $v \in V$ ist $\varphi(-v) = -\varphi(v)$.
- *Verträglichkeit mit den Skalarmultiplikationen.* Für $a \in K$, $v \in V$ ist $\varphi(av) = a\,\varphi(v)$.

Wir werden in Bemerkung (2.36) ein vergleichsweise knappes Kriterium für Vektorraumhomomorphismen sehen. Zur Erinnerung: Eine Familie in einem Körper K über einer Menge I ist ein $x \subseteq I \times X$ so, dass es für jedes $i \in I$ genau ein $y \in X$ mit $(i, y) \in X$ gibt. Ist nun $I = \emptyset$, so ist auch $I \times X = \emptyset$. Die einzige Teilmenge von $\emptyset$ ist $\emptyset$, und diese erfüllt die definierende Eigenschaft einer Familie. Somit besteht $K^0 = K^{[1,0]} = K^\emptyset$ aus genau einem Element, der *leeren Familie*, welche mengentheoretisch nichts anderes ist als die leere Menge.

(2.33) Beispiel. Es sei ein Körper K gegeben.

(a) (i) Die unterliegende abelsche Gruppe von K wird ein K-Vektorraum mit Skalarmultiplikation gegeben durch die Multiplikation des Körpers K.

(ii) Jede einelementige Menge wird ein K-Vektorraum (mit der einzig möglichen Addition und der einzig möglichen Skalarmultiplikation).

(iii) Für jede Menge I wird K^I ein K-Vektorraum mit Addition gegeben durch

$$x +^{K^I} y = (x_i +^K y_i)_{i \in I}$$

für $x, y \in K^I$, und Skalarmultiplikation gegeben durch

$$a \cdot^{K^I} x = (a \cdot^K x_i)_{i \in I}$$

für $a \in K$, $x \in K^I$. Der Nullvektor von K^I ist gegeben durch

$$0^{K^I} = (0^K)_{i \in I}.$$

Für $x \in K^I$ ist

$$(-x)^{K^I} = ((-x_i)^K)_{i \in I}.$$

(iv) Für $n \in \mathbb{N}_0$ wird K^n ein K-Vektorraum mit Addition gegeben durch

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$

für $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in K^n$, und Skalarmultiplikation gegeben durch

$$a(x_1, \ldots, x_n) = (ax_1, \ldots, ax_n)$$

für $a \in K$, $(x_1, \ldots, x_n) \in K^n$. Der Nullvektor von K^n ist gegeben durch

$$0 = (0, \ldots, 0).$$

Für $(x_1, \ldots, x_n) \in K^n$ ist

$$-(x_1, \ldots, x_n) = (-x_1, \ldots, -x_n).$$

(v) Für $m, n \in \mathbb{N}_0$ wird $K^{m \times n}$ ein K-Vektorraum mit Addition gegeben durch

$$A + B = (A_{i,j} + B_{i,j})_{i \in [1,m], j \in [1,n]}$$

für $A, B \in K^{m \times n}$, und Skalarmultiplikation gegeben durch

$$aA = (aA_{i,j})_{i \in [1,m], j \in [1,n]}$$

für $a \in K$, $A \in K^{m \times n}$. Der Nullvektor von $K^{m \times n}$ ist gegeben durch

$$0 = (0)_{i \in [1,m], j \in [1,n]}.$$

Für $A \in K^{m \times n}$ ist

$$-A = (-A_{i,j})_{i \in [1,m], j \in [1,n]}.$$

(vi) Für jede Menge X wird $\mathrm{Map}(X, K)$ ein K-Vektorraum mit Addition gegeben durch

$$(f + g)(x) = f(x) + g(x)$$

für $x \in X$, $f, g \in \mathrm{Map}(X, K)$, und Skalarmultiplikation gegeben durch

$$(af)(x) = af(x)$$

für $x \in X$, $a \in K$, $f \in \mathrm{Map}(X, K)$. Die Null von $\mathrm{Map}(X, K)$ ist gegeben durch

$$0(x) = 0$$

für $x \in X$. Für $f \in \mathrm{Map}(X, K)$ ist

$$(-f)(x) = -f(x)$$

für $x \in X$.

(b) (i) Die Abbildung

$$\varphi\colon K^3 \to K^2,\ (x_1, x_2, x_3) \mapsto (x_3, x_1)$$

ist ein K-Vektorraumhomomorphismus.

(ii) Es sei eine Menge I gegeben. Für alle $i \in I$ ist

$$\pi_i\colon K^I \to K,\ x \mapsto x_i$$

ein K-Vektorraumhomomorphismus.

(iii) Es sei eine Menge I gegeben. Für alle $i \in I$ ist

$$\varepsilon_i\colon K \to K^I,\ a \mapsto (\delta_{i,j}a)_{j\in I}$$

ein K-Vektorraumhomomorphismus.

Beweis.

(a) (i) Die Axiome eines Körpers entsprechen gerade den Axiomen eines K-Vektorraums.

(ii) Die Axiome eines K-Vektorraums sind aus Mangel an Möglichkeiten für die Werte der Addition und der Skalarmultiplikation erfüllt; Details seien dem Leser überlassen.

(iii) Siehe Aufgabe 57(a).

(iv) Dies folgt aus (iii), denn für $n \in \mathbb{N}_0$ ist $K^n = K^{[1,n]}$.

(v) Dies folgt aus (iii), denn für $m, n \in \mathbb{N}_0$ ist $K^{m\times n} = K^{[1,m]\times[1,n]}$.

(vi) Dies ist im Wesentlichen nur eine Umformulierung von (iii): Für jede Menge X liefert jedes Element $f \in \mathrm{Map}(X, K)$, also jede Abbildung $f\colon X \to K$, eine Familie f in K über X via $f_i = f(i)$, also ein Element $f \in K^X$; und umgekehrt.

(b) (i) Für $x, y \in K^3$ gilt

$$\begin{aligned}\varphi(x + y) &= \varphi(x_1 + y_1, x_2 + y_2, x_3 + y_3) = (x_3 + y_3, x_1 + y_1) = (x_3, x_1) + (y_3, y_1)\\ &= \varphi(x) + \varphi(y),\end{aligned}$$

nach Lemma (1.67) ist φ also ein Homomorphismus abelscher Gruppen. Ferner haben wir

$$\varphi(ax) = \varphi(ax_1, ax_2, ax_3) = (ax_3, ax_1) = a(x_3, x_1) = a\,\varphi(x)$$

für $a \in K$, $x \in K^3$, d.h. φ ist auch verträglich mit den Skalarmultiplikationen. Insgesamt ist φ somit ein K-Vektorraumhomomorphismus.

(ii) Siehe Aufgabe 57(b).

(iii) Siehe Aufgabe 57(c). □

Es ist auch nützlich, sich einige Gegenbeispiele zu Vektorraumhomomorphismen klarzumachen:

(2.34) Beispiel.

(a) Die Abbildung

$$\varphi\colon \mathbb{R}^2 \to \mathbb{R}^2,\ (x_1, x_2) \mapsto (x_1, x_2 + 1)$$

ist kein $\mathbb{R}$-Vektorraumhomomorphismus.

(b) Die Abbildung

$$\varphi\colon \mathbb{Q} \to \mathbb{Q}^2,\ x \mapsto (x^2, x^3)$$

ist kein $\mathbb{Q}$-Vektorraumhomomorphismus.

Beweis.

(a) Es ist

$$\varphi(0^{\mathbb{R}^2}) = \varphi(0,0) = (0,0+1) = (0,1) \neq 0^{\mathbb{R}^2}.$$

Somit ist φ kein Homomorphismus von abelschen Gruppen, also auch kein Homomorphismus von $\mathbb{R}$-Vektorräumen.

(b) Es ist $\varphi(1) = (1^2, 1^3) = (1,1)$ und $\varphi(2) = (2^2, 2^3) = (4,8)$, also

$$\varphi(1+1) = \varphi(2) = (4,8) \neq (1,1) + (1,1) = \varphi(1) + \varphi(1).$$

Somit ist φ kein Homomorphismus von abelschen Gruppen und damit insbesondere kein Homomorphismus von $\mathbb{Q}$-Vektorräumen. □

Ein Beispiel für einen Homomorphismus von abelschen Gruppen zwischen Vektorräumen, welcher kein Vektorraumhomomorphismus ist, werden wir in Aufgabe 60(e) kennenlernen.
Schließlich deuten wir noch ein Beispiel aus der Analysis an.

(2.35) Beispiel. Es werden

$$\mathrm{C}(\mathbb{R},\mathbb{R}) = \{f \in \mathrm{Map}(\mathbb{R},\mathbb{R}) \mid f \text{ stetig}\},$$
$$\mathrm{C}^1(\mathbb{R},\mathbb{R}) = \{f \in \mathrm{Map}(\mathbb{R},\mathbb{R}) \mid f \text{ stetig differenzierbar}\}$$

Vektorräume über $\mathbb{R}$ bzgl. der von $\mathrm{Map}(\mathbb{R},\mathbb{R})$ eingeschränkten Addition und Skalarmultiplikation. Bzgl. diesen Strukturen wird der Differentialoperator

$$\mathrm{D}\colon \mathrm{C}^1(\mathbb{R},\mathbb{R}) \to \mathrm{C}(\mathbb{R}),\ f \mapsto f'$$

ein $\mathbb{R}$-Vektorraumhomomorphismus.

Ohne Beweis. □

Im Beweis von Beispiel (2.33)(b) haben wir bereits gesehen, dass wir uns dank Lemma (1.67) einige Arbeit beim Nachweis der Axiome für einen Vektorraumhomomorphismus sparen können. Wir wollen dies noch kurz allgemein festhalten:

(2.36) Bemerkung. Es seien ein Körper K, Vektorräume V und W über K sowie eine Abbildung $\varphi\colon V \to W$ gegeben. Die folgenden Bedingungen sind äquivalent.

(a) Es ist φ ein K-Vektorraumhomomorphismus.

(b) Es gilt:

- *Verträglichkeit mit den Additionen.* Für $v, v' \in V$ ist $\varphi(v+v') = \varphi(v) + \varphi(v')$.
- *Verträglichkeit mit den Skalarmultiplikationen.* Für $a \in K$, $v \in V$ ist $\varphi(av) = a\,\varphi(v)$.

(c) Für $a \in K$, $v, v' \in V$ ist

$$\varphi(av + v') = a\,\varphi(v) + \varphi(v').$$

Beweis. Wenn Bedingung (a) gilt, so insbesondere auch Bedingung (b).
Es gelte Bedingung (b), d.h. es gelte $\varphi(v+v') = \varphi(v) + \varphi(v')$ für $v, v' \in V$ sowie $\varphi(av) = a\,\varphi(v)$ für $a \in K$, $v \in V$. Wir erhalten

$$\varphi(av + v') = \varphi(av) + \varphi(v') = a\,\varphi(v) + \varphi(v')$$

für $a \in K$, $v, v' \in V$, d.h. Bedingung (c) ist erfüllt.
Schließlich gelte Bedingung (c), d.h. es gelte $\varphi(av + v') = a\,\varphi(v) + \varphi(v')$ für $a \in K$, $v, v' \in V$. Dann haben wir

$$\varphi(v + v') = \varphi(1v + v') = 1\,\varphi(v) + \varphi(v') = \varphi(v) + \varphi(v')$$

für $v, v' \in V$. Nach Lemma (1.67) ist φ ein Homomorphismus abelscher Gruppen. Insbesondere gilt $\varphi(0) = 0$ und damit

$$\varphi(av) = \varphi(av + 0) = a\,\varphi(v) + \varphi(0) = a\,\varphi(v)$$

für $a \in K$, $v \in V$. Folglich ist φ ein K-Vektorraumhomomorphismus, d.h. Bedingung (a) gilt.
Insgesamt sind Bedingung (a), Bedingung (b) und Bedingung (c) äquivalent. □

Komposition von Vektorraumhomomorphismen

Gewisse Paare von Abbildungen können komponiert werden, gewisse Abbildungen können invertiert werden. Wir wollen nun Komposition und Inversion von Vektorraumhomomorphismen studieren.

(2.37) Bemerkung. Es sei ein Körper K gegeben.

(a) Für alle K-Vektorraumhomomorphismen $\varphi\colon V \to W$ und $\psi\colon W \to X$ ist $\psi \circ \varphi\colon V \to X$ ein K-Vektorraumhomomorphismus.

(b) Für jeden K-Vektorraum V ist $\mathrm{id}_V\colon V \to V$ ein K-Vektorraumhomomorphismus.

Beweis.

(a) Es seien K-Vektorraumhomomorphismen $\varphi\colon V \to W$ und $\psi\colon W \to X$ gegeben. Nach Bemerkung (2.36) gilt dann

$$(\psi \circ \varphi)(v + v') = \psi(\varphi(v + v')) = \psi(\varphi(v) + \varphi(v')) = \psi(\varphi(v)) + \psi(\varphi(v')) = (\psi \circ \varphi)(v) + (\psi \circ \varphi)(v')$$

für $v, v' \in V$ und

$$(\psi \circ \varphi)(av) = \psi(\varphi(av)) = \psi(a\,\varphi(v)) = a\,\psi(\varphi(v)) = a\,(\psi \circ \varphi)(v)$$

für $a \in K$, $v \in V$. Folglich ist auch $\psi \circ \varphi\colon V \to X$ ein K-Vektorraumhomomorphismus nach Bemerkung (2.36).

(b) Es sei ein K-Vektorraum V gegeben. Für $a \in K$, $v, v' \in V$ gilt

$$\mathrm{id}_V(av + v') = av + v' = a\,\mathrm{id}_V(v) + \mathrm{id}_V(v'),$$

d.h. $\mathrm{id}_V\colon V \to V$ ist ein K-Vektorraumhomomorphismus nach Bemerkung (2.36). □

(2.38) Definition (Vektorraumisomorphismus)**.** Es seien ein Körper K und K-Vektorräume V und W gegeben.

(a) Ein *Vektorraumisomorphismus über K* (oder *K-Vektorraumisomorphismus* oder *Isomorphismus von K-Vektorräumen* oder *K-Isomorphismus* oder *Isomorphismus*) von V nach W ist ein K-Vektorraumhomomorphismus $\varphi\colon V \to W$ so, dass φ eine invertierbare Abbildung und $\varphi^{-1}\colon W \to V$ ein K-Vektorraumhomomorphismus ist.

(b) Wir sagen, dass V *isomorph* zu W (*als K-Vektorräume*) ist, geschrieben $V \cong W$, falls ein K-Vektorraumisomorphismus von V nach W existiert.

(2.39) Beispiel. Es sei ein Körper K gegeben. Die Abbildung

$$K^2 \to K^{2\times 1},\ (x_1, x_2) \mapsto \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

ist ein K-Vektorraumisomorphismus.

Die folgende Bemerkung besagt, dass die Forderung der Linearität von φ^{-1} in Definition (2.38)(a) redundant ist.

(2.40) Bemerkung. Es seien ein Körper K und ein K-Vektorraumhomomorphismus $\varphi\colon V \to W$ gegeben. Die folgenden Bedingungen sind äquivalent.

(a) Es ist φ ein K-Vektorraumisomorphismus.

(b) Es ist φ eine invertierbare Abbildung.

(c) Es ist φ bijektiv.

Beweis. Die Äquivalenz von Bedingung (b) und Bedingung (c) ist bekannt. Ferner ist jeder Isomorphismus insbesondere eine invertierbare Abbildung, d.h. Bedingung (a) impliziert Bedingung (b). Um zu zeigen, dass die drei Bedingungen äquivalent sind, genügt es zu zeigen, dass Bedingung (b) Bedingung (a) impliziert.
Es gelte also Bedingung (b), d.h. es sei φ eine invertierbare Abbildung. Da φ ein Homomorphismus ist, haben wir

$$\varphi^{-1}(aw + w') = \varphi^{-1}(a\,\varphi(\varphi^{-1}(w)) + \varphi(\varphi^{-1}(w'))) = \varphi^{-1}(\varphi(a\,\varphi^{-1}(w) + \varphi^{-1}(w'))) = a\,\varphi^{-1}(w) + \varphi^{-1}(w')$$

für $a \in K$, $w, w' \in W$ nach Bemerkung (2.36). Also ist φ^{-1} ein Homomorphismus nach Bemerkung (2.36) und damit φ ein Isomorphismus, d.h. es gilt Bedingung (a).
Insgesamt sind Bedingung (a), Bedingung (b) und Bedingung (c) äquivalent. □

Elementare Eigenschaften

Schließlich leiten wir noch einige elementare Eigenschaften für Vektorräume her. Die Distributivgesetze lassen sich auch noch wie folgt lesen:

(2.41) Bemerkung. Es seien ein Körper K und ein K-Vektorraum V gegeben.

(a) Für $a \in K$ ist

$$\lambda_a \colon V \to V,\ v \mapsto av$$

ein Homomorphismus abelscher Gruppen.

(b) Für $v \in V$ ist

$$\rho_v \colon K \to V,\ a \mapsto av$$

ein Homomorphismus abelscher Gruppen.

Beweis.

(a) Es sei $a \in K$ gegeben. Da für $v, w \in V$ stets

$$\lambda_a(v+w) = a(v+w) = av + aw = \lambda_a(v) + \lambda_a(w)$$

gilt, ist λ_a nach Lemma (1.67) ein Homomorphismus abelscher Gruppen.

(b) Es sei $v \in V$ gegeben. Da für $a, b \in K$ stets

$$\rho_v(a+b) = (a+b)v = av + bv = \rho_v(a) + \rho_v(b)$$

gilt, ist ρ_v nach Lemma (1.67) ein Homomorphismus abelscher Gruppen. □

(2.42) Korollar. Es seien ein Körper K und ein K-Vektorraum V gegeben.

(a) Für $v \in V$ gilt $0v = 0$.

(b) Für $a \in K$ gilt $a0 = 0$.

(c) Für $a \in K$, $v \in V$ gilt $(-a)v = a(-v) = -(av)$.

(d) Für $v \in V$ gilt $(-1)v = -v$.

(e) Für $a \in K$, $v \in V$ gilt $(-a)(-v) = av$.

Beweis.

(a) Für $v \in V$ ist $\rho_v \colon K \to V,\ a \mapsto av$ ein Homomorphismus abelscher Gruppen nach Bemerkung (2.41)(b), es gilt also

$$0v = \rho_v(0) = 0.$$

(b) Für $a \in K$ ist $\lambda_a \colon V \to V,\ v \mapsto av$ ein Homomorphismus abelscher Gruppen nach Bemerkung (2.41)(a), es gilt also

$$a0 = \lambda_a(0) = 0.$$

(c) Für $v \in V$ ist $\rho_v \colon K \to V,\ a \mapsto av$ ein Homomorphismus abelscher Gruppen nach Bemerkung (2.41)(b), es gilt also

$$(-a)v = \rho_v(-a) = -\rho_v(a) = -(av)$$

für alle $v \in V$. Ferner ist für $a \in K$ stets $\lambda_a \colon V \to V,\ v \mapsto av$ ein Homomorphismus abelscher Gruppen nach Bemerkung (2.41)(a), es gilt also auch

$$a(-v) = \lambda_a(-v) = -\lambda_a(v) = -(av)$$

für alle $a \in K$.

(d) Für $v \in V$ ist

$$(-1)v = -(1v) = -v$$

nach (c).

(e) Für $a \in K$, $v \in V$ ist

$$(-a)(-v) = -((-a)v) = -(-(av)) = av$$

nach (d) und Proposition (1.47)(c). □

(2.43) Bemerkung. Es seien ein Körper K, ein K-Vektorraum V und $a \in K^\times$, $v, w \in V$ gegeben.

(a) Genau dann gilt $av = w$, wenn $v = a^{-1}w$ ist.

(b) Genau dann gilt $av = aw$, wenn $v = w$ ist.

Beweis.

(a) Wenn $av = w$ gilt, dann auch

$$v = 1v = a^{-1}av = a^{-1}w.$$

Umgekehrt, wenn $v = a^{-1}w$ ist, dann haben wir auch

$$av = aa^{-1}w = 1w = w.$$

(b) Wenn $v = w$ ist, dann auch $av = aw$. Es gelte umgekehrt $av = aw$. Nach (a) ist dann

$$v = a^{-1}aw = 1w = w.$$ □

(2.44) Lemma. Es seien ein Körper K, ein K-Vektorraum V sowie $a \in K$, $v \in V$ gegeben. Wenn $av = 0$ gilt, dann ist $a = 0$ oder $v = 0$.

Beweis. Es gelte $av = 0$ und es sei $a \neq 0$. Dann ist $a \in K^\times$, nach Bemerkung (2.43)(a) und Korollar (2.42)(b) gilt also $v = a^{-1}0 = 0$. □

(2.45) Korollar. Es seien ein Körper K, ein K-Vektorraum V sowie $a, b \in K$, $v \in V \setminus \{0\}$ gegeben. Genau dann gilt $av = bv$, wenn $a = b$ ist.

Beweis. Wenn $a = b$ ist, dann auch $av = bv$. Es gelte umgekehrt $av = bv$, so dass $(a - b)v = av - bv = 0$. Da $v \neq 0$ ist, folgt $a - b = 0$ nach Lemma (2.44), also $a = b$. □

Es seien ein Körper K und ein K-Vektorraum V gegeben. In Notation (1.61)(b) haben wir für $v \in V$ die Schreibweise $0v = 0^V$, $1v = v$, $2v = v + v$, $3v = v + v + v$, etc. festgelegt. Ist nun etwa $K = \mathbb{Q}$ oder $K = \mathbb{R}$, so stellt sich die Frage, ob diese Festlegung für diejenigen $a \in K$, welche in $\mathbb{Z}$ liegen, mit der Skalarmultiplikation des K-Vektorraums übereinstimmt.
Wir haben für $k \in \mathbb{Z}$ in Notation (1.105) sogar $k^K = k1^K$ festgelegt (diese Notation ist mit der Notation 0^K für die Null bzw. 1^K für die Eins von K konform). Die folgende Bemerkung zeigt nun, dass die Skalarmultiplikation von k^K mit einem $v \in V$ gleich kv im Sinne von Notation (1.61)(b) ist.

(2.46) Bemerkung. Es seien ein Körper K und ein K-Vektorraum V gegeben. Für $k \in \mathbb{Z}$, $v \in V$ ist

$$k^K \cdot^V v = kv.$$

Beweis. Der Deutlichkeit wegen schreiben wir in diesem Beweis die Multiplikation in K stets als $\cdot^K$, die Skalarmultiplikation von V als $\cdot^V$ und die „Multiplikation“ nach Notation (1.61)(b) ohne Symbol. Ferner schreiben wir für $k \in \mathbb{Z}$ stets $k^{\mathbb{Z}}$ für das Element in $\mathbb{Z}$ und $k^K = k1^K = k^{\mathbb{Z}}1^K$ für das Element in K nach Notation (1.105). Es seien zunächst $k \in \mathbb{Z}$ mit $k \geq 0$ und $v \in V$ gegeben. Wir führen vollständige Induktion nach k. Für $k = 0$ haben wir

$$k^K \cdot^V v = 0^K \cdot^V v = 0^V = 0^{\mathbb{Z}}v = k^{\mathbb{Z}}v$$

nach Korollar (2.42)(a). Es sei also $k > 0$ und gelte $(k-1)^K v = (k-1)^{\mathbb{Z}} v$. Unter Verwendung von Bemerkung (1.106) haben wir dann aber auch

$$k^K \cdot^V v = ((k-1)^K +^K 1^K) \cdot^V v = (k-1)^K \cdot^V v +^V 1^K \cdot^V v = (k-1)^{\mathbb{Z}} v +^V v = k^{\mathbb{Z}} v.$$

Nach dem Induktionsprinzip gilt also $k^K \cdot^V v = k^{\mathbb{Z}} v$ für $k \in \mathbb{Z}$ mit $k \geq 0$ und $v \in V$.
Für $k \in \mathbb{Z}$ mit $k < 0$ und $v \in V$ haben wir jedoch ebenfalls

$$\begin{aligned} k^K \cdot^V v &= (-|k|^K)^K \cdot^V v = (|k|^K \cdot^K (-1)^K) \cdot^V v = |k|^K \cdot^V ((-1)^K \cdot^V v) = |k|^K \cdot^V (-v)^V = |k|^{\mathbb{Z}} (-v)^V \\ &= (-|k|)^{\mathbb{Z}} v = k^{\mathbb{Z}} v \end{aligned}$$

nach Bemerkung (1.106) und Korollar (2.42)(d).
Insgesamt gilt somit $k^K \cdot^V v = k^{\mathbb{Z}} v$ für alle $k \in \mathbb{Z}$, $v \in V$. □

Aufgaben

Aufgabe 57 (Standardbeispiel eines Vektorraums)**.** Es seien ein Körper K und eine Menge I gegeben. Zeigen Sie:

(a) Es wird K^I ein K-Vektorraum mit Addition gegeben durch

$$x + y = (x_i + y_i)_{i \in I}$$

für $x, y \in K^I$, und Skalarmultiplikation gegeben durch

$$ax = (ax_i)_{i \in I}$$

für $a \in K$, $x \in K^I$.

(b) Für alle $i \in I$ ist

$$\pi_i \colon K^I \to K,\ x \mapsto x_i$$

ein K-Vektorraumhomomorphismus.

(c) Für alle $i \in I$ ist

$$\varepsilon_i \colon K \to K^I,\ x \mapsto (\delta_{i,j} x)_{j \in I}$$

ein K-Vektorraumhomomorphismus.

(d) Für jede Teilmenge J von I ist

$$K^I \to K^J,\ x \mapsto x|_J = (x_j)_{j \in J}$$

ein K-Vektorraumhomomorphismus.

Aufgabe 58 (Vektorräume über $\mathbb{R}$ und $\mathbb{Q}$)**.** Zeigen Sie: Jeder $\mathbb{R}$-Vektorraum trägt die Struktur eines $\mathbb{Q}$-Vektorraums (bzgl. geeignet definierter Addition und Skalarmultiplikation).

Aufgabe 59 (Produkt)**.** Es seien ein Körper K und eine Familie $(V_i)_{i \in I}$ bestehend aus K-Vektorräumen V_i für $i \in I$ gegeben. Zeigen Sie:

(a) Das kartesische Produkt $\times_{i \in I} V_i$ wird ein K-Vektorraum mit Addition gegeben durch

$$v + w = (v_i + w_i)_{i \in I}$$

für $v, w \in \times_{i \in I} V_i$, und Skalarmultiplikation gegeben durch

$$av = (av_i)_{i \in I}$$

für $a \in K$, $v \in \times_{i \in I} V_i$.

(b) Für alle $i \in I$ wird

$$\mathrm{pr}_i \colon \bigtimes_{j \in I} V_j \to V_i,\ v \mapsto v_i$$

bzgl. der Struktur aus (a) ein K-Vektorraumhomomorphismus.

Aufgabe 60 (komplexe Zahlen)**.** Der Körper $\mathbb{C}$ mit unterliegender Menge $\mathbb{R}\times\mathbb{R}$ und Addition und Multiplikation gegeben durch

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2),$$
$$(x_1, x_2)(y_1, y_2) = (x_1 y_1 - x_2 y_2, x_1 y_2 + x_2 y_1).$$

heißt *Körper der komplexen Zahlen*, vgl. Aufgabe 40(b). Das Element $\mathrm{i} := (0, 1) \in \mathbb{C}$ wird *imaginäre Einheit* genannt.

(a) Zeigen Sie, dass es für alle $z \in \mathbb{C}$ eindeutige $x, y \in \mathbb{R}$ mit $z = 1^{\mathbb{C}} x + \mathrm{i}y$ gibt.

Es seien $z \in \mathbb{C}$, $x, y \in \mathbb{R}$ mit $z = 1^{\mathbb{C}} x + \mathrm{i}y$ gegeben. Wir nennen x den *Realteil* von z und y den *Imaginärteil* von z, und wir schreiben $\mathrm{Re}\, z := x$ sowie $\mathrm{Im}\, z := y$.

(b) Beschreiben Sie Addition, Multiplikation und Skalarmultiplikation (mit Elementen aus $\mathbb{R}$) mittels der Darstellung aus (a).

(c) Zeigen Sie, dass Skalarmultiplikation und Multiplikation im Körper $\mathbb{C}$ verträglich sind: Für alle $a \in \mathbb{R}$, $z, w \in \mathbb{C}$ gilt

$$(az)w = z(aw) = a(zw).$$

(d) Zeigen Sie, dass die Abbildung

$$\iota \colon \mathbb{R} \to \mathbb{C},\ x \mapsto 1^{\mathbb{C}} x$$

injektiv, ein $\mathbb{R}$-Vektorraumhomomorphismus und ein Ringhomomorphismus ist.

Nach (d) macht es also keinen Unterschied, ob wir in $\mathbb{R}$ selbst oder in $\mathrm{Im}\, \iota \subseteq \mathbb{C}$ bzgl. der von $\mathbb{C}$ eingeschränkten Verknüpfungen rechnen. Daher werden wir in Zukunft $\mathbb{R}$ mit $\mathrm{Im}\, \iota$ identifizieren, d.h. wir schreiben, unter Missbrauch der Notation, $\mathbb{R}$ anstatt $\mathrm{Im}\, \iota$ und, für gegebenes $x \in \mathbb{R}$, schreiben wir x anstelle von $\iota(x) = 1^{\mathbb{C}} x \in \mathbb{C}$. Insbesondere schreiben wir also auch $1^{\mathbb{R}}$ anstelle von $\iota(1^{\mathbb{R}}) = 1^{\mathbb{C}}$, wir haben also $z = \mathrm{Re}\, z + \mathrm{i}\,(\mathrm{Im}\, z)$.
Für $z \in \mathbb{C}$ heißt $\overline{z} := \mathrm{Re}\, z - \mathrm{i}\,(\mathrm{Im}\, z)$ das *komplex Konjugierte* zu z. Die Abbildung $\mathbb{C} \to \mathbb{C}$, $z \mapsto \overline{z}$ wird *komplexe Konjugation* genannt.

(e) Zeigen Sie, dass die komplexe Konjugation ein $\mathbb{R}$-Vektorraumhomomorphismus und ein Ringhomomorphismus, aber kein $\mathbb{C}$-Vektorraumhomomorphismus ist.

Aufgabe 61 (Beispiele und Gegenbeispiele für Homomorphismen)**.** Untersuchen Sie, ob die folgenden Abbildungen linear über den angegebenen Körpern sind.

(a) Die Abbildung $\mathbb{R}^3 \to \mathbb{R}^2$, $(x_1, x_2, x_3) \mapsto (x_1, x_1 + x_3)$, über $\mathbb{R}$.

(b) Die Abbildung $\mathbb{C}^4 \to \mathbb{C}^3$, $(z_1, z_2, z_3, z_4) \mapsto (2z_2 + \mathrm{i}z_4, -z_1, (3 - 2\mathrm{i})z_3 + z_4)$, über $\mathbb{C}$.

(c) Die Abbildung $\mathbb{Q}^2 \to \mathbb{Q}^3$, $(x_1, x_2) \mapsto (x_1 + x_2, 1, x_1)$, über $\mathbb{Q}$.

(d) Die Abbildung $\mathbb{R} \to \mathbb{R}^1$, $x \mapsto (x\sqrt{2})$, über $\mathbb{R}$.

(e) Die Abbildung $\mathbb{C}^3 \to \mathbb{C}^2$, $(z_1, z_2, z_3) \mapsto (z_1, z_1 + z_3)$, über $\mathbb{C}$.

(f) Die Abbildung $\mathbb{C}^4 \to \mathbb{C}^2$, $(z_1, z_2, z_3) \mapsto (2z_2 + \mathrm{i}z_4, 2z_2 + (3 - 2\mathrm{i})z_3 + (1 + \mathrm{i})z_4)$, über $\mathbb{C}$.

(g) Die Abbildung $\mathbb{F}_2^2 \to \mathbb{F}_2^2$, $(x_1, x_2) \mapsto (x_1^2, x_1 + x_2)$, über $\mathbb{F}_2$.

(h) Die Abbildung $\mathbb{R}^2 \to \mathbb{R}$, $(x_1, x_2) \mapsto x_1 x_2$, über $\mathbb{Q}$.

(i) Die Abbildung $\mathbb{F}_5 \to \mathbb{F}_5^2$, $x \mapsto (-5x, 10x)$, über $\mathbb{F}_5$.

Aufgabe 62 (Potenzmenge als $\mathbb{F}_2$-Vektorraum)**.** Es sei $n \in \mathbb{N}$. Zeigen Sie:

(a) Es wird $\mathrm{Pot}([1,n])$ ein $\mathbb{F}_2$-Vektorraum, mit Addition gegeben durch

$$U + V = \{i \in [1,n] \mid \text{entweder } i \in U \text{ oder } i \in V\}$$

für $U, V \in \mathrm{Pot}([1,n])$ und geeignet zu definierender Skalarmultiplikation.

(b) Es ist $\mathrm{Pot}([1,n]) \cong \mathbb{F}_2^n$.

3 Untervektorräume

In diesem und den folgenden Abschnitten wollen wir unter anderem der Frage nachgehen, wie man aus gegebenen Vektorräumen neue Vektorräume konstruieren kann. Zunächst betrachten wir den Fall von Untervektorräumen, welche in Analogie zu den abelschen Untergruppen definiert sind, vgl. Definition (1.69)(b).

Definition und Beispiele

(2.47) Definition (Untervektorraum)**.** Es seien ein Körper K und ein K-Vektorraum V gegeben. Ein *K-Untervektorraum* (oder *Untervektorraum* oder *linearer Unterraum* oder *linearer Teilraum*) von V ist ein K-Vektorraum U so, dass die unterliegende abelsche Gruppe von U eine abelsche Untergruppe von V ist und so, dass

$$a \cdot^U u = a \cdot^V u$$

für alle $a \in K$, $u \in U$ gilt.
Ein Untervektorraum U von V heißt *echt* (oder *strikt*), falls $U \neq V$ gilt.
Ist U ein Untervektorraum von V, so schreiben wir $U \leq V$. Ist U kein Untervektorraum von V, so schreiben wir $U \not\leq V$. Ist U ein echter Untervektorraum von V, so schreiben wir $U < V$.

(2.48) Bemerkung. Es sei ein Körper K gegeben. Für jeden K-Vektorraum V gilt $V \leq V$.

Bevor wir zu weiteren Beispielen kommen, leiten wir zunächst einige Resultate über Untervektorräume in Analogie zur Theorie der Untergruppen her, vgl. Kapitel I, Abschnitt 4. Dies wird uns die Beantwortung der Frage, ob wir in einer konkreten Situation einen Untervektorraum vorliegen haben oder nicht, erleichtern.

(2.49) Bemerkung. Es seien ein Körper K und K-Vektorräume V und U so gegeben, dass die unterliegende Menge von U eine Teilmenge von V ist. Genau dann ist U ein K-Untervektorraum von V, wenn die Inklusion $\mathrm{inc}\colon U \to V$ ein K-Vektorraumhomomorphismus ist.

(2.50) Korollar. Es seien ein Körper K und K-Vektorräume V und U so gegeben, dass die unterliegende Menge von U eine Teilmenge von V ist. Die folgenden Bedingungen sind äquivalent.

(a) Es ist U ein K-Untervektorraum von V.

(b) Es gilt

$$u +^U u' = u +^V u'$$

für alle $u, u' \in U$ und

$$a \cdot^U u = a \cdot^V u$$

für alle $a \in K$, $u \in U$.

(c) Es gilt

$$a \cdot^U u +^U u' = a \cdot^V u +^V u'$$

für alle $a \in K$, $u, u' \in U$.

Beweis. Dies folgt aus Bemerkung (2.49) und Bemerkung (2.36). □

Das Untervektorraumkriterium

Da die Struktur eines Untervektorraums durch die unterliegende Menge festgelegt ist, treffen wir folgende Vereinbarung in Analogie zu Konvention (1.73).

(2.51) Konvention. Es seien ein Körper K, ein K-Vektorraum V und eine Teilmenge U von V gegeben. Da die Addition und die Skalarmultiplikation jedes Untervektorraums von V vollständig durch die Addition und die Skalarmultiplikation von V bestimmt ist, gibt es höchstens eine Vektorraumstruktur auf U so, dass U mit dieser Vektorraumstruktur ein Untervektorraum von V wird. Wir sagen daher auch, dass U ein Untervektorraum von V *ist*, falls so eine Vektorraumstruktur auf U existiert.

Wir entwickeln ein Kriterium zum Nachweis von Untervektorräumen:

(2.52) Lemma (Untervektorraumkriterium)**.** Es seien ein Körper K, ein K-Vektorraum V und eine Teilmenge U von V gegeben. Die folgenden Bedingungen sind äquivalent.

(a) Es ist U ein K-Untervektorraum von V.

(b) Es gilt:

- Es ist U eine abelsche Untergruppe von V.
- *Abgeschlossenheit unter Skalarmultiplikation.* Für alle $a \in K$, $u \in U$ ist

  $$au \in U.$$

(c) Es gilt:

- *Abgeschlossenheit unter Addition.* Für alle $u, u' \in U$ ist

  $$u + u' \in U.$$

- *Abgeschlossenheit unter dem Nullvektor.* Es ist

  $$0 \in U.$$

- *Abgeschlossenheit unter Skalarmultiplikation.* Für alle $a \in K$, $u \in U$ ist

  $$au \in U.$$

(d) Es gilt:

- Es ist

  $$U \neq \emptyset.$$

- Für alle $a \in K$, $u, u' \in U$ ist

  $$au + u' \in U.$$

Beweis. Wir zeigen zuerst die Äquivalenz von Bedingung (a) und Bedingung (b), danach die Äquivalenz von Bedingung (b), Bedingung (c) und Bedingung (d).
Es gelte also zunächst Bedingung (a), d.h. es sei U ein Untervektorraum von V. Dann ist U insbesondere eine abelsche Untergruppe von V, und für $a \in K$, $u \in U$ ist $a \cdot^V u = a \cdot^U u \in U$. Folglich gilt Bedingung (b).
Nun gelte umgekehrt Bedingung (b). Da für $a \in K$, $u \in U$ auch $a \cdot^V u \in U$ ist, erhalten wir eine wohldefinierte Abbildung $s\colon K \times U \to U$, $(a, u) \mapsto a \cdot^V u$. Um zu zeigen, dass U ein K-Vektorraum mit Skalarmultiplikation s wird, verifizieren wir die Axiome aus Definition (2.30)(a):

- *Assoziativität.* Für $a, b \in K$, $u \in U$ ist

  $$s(a, s(b, u)) = a \cdot^V (b \cdot^V u) = (ab) \cdot^V u = s(ab, u).$$

- *Einselement.* Für $u \in U$ ist

$$s(1,u) = 1 \cdot^V u = u.$$

- *Distributivität.* Für $a,b \in K$, $u \in U$ ist

$$s(a+b,u) = (a+b) \cdot^V u = a \cdot^V u +^V b \cdot^V u = a \cdot^V u +^U b \cdot^V u = s(a,u) +^U s(b,u).$$

Für $a \in K$, $u,u' \in U$ ist

$$\begin{aligned} s(a, u +^U u') &= s(a, u +^V u') = a \cdot^V (u +^V u') = a \cdot^V u +^V a \cdot^V u' = a \cdot^V u +^U a \cdot^V u' \\ &= s(a,u) +^U s(a,u'). \end{aligned}$$

Somit wird U in der Tat ein K-Vektorraum mit $a \cdot^U u = s(a,u)$ für $a \in K$, $u \in U$. Nach Definition der Skalarmultiplikation von U ist dann U aber sogar ein Untervektorraum von V, d.h. es gilt Bedingung (a).
Wir haben also gezeigt, dass Bedingung (a) und Bedingung (b) äquivalent sind. Somit kommen wir zur Äquivalenz von Bedingung (b), Bedingung (c) und Bedingung (d).
Wenn Bedingung (b) gilt, dann auch Bedingung (c) nach dem Untergruppenkriterium (1.74).
Als nächstes gelte Bedingung (c). Da U abgeschlossen unter dem Nullelement ist, gilt $0^V \in U$, also insbesondere $U \neq \emptyset$. Sind $a \in K$, $u,u' \in U$ gegeben, so ist ferner $a \cdot^V u \in U$, da U abgeschlossen unter der Skalarmultiplikation ist, und folglich $a \cdot^V u +^V u' \in U$, da U abgeschlossen unter der Addition ist. Wir haben somit die Gültigkeit von Bedingung (d) gezeigt.
Schließlich gelte Bedingung (d). Für $u,u' \in U$ gilt dann $-u+u' = (-1) \cdot^V u +^V u' \in U$ nach Korollar (2.42)(d). Folglich ist U eine abelsche Untergruppe von V nach dem Untergruppenkriterium (1.74). Insbesondere ist $0^V \in U$ und damit $a \cdot^V u = a \cdot^V u +^V 0^V \in U$ für $a \in K$, $u \in U$. Somit gilt Bedingung (b).
Wir haben also auch die Äquivalenz von Bedingung (b), Bedingung (c) und Bedingung (d) gezeigt. Insgesamt sind Bedingung (a), Bedingung (b), Bedingung (c) und Bedingung (d) äquivalent. □

Wir kommen nun zu einigen Beispielen von Untervektorräumen.
Es seien ein Körper K und eine Menge I gegeben. Für $x \in K^I$ sagen wir, dass $x_i = 0$ *für fast alle* $i \in I$ gilt, falls $\{i \in I \mid x_i \neq 0\}$ endlich ist.

(2.53) Beispiel. Es sei ein Körper K gegeben. Für jede Menge I ist

$$K^{(I)} := \{x \in K^I \mid x_i = 0 \text{ für fast alle } i \in I\}$$

ein K-Untervektorraum von K^I.

Beweis. Siehe Aufgabe 65. □

(2.54) Beispiel.

(a) Es ist $\{(x,-x) \mid x \in \mathbb{R}\}$ ein $\mathbb{R}$-Untervektorraum von $\mathbb{R}^2$.

(b) Es ist $\{(1+x,-x) \mid x \in \mathbb{R}\}$ kein $\mathbb{R}$-Untervektorraum von $\mathbb{R}^2$.

Beweis.

(a) Es sei $U := \{(x,-x) \mid x \in \mathbb{R}\}$. Dann ist $0^{\mathbb{R}^2} = (0,0) = (0,-0) \in U$, also insbesondere $U \neq \emptyset$. Es seien $a \in \mathbb{R}$, $u,u' \in U$ gegeben. Dann gibt es $x,x' \in \mathbb{R}$ mit $u = (x,-x)$, $u' = (x',-x')$, es folgt also

$$au + u' = a(x,-x) + (x',-x') = (ax+x', a(-x)+(-x')) = (ax+x', -(ax+x')) \in U.$$

Nach dem Untervektorraumkriterium (2.52) ist U ein Untervektorraum von $\mathbb{R}^2$.

(b) Es sei $U := \{(1+x,-x) \mid x \in \mathbb{R}\}$. Für $x \in \mathbb{R}$ ist genau dann $1+x = 0$, wenn $-x = 1$ ist. Dies bedeutet, dass $0^{\mathbb{R}^2} = (0,0) \notin U$ ist. Nach dem Untervektorraumkriterium (2.52) ist U kein Untervektorraum von $\mathbb{R}^2$. □

(2.55) Beispiel. Es ist $\mathrm{C}(\mathbb{R},\mathbb{R})$ ein $\mathbb{R}$-Untervektorraum von $\mathrm{Map}(\mathbb{R},\mathbb{R})$ und es ist $\mathrm{C}^1(\mathbb{R},\mathbb{R})$ ein $\mathbb{R}$-Untervektorraum von $\mathrm{C}(\mathbb{R},\mathbb{R})$.

Ohne Beweis. □

Konstruktion von Untervektorräumen durch Homomorphismen

Um neue Vektorräume aus gegebenen Vektorräumen als Untervektorräume konstruieren zu können, ist es praktisch, möglichst einfache Kriterien hierfür zu haben. Wir werden daher im Folgenden einige Operationen auf Untervektorräumen studieren.

(2.56) Proposition. Es seien ein Körper K und ein K-Vektorraumhomomorphismus $\varphi\colon V \to W$ gegeben.

(a) Für jeden K-Untervektorraum U von V ist $\varphi(U)$ ein K-Untervektorraum von W.

(b) Für jeden K-Untervektorraum U von W ist $\varphi^{-1}(U)$ ein K-Untervektorraum von V.

Beweis.

(a) Es sei ein Untervektorraum U von V gegeben. Dann ist $U \neq \emptyset$ nach dem Untervektorraumkriterium (2.52), also ist auch $\varphi(U) \neq \emptyset$. Da φ ein K-Vektorraumhomomorphismus ist, gilt ferner $a\,\varphi(u) + \varphi(u') = \varphi(au + u') \in \varphi(U)$ für $a \in K$, $u, u' \in U$. Nach dem Untervektorraumkriterium (2.52) ist also $\varphi(U)$ ein Untervektorraum von W.

(b) Es sei ein Untervektorraum U von W gegeben. Dann ist $\varphi(0) = 0 \in U$ nach dem Untervektorraumkriterium (2.52), also auch $0 \in \varphi^{-1}(U)$. Für $v, v' \in \varphi^{-1}(U)$ ist $\varphi(v), \varphi(v') \in U$, also auch $\varphi(v + v') = \varphi(v) + \varphi(v') \in U$ nach dem Untervektorraumkriterium (2.52) und damit $v + v' \in \varphi^{-1}(U)$. Ferner gilt für $v \in \varphi^{-1}(U)$ stets $\varphi(v) \in U$, also auch $\varphi(av) = a\,\varphi(v) \in U$ nach dem Untervektorraumkriterium (2.52) und somit $av \in \varphi^{-1}(U)$ für $a \in K$. Insgesamt ist $\varphi^{-1}(U)$ nach dem Untervektorraumkriterium (2.52) ein Untervektorraum von V. □

(2.57) Korollar. Es seien ein Körper K und ein K-Vektorraumhomomorphismus $\varphi\colon V \to W$ gegeben. Dann ist $\operatorname{Im}\varphi$ ein K-Untervektorraum von W.

Beweis. Es ist $V \leq V$ und damit $\operatorname{Im}\varphi = \varphi(V) \leq W$ nach Proposition (2.56)(a). □

Die Tatsache, dass das Bild eines Vektorraumhomomorphismus ein Untervektorraum ist, lässt sich gut zum Nachweis der Eigenschaft, ein Untervektorraum zu sein, benutzen:

Alternativer Beweis zu Beispiel (2.54)(a). Wir betrachten die Abbildung $\varphi\colon \mathbb{R} \to \mathbb{R}^2$, $x \mapsto (x, -x)$. Da für $a \in \mathbb{R}$, $x, x' \in \mathbb{R}$ stets

$$\varphi(ax + x') = (ax + x', -(ax + x')) = (ax + x', a(-x) + (-x')) = a(x, -x) + (x', -x') = a\,\varphi(x) + \varphi(x')$$

gilt, ist φ nach Bemerkung (2.36) ein $\mathbb{R}$-Vektorraumhomomorphismus. Nach Korollar (2.57) ist

$$\operatorname{Im}\varphi = \{\varphi(x) \mid x \in \mathbb{R}\} = \{(x, -x) \mid x \in \mathbb{R}\}$$

ein $\mathbb{R}$-Untervektorraum von φ. □

(2.58) Korollar. Es seien ein Körper K und ein K-Vektorraum V gegeben.

(a) Für jedes $v \in V$ ist

$$Kv = \{av \mid a \in K\}$$

ein K-Untervektorraum von V.

(b) Es ist $\{0\}$ ein K-Untervektorraum von V.

Beweis.

(a) Für jedes $v \in V$ ist $\rho_v\colon K \to V$, $a \mapsto av$ ein K-Vektorraumhomomorphismus und damit

$$\operatorname{Im}\rho_v = \{\rho_v(a) \mid a \in K\} = \{av \mid a \in K\} = Kv$$

ein K-Untervektorraum von V nach Korollar (2.57).

(b) Nach (a) ist $\{0\} = K0$ ein K-Untervektorraum von V. □

Kern eines Vektorraumhomomorphismus

Es seien ein Körper K und ein K-Vektorraumhomomorphismus $\varphi\colon V \to W$ gegeben. Dann ist $\{0\}$ ein Untervektorraum von W nach Korollar (2.58)(b) und damit $\varphi^{-1}(\{0\}) = \{v \in V \mid \varphi(v) = 0\}$ ein Untervektorraum von V nach Proposition (2.56)(b).

(2.59) Definition (Kern)**.** Es seien ein Körper K und ein K-Vektorraumhomomorphismus $\varphi\colon V \to W$ gegeben. Der K-Untervektorraum

$$\operatorname{Ker}\varphi := \varphi^{-1}(\{0\})$$

von V heißt *Kern* von φ.

Wir ermitteln als Beispiel den Kern des Vektorraumhomomorphismus aus Beispiel (2.33)(b)(i):

(2.60) Beispiel. Es sei ein Körper K gegeben. Der Kern von $\varphi\colon K^3 \to K^2$, $(x_1, x_2, x_3) \mapsto (x_3, x_1)$ ist gegeben durch

$$\operatorname{Ker}\varphi = \{(0, a, 0) \mid a \in K\}.$$

Beweis. Es ist

$$\begin{aligned}\operatorname{Ker}\varphi &= \{(x_1, x_2, x_3) \in K^3 \mid \varphi(x_1, x_2, x_3) = 0\} = \{(x_1, x_2, x_3) \in K^3 \mid (x_3, x_1) = 0\}\\ &= \{(x_1, x_2, x_3) \in K^3 \mid x_1 = 0,\ x_3 = 0\} = \{(0, a, 0) \mid a \in K\}.\end{aligned}$$ □

Man kann die Eigenschaft, dass der Kern ein Untervektorraum ist, manchmal auch für den Nachweis nutzen, dass man bei einer gegebenen Teilmenge einen Untervektorraum vorliegen hat:

(2.61) Beispiel. Es ist $\{(x_1, x_2) \in \mathbb{R}^2 \mid x_1 + x_2 = 0\}$ ein $\mathbb{R}$-Untervektorraum von $\mathbb{R}^2$.

Beweis. Wir betrachten die Abbildung $\varphi\colon \mathbb{R}^2 \to \mathbb{R}$, $(x_1, x_2) \mapsto x_1 + x_2$. Da für $a \in \mathbb{R}$, $(x_1, x_2), (x_1', x_2') \in \mathbb{R}^2$ stets

$$\begin{aligned}\varphi(a(x_1, x_2) + (x_1', x_2')) &= \varphi(ax_1 + x_1', ax_2 + x_2') = ax_1 + x_1' + ax_2 + x_2' = a(x_1 + x_2) + (x_1' + x_2')\\ &= a\,\varphi(x_1, x_2) + \varphi(x_1', x_2')\end{aligned}$$

gilt, ist φ nach Bemerkung (2.36) ein $\mathbb{R}$-Vektorraumhomomorphismus. Folglich ist

$$\operatorname{Ker}\varphi = \{(x_1, x_2) \in \mathbb{R}^2 \mid \varphi(x_1, x_2) = 0\} = \{(x_1, x_2) \in \mathbb{R}^2 \mid x_1 + x_2 = 0\}$$

ein $\mathbb{R}$-Untervektorraum von φ. □

Alternativer Beweis zu Beispiel (2.54)(a). Nach Beispiel (2.61) ist

$$\{(x_1, x_2) \in \mathbb{R}^2 \mid x_1 + x_2 = 0\} = \{(x_1, x_2) \in \mathbb{R}^2 \mid x_2 = -x_1\} = \{(x, -x) \mid x \in \mathbb{R}\}$$

ein $\mathbb{R}$-Untervektorraum von φ. □

In der Analysis studiert man Kern und Bild des Differentialoperators

$$\mathrm{D}\colon \mathrm{C}^1(\mathbb{R}, \mathbb{R}) \to \mathrm{C}(\mathbb{R}, \mathbb{R}),\ f \mapsto f',$$

vgl. Beispiel (2.35):

(2.62) Beispiel. Es ist

$$\begin{aligned}\operatorname{Ker}\mathrm{D} &= \{f \in \operatorname{Map}(\mathbb{R}, \mathbb{R}) \mid \text{es gibt ein } a \in \mathbb{R} \text{ mit } f(x) = a \text{ für alle } x \in \mathbb{R}\} \cong \mathbb{R},\\ \operatorname{Im}\mathrm{D} &= \mathrm{C}(\mathbb{R}, \mathbb{R}).\end{aligned}$$

Ohne Beweis. □

(2.63) Lemma. Es seien ein Körper K und ein K-Vektorraumhomomorphismus $\varphi\colon V \to W$ gegeben. Genau dann ist φ injektiv, wenn $\operatorname{Ker}\varphi = \{0\}$ ist.

Beweis. Zunächst sei φ injektiv. Für $v \in \operatorname{Ker}\varphi$ ist $\varphi(v) = 0 = \varphi(0)$, wegen der Injektivität also $v = 0$. Somit ist $\operatorname{Ker}\varphi \subseteq \{0\}$. Da aber 0 in jedem Untervektorraum enthalten ist, impliziert dies schon $\operatorname{Ker}\varphi = \{0\}$.
Nun gelte umgekehrt $\operatorname{Ker}\varphi = \{0\}$ und es seien $v, v' \in V$ mit $\varphi(v) = \varphi(v')$ gegeben. Da φ Homomorphismus ist, folgt $\varphi(v - v') = \varphi(v) - \varphi(v') = 0$, d.h. es ist $v - v' \in \operatorname{Ker}\varphi = \{0\}$, also $v - v' = 0$ und damit $v = v'$. Folglich ist φ injektiv. □

Man kann also sagen: Der Kern eines Vektorraumhomomorphismus „misst“, wie weit der Homomorphismus davon entfernt ist, injektiv zu sein.

(2.64) Korollar. Es sei ein Körper K gegeben. Ein K-Vektorraumhomomorphismus $\varphi\colon V \to W$ ist genau dann ein K-Vektorraumisomorphismus, wenn $\operatorname{Ker}\varphi = \{0\}$ und $\operatorname{Im}\varphi = W$ ist.

Beweis. Nach Bemerkung (2.40) ist ein Homomorphismus $\varphi\colon V \to W$ genau dann ein Isomorphismus, wenn er bijektiv, also injektiv und surjektiv, ist. Nach Lemma (2.63) ist φ genau dann injektiv, wenn $\operatorname{Ker}\varphi = \{0\}$. Ferner ist φ genau dann surjektiv, wenn $\operatorname{Im}\varphi = W$ ist. □

Mit Hilfe des Kerns, also der Faser über dem Nullvektor, können wir alle nicht-leeren Fasern beschreiben:

(2.65) Proposition. Es seien ein Körper K und ein K-Vektorraumhomomorphismus $\varphi\colon V \to W$ gegeben. Für alle $v \in V$ ist

$$\varphi^{-1}(\{\varphi(v)\}) = v + \operatorname{Ker}\varphi.$$

Beweis. Es ist

$$\begin{aligned}\varphi^{-1}(\{\varphi(v)\}) &= \{v' \in V \mid \varphi(v') = \varphi(v)\} = \{v' \in V \mid \varphi(v') - \varphi(v) = 0\} = \{v' \in V \mid \varphi(v' - v) = 0\} \\ &= \{v' \in V \mid v' - v \in \operatorname{Ker}\varphi\} = \{v' \in V \mid v' \in v + \operatorname{Ker}\varphi\} = v + \operatorname{Ker}\varphi.\end{aligned}$$ □

Schnitt und innere Summe von Untervektorräumen

(2.66) Proposition. Es seien ein Körper K, ein K-Vektorraum V und eine Familie $(U_i)_{i\in I}$ von K-Untervektorräumen von V gegeben.

(a) Es ist $\bigcap_{i\in I} U_i$ ein K-Untervektorraum von V.

(b) Es ist $\{\sum_{i\in I} u_i \mid (u_i)_{i\in I} \in \times_{i\in I} U_i \text{ mit } u_i = 0 \text{ für fast alle } i \in I\}$ ein K-Untervektorraum von V.

Beweis.

(a) Siehe Aufgabe 66(a).

(b) Siehe Aufgabe 66(b). □

(2.67) Definition (Schnitt, innere Summe)**.** Es seien ein Körper K, ein K-Vektorraum V und eine Familie $(U_i)_{i\in I}$ von K-Untervektorräumen von V gegeben.

(a) Der Untervektorraum $\bigcap_{i\in I} U_i$ von V aus Proposition (2.66)(a) heißt *Schnitt* (oder *Durchschnitt*) von $(U_i)_{i\in I}$.
Ist $I = [1, n]$ für ein $n \in \mathbb{N}_0$, so schreiben wir auch

$$U_1 \cap \ldots \cap U_n := \bigcap_{i\in[1,n]} U_i$$

und sprechen vom *Schnitt* (oder *Durchschnitt*) von $U_1, \ldots, U_n$.

(b) Der Untervektorraum

$$\sum_{i\in I} U_i := \{\sum_{i\in I} u_i \mid (u_i)_{i\in I} \in \bigtimes_{i\in I} U_i \text{ mit } u_i = 0 \text{ für fast alle } i \in I\}$$

von V aus Proposition (2.66)(b) heißt *innere Summe* von $(U_i)_{i\in I}$ (oder *Summe von* $(U_i)_{i\in I}$ *in* V).
Ist $I = [1, n]$ für ein $n \in \mathbb{N}_0$, so schreiben wir auch

$$U_1 + \cdots + U_n := \sum_{i\in[1,n]} U_i$$

und sprechen von der *inneren Summe* von $U_1, \ldots, U_n$ (oder von der *Summe von* $U_1, \ldots, U_n$ *in* V).

Insbesondere gilt nach Proposition (2.66) für Untervektorräume U_1 und U_2 eines Vektorraums V über einem Körper K, dass $U_1 \cap U_2 = \{u \mid u \in U_1 \text{ und } u \in U_2\}$ und $U_1 + U_2 = \{u_1 + u_2 \mid u_1 \in U_1, u_2 \in U_2\}$ wieder Untervektorräume von V sind.

(2.68) Beispiel. Es sind $U_1 = \mathbb{R}(0,1,0) + \mathbb{R}(0,0,1)$ und $U_2 = \mathbb{R}(1,0,0) + \mathbb{R}(0,1,1)$ Untervektorräume über $\mathbb{R}$ von $\mathbb{R}^3$. Der Schnitt von U_1 und U_2 ist gegeben durch

$$U_1 \cap U_2 = \mathbb{R}(0,1,1).$$

Beweis. Nach Korollar (2.58)(a) sind $\mathbb{R}(0,1,0), \mathbb{R}(0,0,1), \mathbb{R}(1,0,0)$ und $\mathbb{R}(0,1,1)$ Untervektorräume von $\mathbb{R}^3$, also auch die inneren Summen $U_1 = \mathbb{R}(0,1,0) + \mathbb{R}(0,0,1)$ und $U_2 = \mathbb{R}(1,0,0) + \mathbb{R}(0,1,1)$ nach Proposition (2.66)(b). Es ergibt sich

$$\begin{aligned} U_1 \cap U_2 &= (\mathbb{R}(0,1,0) + \mathbb{R}(0,0,1)) \cap (\mathbb{R}(1,0,0) + \mathbb{R}(0,1,1)) = \{(0,a,b) \mid a,b \in \mathbb{R}\} \cap \{(c,d,d) \mid c,d \in \mathbb{R}\} \\ &= \{(0,d,d) \mid d \in \mathbb{R}\} = \mathbb{R}(0,1,1). \end{aligned}$$ □

Aufgaben

Aufgabe 63 (Untervektorräume)**.**

(a) Bestimmen Sie alle $\mathbb{R}$-Untervektorräume von $\mathbb{R}^2$. Wie kann man diese graphisch interpretieren?

(b) Es sei ein Körper K gegeben. Bestimmen Sie alle K-Untervektorräume von K.

(c) Zeigen Sie, dass es unendlich viele $\mathbb{Q}$-Untervektorräume von $\mathbb{R}$ gibt.

Aufgabe 64 (Koprodukt)**.** Es seien ein Körper K und eine Familie $(V_i)_{i\in I}$ bestehend aus K-Vektorräumen V_i für $i \in I$ gegeben. Für $v \in \times_{i\in I} V_i$ sagen wir, dass $v_i = 0$ *für fast alle* $i \in I$ *ist*, falls $v_i \neq 0$ für nur endlich viele $i \in I$ gilt. Wir setzen

$$U := \{v \in \bigtimes_{i\in I} V_i \mid v_i = 0 \text{ für fast alle } i \in I\}.$$

Zeigen Sie:

(a) Es wird U bzgl. der Struktur aus Aufgabe 59(a) ein K-Untervektorraum von $\times_{i\in I} V_i$.

(b) Für alle $i \in I$ wird $\mathrm{emb}_i \colon V_i \to U$ gegeben durch

$$(\mathrm{emb}_i(v_i))_j = \begin{cases} v_i, & \text{falls } j = i, \\ 0, & \text{falls } j \neq i, \end{cases}$$

für $j \in I$ bzgl. der Struktur aus (a) ein K-Vektorraumhomomorphismus.

Aufgabe 65 (Standardvektorraum)**.** Es seien ein Körper K und eine Menge I gegeben. Zeigen Sie, dass

$$K^{(I)} = \{x \in K^I \mid x_i = 0 \text{ für fast alle } i \in I\}$$

ein K-Untervektorraum von K^I ist.

Aufgabe 66 (Schnitt und innere Summe)**.** Es seien ein Körper K, ein K-Vektorraum V und eine Familie $(U_i)_{i\in I}$ von K-Untervektorräumen von V gegeben. Zeigen Sie:

(a) Es ist $\bigcap_{i\in I} U_i$ ein K-Untervektorraum von V.

(b) Es ist $\{\sum_{i\in I} u_i \mid (u_i)_{i\in I} \in \times_{i\in I} U_i \text{ mit } u_i = 0 \text{ für fast alle } i \in I\}$ ein K-Untervektorraum von V.

Aufgabe 67 (Untervektorraumoperationen)**.** Es seien ein Körper K und ein K-Vektorraum V gegeben.
Für Teilmengen $X, Y \subseteq V$ schreiben wir $X + Y := \{x + y \mid x \in X, y \in Y\}$. Für $v \in V$, $X \subseteq V$ schreiben wir $v + X := \{v\} + X$. Für $a \in K$, $X \subseteq V$ schreiben wir $aX := \{ax \mid x \in X\}$.
Zeigen oder widerlegen Sie:

(a) Für alle $U_1, U_2 \leq V$ ist $U_1 \cap U_2 \leq V$.

(b) Für alle $U_1, U_2 \leq V$ ist $U_1 \cup U_2 \leq V$.

(c) Für alle $v \in V$, $U \leq V$ ist $v + U \leq V$.

(d) Für alle $a_1, a_2 \in K$, $U_1, U_2 \leq V$ ist $a_1U_1 + a_2U_2 \leq V$.

(e) Genau dann ist $U_1 + U_2 = U_1$, wenn $U_2 \leq U_1$ gilt.

(f) Für alle $U_1, U_2, U_3 \leq V$ ist $U_1 \cap (U_2 + U_3) = (U_1 \cap U_2) + (U_1 \cap U_3)$.

(g) Für alle $U_1, U_2, U_3 \leq V$ ist $U_1 + (U_2 \cap U_3) = (U_1 + U_2) \cap (U_1 + U_3)$.

4 Linearkombinationen

Erzeugnis

(2.69) Definition (Erzeugnis)**.** Es seien ein Körper K und ein K-Vektorraum V gegeben.

(a) Für eine Teilmenge S von V heißt der K-Untervektorraum

$$\langle S\rangle = \langle S\rangle_K = \langle S\rangle_{\mathbf{Vec}(K)} := \bigcap \{U \mid U \text{ ist ein } K\text{-Untervektorraum von } V \text{ mit } S \subseteq U\}$$

von V das *Vektorraumerzeugnis* über K (oder K-*Vektorraumerzeugnis* oder K-*Erzeugnis* oder *Erzeugnis*) von S in V.

(b) Für eine Familie $s = (s_i)_{i\in I}$ in V heißt

$$\langle s_i \mid i \in I\rangle = \langle s_i \mid i \in I\rangle_K = \langle s_i \mid i \in I\rangle_{\mathbf{Vec}(K)} := \langle \{s_i \mid i \in I\}\rangle_{\mathbf{Vec}(K)}$$

das *Vektorraumerzeugnis* über K (oder K-*Vektorraumerzeugnis* oder K-*Erzeugnis* oder *Erzeugnis*) von s in V.

Für $n \in \mathbb{N}_0$, $s_i \in V$ für $i \in [1, n]$ schreiben wir auch

$$\langle s_1, \ldots, s_n\rangle := \langle s_i \mid i \in [1, n]\rangle.$$

(2.70) Bemerkung. Es seien ein Körper K, ein K-Vektorraum V und eine Teilmenge S von V gegeben. Dann ist $\langle S\rangle$ der bzgl. Inklusion kleinste K-Untervektorraum von V, welcher S als Teilmenge enthält.

Beweis. Es sei $\mathcal{U} := \{U \mid U \text{ ist ein Untervektorraum von } V \text{ mit } S \subseteq U\}$, so dass

$$\langle S\rangle = \bigcap \mathcal{U} = \bigcap_{U\in\mathcal{U}} U$$

gilt. Dann ist $S \subseteq U$ für alle $U \in \mathcal{U}$, also auch

$$S \subseteq \bigcap_{U\in\mathcal{U}} U = \langle S\rangle.$$

Für einen beliebigen Untervektorraum U von V mit $S \subseteq U$ gilt hingegen $U \in \mathcal{U}$, also

$$\langle S\rangle = \bigcap_{U'\in\mathcal{U}} U' \subseteq U. \qquad \square$$

(2.71) Korollar. Es seien ein Körper K und ein K-Vektorraum V gegeben.

(a) Es ist

$$\langle \emptyset\rangle = \{0\}.$$

(b) Es ist

$$\langle V\rangle = V.$$

Beweis.

(a) Da $\{0\}$ stets ein Untervektorraum von V ist und $0 \in U$ für jeden Untervektorraum U von V gilt, ist $\{0\}$ der bzgl. Inklusion kleinste Untervektorraum von V, welcher $\emptyset$ als Teilmenge enthält. Nach Bemerkung (2.70) ist also $\langle\emptyset\rangle = \{0\}$.

(b) Nach Bemerkung (2.70) ist $\langle V\rangle$ der bzgl. Inklusion kleinste Untervektorraum von V, welcher V als Teilmenge enthält. Es gilt also $V \subseteq \langle V\rangle \subseteq V$ und damit $\langle V\rangle = V$. □

(2.72) Korollar. Es seien ein Körper K, ein K-Vektorraum V und Teilmengen S und T von V gegeben. Wenn $S \subseteq T$ ist, dann ist $\langle S\rangle \leq \langle T\rangle$.

Beweis. Nach Bemerkung (2.70) gilt $T \subseteq \langle T\rangle$, wegen $S \subseteq T$ also auch $S \subseteq \langle T\rangle$. Ebenfalls nach Bemerkung (2.70) ist nun aber $\langle S\rangle$ der bzgl. Inklusion kleinste Untervektorraum von V, welcher S als Teilmenge enthält, d.h. wir haben $\langle S\rangle \leq \langle T\rangle$. □

Lineare Hülle

In der Praxis ist die definierende Eigenschaft des Erzeugnisses unhandlich: Die Menge aller Untervektorräume, welche eine gegebene Menge enthalten, kann sehr groß sein, oftmals sogar unendlich, und ist daher im Allgemeinen nur vergleichsweise schwer zu überblicken. Aus diesem Grund wollen wir im Folgenden eine deutlich einfachere Beschreibung des Erzeugnisses herleiten.

(2.73) Definition (Linearkombination)**.** Es seien ein Körper K und ein K-Vektorraum V gegeben.

(a) Es sei eine Familie $s = (s_i)_{i\in I}$ in V gegeben. Für $a \in K^{(I)}$ heißt $\lambda_s(a) := \sum_{i\in I} a_i s_i$ die *Linearkombination* von s zu a.

Eine *Linearkombination* von s ist eine Linearkombination von s zu einem $a \in K^{(I)}$.

Die *Menge aller Linearkombinationen* $\sum_{i\in I} Ks_i$ von s heißt *lineare Hülle* (oder *Spann*) von s.

(b) Es sei eine Teilmenge S von V gegeben. Für $a \in K^{(S)}$ heißt $\lambda_S(a) := \sum_{s\in S} a_s s$ die *Linearkombination* von S zu a.

Eine *Linearkombination* von S ist eine Linearkombination von S zu einem $a \in K^{(S)}$.

Die *Menge aller Linearkombinationen* $\sum_{s\in S} Ks$ von S heißt *lineare Hülle* (oder *Spann*) von S.

In einem Vektorraum V über einem Körper K seien eine Familie $s = (s_i)_{i\in I}$ sowie ein Element v gegeben. Genau dann ist v eine Linearkombination von s, wenn $v \in \sum_{i\in I} Ks_i$ ist, d.h. wenn es $a_i \in K$ für $i \in I$ so gibt, dass $a_i = 0$ für fast alle $i \in I$ und $v = \sum_{i\in I} a_i s_i$ ist. Mit anderen Worten: Genau dann ist v eine Linearkombination von s, wenn es ein $n \in \mathbb{N}_0$ sowie $a_j \in K$, $i_j \in I$ für $j \in [1,n]$ mit $v = \sum_{j\in[1,n]} a_j s_{i_j}$ gibt. Insbesondere ist v genau dann Linearkombination eines n-Tupels $t = (t_j)_{j\in[1,n]}$ in V für ein $n \in \mathbb{N}_0$, wenn es $a_j \in K$ für $j \in [1,n]$ mit $v = \sum_{j\in[1,n]} a_j t_j$ gibt.

(2.74) Beispiel.

(a) In $\mathbb{Q}^2$ ist $(-1,-4)$ eine Linearkombination von $\{(1,2),(1,3)\}$.

(b) In $\mathbb{R}^3$ ist jedes $x \in \mathbb{R}^3$ eine Linearkombination von $\{(1,0,0),(0,1,0),(0,0,1)\}$.

Beweis.

(a) Wir haben

$$(-1,-4) = (1,2) - 2(1,3) = 1(1,2) + (-2)(1,3).$$

(b) Für $x \in \mathbb{R}^3$ ist

$$x = (x_1,x_2,x_3) = (x_1,0,0) + (0,x_2,0) + (0,0,x_3) = x_1(1,0,0) + x_2(0,1,0) + x_3(0,0,1).$$ □

Nach Definition (2.73) betrachten wir Linearkombinationen von Tupeln sowie von Teilmengen. Der Grund hierfür liegt in der definierenden Gestalt von Mengen begründet: Während in Mengen Elemente stets eindeutig sind, können die Einträge in Familien unter Umständen mehrfach auftreten. Wir sagen, dass die Einträge einer Familie $s = (s_i)_{i\in I}$ verschieden sind, wenn für $i, j \in I$ aus $i \neq j$ stets $s_i \neq s_j$ folgt.
Das Konzept der Linearkombination einer Familie ist also leicht allgemeiner als das einer Teilmenge. Es besteht folgender Zusammenhang:

(2.75) Bemerkung. Es seien ein Körper K, ein K-Vektorraum V und ein $v \in V$ gegeben.

(a) Es sei eine Familie $s = (s_i)_{i\in I}$ in V gegeben. Genau dann ist v eine Linearkombination von s, wenn v eine Linearkombination von $\{s_i \mid i \in I\}$ ist.

(b) Es sei eine Teilmenge S von V gegeben. Genau dann ist v eine Linearkombination von S, wenn v eine Linearkombination von $(s)_{s\in S}$ ist.

(2.76) Bemerkung. Es seien ein Körper K, ein K-Vektorraum V und eine Familie $s = (s_i)_{i\in I}$ in V gegeben. Die Abbildung

$$\lambda_s \colon K^{(I)} \to V,\ a \mapsto \sum_{i\in I} a_i s_i$$

ist ein K-Vektorraumhomomorphismus mit

$$\operatorname{Im}\lambda_s = \sum_{i\in I} K s_i.$$

Beweis. Für $c \in K$, $a, a' \in K^{(I)}$ gilt

$$\begin{aligned}\lambda_s(ca + a') &= \sum_{i\in I}(ca + a')_i s_i = \sum_{i\in I}(ca_i + a'_i)s_i = \sum_{i\in I}(ca_i s_i + a'_i s_i) = c\sum_{i\in I} a_i s_i + \sum_{i\in I} a'_i s_i \\ &= c\lambda_s(a) + \lambda_s(a').\end{aligned}$$

Nach Bemerkung (2.36) ist also λ_s ein Vektorraumhomomorphismus. Ferner gilt

$$\operatorname{Im}\lambda_s = \{\lambda_s(a) \mid a \in K^{(I)}\} = \{\sum_{i\in I} a_i s_i \mid a \in K^{(I)}\} = \sum_{i\in I} K s_i. \qquad \square$$

(2.77) Bemerkung. Es seien ein Körper K, ein K-Vektorraum V und eine Familie $s = (s_i)_{i\in I}$ in V gegeben.

(a) Es ist 0 eine Linearkombination von s.

(b) Für alle $i \in I$ ist s_i eine Linearkombination von s.

Beweis.

(a) Es ist $0 = \sum_{i\in I} 0 s_i$.

(b) Für alle $i \in I$ ist $s_i = \sum_{j\in I\setminus\{i\}} 0 s_j + 1 s_i$. $\square$

(2.78) Bemerkung. Es seien ein Körper K, ein K-Vektorraum V, eine Familie $s = (s_i)_{i\in I}$ in V und ein $v \in V$ gegeben.

(a) Wenn v eine Linearkombination von s ist, dann ist für alle $a \in K$ auch av eine Linearkombination von s.

(b) Wenn av für ein $a \in K^\times$ eine Linearkombination von s ist, dann ist auch v eine Linearkombination von s.

Die folgende Bemerkung besagt, dass Linearkombinationen und Vektorraumhomomorphismen verträglich sind. Für eine Abbildung $f \colon X \to Y$ und eine Familie $x = (x_i)_{i\in I}$ in X erhalten wir die Familie $f \circ x = (f(x_i))_{i\in I}$ in Y.

(2.79) Bemerkung. Es seien ein Körper K, ein K-Vektorraumhomomorphismus $\varphi \colon V \to W$ und eine Familie $s = (s_i)_{i\in I}$ in V gegeben. Dann ist

$$\varphi \circ \lambda_s = \lambda_{\varphi\circ s}.$$

Beweis. Da φ ein K-Vektorraumhomomorphismus ist, gilt für $a \in K^{(I)}$ stets

$$\varphi(\lambda_s(a)) = \varphi(\sum_{i\in I} a_i s_i) = \sum_{i\in I} \varphi(a_i s_i) = \sum_{i\in I} a_i\, \varphi(s_i) = \lambda_{\varphi\circ s}(a),$$

d.h. es ist $\varphi \circ \lambda_s = \lambda_{\varphi\circ s}$. □

Wir werden nun sehen, dass das Erzeugnis einer Teilmenge eines Vektorraums gerade gleich der linearen Hülle dieser Teilmenge ist.

(2.80) Lemma. Es seien ein Körper K und ein K-Vektorraum V gegeben.

(a) Für jede Familie $s = (s_i)_{i\in I}$ in V ist

$$\langle s\rangle = \sum_{i\in I} Ks_i.$$

(b) Für jede Teilmenge S von V ist

$$\langle S\rangle = \sum_{s\in S} Ks.$$

Beweis.

(a) Es sei eine Familie $s = (s_i)_{i\in I}$ in V gegeben. Für alle $j \in I$ ist $s_j \in \sum_{i\in I} Ks_i$ nach Bemerkung (2.77)(b). Da $\langle s\rangle = \langle s_j \mid j \in I\rangle$ nach Bemerkung (2.70) aber der bzgl. Inklusion kleinste Untervektorraum von V, welcher $\{s_j \mid j \in I\}$ als Teilmenge enthält, ist, impliziert dies bereits $\langle s\rangle \subseteq \sum_{i\in I} Ks_i$. Umgekehrt ist insbesondere $\{s_i \mid i \in I\} \subseteq \langle s\rangle$ nach Bemerkung (2.70), d.h. es ist $s_i \in \langle s\rangle$ für alle $i \in I$. Dann ist aber auch $\sum_{i\in I} a_i s_i \in \langle s\rangle$ für alle $a \in K^{(I)}$ nach dem Untervektorraumkriterium (2.52), d.h. es ist $\sum_{i\in I} Ks_i \subseteq \langle s\rangle$. Insgesamt haben wir also $\langle s\rangle = \sum_{i\in I} Ks_i$.

(b) Nach (a) ist

$$\langle S\rangle = \langle s \mid s \in S\rangle = \sum_{s\in S} Ks$$

für jede Teilmenge S von V. □

(2.81) Bemerkung. Es seien ein Körper K, ein K-Vektorraum V, eine Familie $s = (s_i)_{i\in I}$ in V und Teilmengen I_1 und I_2 von I mit $I = I_1 \dot\cup I_2$ gegeben. Für $a \in K^{(S)}$ ist dann

$$\lambda_s(a) = \lambda_{s|_{I_1}}(a|_{I_1}) + \lambda_{s|_{I_2}}(a|_{I_2}).$$

Auf Grund von Bemerkung (2.75) beschränken wir uns bei den folgenden Aussagen in der Regel auf Linearkombinationen von Mengen, sofern wir die lineare Hülle, nach Lemma (2.80) also das Erzeugnis, studieren.

(2.82) Proposition. Es seien ein Körper K, ein K-Vektorraum V, eine Teilmenge S von V und ein $v \in V$ gegeben. Die folgenden Bedingungen sind äquivalent.

(a) Es ist v eine Linearkombination von S.

(b) Es ist $\langle S \cup \{v\}\rangle \subseteq \langle S\rangle$.

(c) Es ist $\langle S \cup \{v\}\rangle = \langle S\rangle$.

Beweis. Es gelte zunächst Bedingung (a), d.h. es sei v eine Linearkombination von S. Ferner sei ein $w \in \langle S \cup \{v\}\rangle$ gegeben. Dann gibt es $a \in K^{(S)}$, $b \in K^{(S\cup\{v\})}$ mit $v = \lambda_S(a)$ und $w = \lambda_{S\cup\{v\}}(b)$. Da λ_S ein Vektorraumhomomorphismus ist, folgt

$$w = \lambda_{S\cup\{v\}}(b) = \lambda_S(b|_S) + \lambda_{\{v\}}(b|_{\{v\}}) = \lambda_S(b|_S) + b_v v = \lambda_S(b|_S) + b_v\lambda_S(a) = \lambda_S(b|_S + b_v a).$$

Somit ist $w \in \sum_{s\in S} Ks = \langle S\rangle$ nach Lemma (2.80)(b). Folglich haben wir $\langle S \cup \{v\}\rangle \subseteq \langle S\rangle$, d.h. es gilt Bedingung (b).

Gilt umgekehrt Bedingung (b), d.h. ist $\langle S \cup \{v\}\rangle \subseteq \langle S\rangle$, so gilt insbesondere $v \in \langle S \cup \{v\}\rangle = \langle S\rangle = \sum_{s\in S} Ks$ nach Bemerkung (2.70) und Lemma (2.80)(b). Dies bedeutet, dass v eine Linearkombination von S ist, d.h. Bedingung (a) gilt.
Wir haben also gezeigt, dass Bedingung (a) und Bedingung (b) äquivalent sind. Da nach Korollar (2.72) aber ohnehin $\langle S\rangle \subseteq \langle S\cup\{v\}\rangle$ ist, sind auch Bedingung (b) und Bedingung (c) äquivalent. Insgesamt sind Bedingung (a), Bedingung (b) und Bedingung (c) äquivalent. □

(2.83) Korollar. Es seien ein Körper K und ein K-Vektorraum V gegeben. Für jede Teilmenge S von V ist

$$\langle S\rangle = \langle S \cup \{0\}\rangle.$$

Beweis. Dies folgt aus Bemerkung (2.77)(a) und Proposition (2.82). □

Die folgende Proposition gibt eine Antwort auf die Frage, wie wir die Beschreibungen von Erzeugnissen modifizieren können.

(2.84) Proposition. Es seien ein Körper K, ein K-Vektorraum V und eine Teilmenge S von V gegeben.

(a) Für $a \in K$, $s, s' \in S$ mit $s \neq s'$ ist

$$\langle S\rangle = \langle (S \setminus \{s'\}) \cup \{s' + as\}\rangle.$$

(b) Für $a \in K^\times$, $s \in S$ ist

$$\langle S\rangle = \langle (S \setminus \{s\}) \cup \{as\}\rangle.$$

Beweis.

(a) Es seien $a \in K$, $s, s' \in S$ mit $s \neq s'$ gegeben.

Zunächst gelte $s = s' + as$. Dann ist $s' = s - as = (1-a)s$, also $s, s' \in \sum_{t\in S\setminus\{s'\}} Kt = \langle S \setminus \{s'\}\rangle$ nach Lemma (2.80)(b). Mit Proposition (2.82) erhalten wir

$$\langle S\rangle = \langle (S \setminus \{s'\}) \cup \{s'\}\rangle = \langle S \setminus \{s'\}\rangle = \langle (S \setminus \{s'\}) \cup \{s\}\rangle = \langle (S \setminus \{s'\}) \cup \{s' + as\}\rangle.$$

Als nächstes gelte $s \neq s' + as$. Nach Lemma (2.80)(b) ist $\langle S\rangle = \sum_{t\in S} Kt$, für $v \in \langle S\rangle$ gibt es also ein $a \in K^{(S)}$ mit

$$\begin{aligned} v &= \sum_{t\in S} a_t t = \sum_{t\in S\setminus\{s,s'\}} a_t t + a_s s + a_{s'} s' = \sum_{t\in S\setminus\{s,s'\}} a_t t + a_s s - a_{s'} as + a_{s'} s' + a_{s'} as \\ &= \sum_{t\in S\setminus\{s,s'\}} a_t t + (a_s - a_{s'} a)s + a_{s'}(s' + as). \end{aligned}$$

also mit $v \in \sum_{t\in S\setminus\{s'\}} Kt + K(s'+as) = \langle (S \setminus \{s'\}) \cup \{s'+as\}\rangle$. Folglich ist $\langle S\rangle \subseteq \langle (S \setminus \{s'\}) \cup \{s'+as\}\rangle$. Umgekehrt folgt wegen $s \neq s' + as$ nun aber auch

$$\begin{aligned} \langle (S \setminus \{s'\}) \cup \{s' + as\}\rangle &\subseteq \langle (((S \setminus \{s'\}) \cup \{s' + as\}) \setminus \{s' + as\}) \cup \{(s' + as) + (-a)s\}\rangle \\ &= \langle (S \setminus \{s'\}) \cup \{s'\}\rangle = \langle S\rangle \end{aligned}$$

Insgesamt gilt in jedem Fall $\langle S\rangle = \langle (S \setminus \{s'\}) \cup \{s' + as\}\rangle$.

(b) Es seien $a \in K^\times$, $s \in S$ gegeben. Nach Lemma (2.80)(b) ist $\langle S\rangle = \sum_{t\in S} Kt$, für $v \in \langle S\rangle$ gibt es also ein $a \in K^{(S)}$ mit

$$v = \sum_{t\in S} a_t s = \sum_{t\in S\setminus\{s\}} a_t t + a_s s = \sum_{t\in S\setminus\{s\}} a_t t + a_s a^{-1}(as),$$

also mit $v \in \sum_{t\in S\setminus\{s\}} Kt + K(as) = \langle (S \setminus \{s\}) \cup \{as\}\rangle$. Folglich ist $\langle S\rangle \subseteq \langle (S \setminus \{s\}) \cup \{as\}\rangle$. Umgekehrt folgt nun aber auch

$$\langle (S \setminus \{s\}) \cup \{as\}\rangle \subseteq \langle (((S \setminus \{s\}) \cup \{as\}) \setminus \{as\}) \cup \{a^{-1}(as)\}\rangle = \langle (S \setminus \{s\}) \cup \{s\}\rangle = \langle S\rangle.$$

Insgesamt gilt $\langle S\rangle = \langle (S \setminus \{s\}) \cup \{as\}\rangle$. □

Die vorangegangene Proposition liefert uns eine Methode, die Beschreibungen von erzeugten Untervektorräumen zu vereinfachen. Wir begnügen uns hier mit einem Beispiel.

(2.85) Beispiel. In $\mathbb{R}^4$ ist

$$\langle (3,-2,-3,4),(1,1,-1,1),(-1,-1,1,3),(-2,2,2,1)\rangle = \langle (1,0,-1,0),(0,1,0,0),(0,0,0,1)\rangle.$$

Beweis. Wir schreiben die Quadrupel als Zeilen in eine Matrix und wenden elementare Zeilenoperationen an:

$$\begin{pmatrix} 3 & -2 & -3 & 4 \\ 1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 3 \\ -2 & 2 & 2 & 1 \end{pmatrix} \xmapsto{\mathrm{add}_{4,2,2}\circ\mathrm{add}_{3,2,1}\circ\mathrm{add}_{1,2,-3}} \begin{pmatrix} 0 & -5 & 0 & 1 \\ 1 & 1 & -1 & 1 \\ 0 & 0 & 0 & 4 \\ 0 & 4 & 0 & 3 \end{pmatrix} \xmapsto{\mathrm{mul}_{3,\frac{1}{4}}} \begin{pmatrix} 0 & -5 & 0 & 1 \\ 1 & 1 & -1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 4 & 0 & 3 \end{pmatrix}$$

$$\xmapsto{\mathrm{add}_{4,3,-3}\circ\mathrm{add}_{2,3,-1}\circ\mathrm{add}_{1,3,-1}} \begin{pmatrix} 0 & -5 & 0 & 0 \\ 1 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 4 & 0 & 0 \end{pmatrix} \xmapsto{\mathrm{mul}_{1,-\frac{1}{5}}} \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 4 & 0 & 0 \end{pmatrix}$$

$$\xmapsto{\mathrm{add}_{4,1,-4}\circ\mathrm{add}_{2,1,-1}} \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xmapsto{\mathrm{sw}_{1,2}} \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Nach Proposition (2.84) und Proposition (2.82) gilt also

$$\langle (3,-2,-3,4),(1,1,-1,1),(-1,-1,1,3),(-2,2,2,1)\rangle = \langle (1,0,-1,0),(0,1,0,0),(0,0,0,1)\rangle. \qquad \square$$

Erzeugendensysteme

(2.86) Definition (Erzeugendensystem)**.** Es seien ein Körper K und ein K-Vektorraum V gegeben.

(a) Eine Familie $s = (s_i)_{i\in I}$ in V heißt (*parametrisiertes*) *Erzeugendensystem* über K (oder (*parametrisiertes*) *K-Erzeugendensystem* oder (*parametrisiertes*) *Erzeugendensystem*) von V, wenn $V = \langle s\rangle$ gilt.

(b) Eine Teilmenge S von V heißt *Erzeugendensystem* über K (oder *K-Erzeugendensystem* oder *Erzeugendensystem*) von V, wenn $V = \langle S\rangle$ gilt.

(2.87) Beispiel.

(a) Es ist $\{(1,0,0),(0,1,0),(0,0,1)\}$ ein Erzeugendensystem von $\mathbb{R}^3$.

(b) Es sind

$$S_1 = \{(3,-2,-3,4),(1,1,-1,1),(-1,-1,1,3),(-2,2,2,1)\},$$
$$S_2 = \{(1,0,-1,0),(0,1,0,0),(0,0,0,1)\}$$

Erzeugendensysteme des Unterraums $\langle S_1\rangle = \langle S_2\rangle$ von $\mathbb{R}^4$.

(c) Es ist

$$\left\{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}\right\}$$

ein Erzeugendensystem von $\mathbb{F}_3^{2\times 2}$.

Beweis.

(a) Nach Beispiel (2.74)(b) und Lemma (2.80)(b) ist

$$\mathbb{R}^3 = \mathbb{R}(1,0,0) + \mathbb{R}(0,1,0) + \mathbb{R}(0,0,1) = \langle (1,0,0),(0,1,0),(0,0,1)\rangle. \qquad \square$$

(b) Dies folgt aus Beispiel (2.85).

(c) Dies lässt sich analog zu (a) beweisen.

(2.88) Bemerkung. Es seien ein Körper K und ein K-Vektorraum V gegeben.

(a) Eine Familie $s = (s_i)_{i\in I}$ in V ist genau dann ein Erzeugendensystem von V, wenn $\{s_i \mid i \in I\}$ ein Erzeugendensystem von V ist.

(b) Eine Teilmenge S von V ist genau dann ein Erzeugendensystem von V, wenn $(s)_{s\in S}$ ein Erzeugendensystem von V ist.

(2.89) Bemerkung. Es seien ein Körper K und ein K-Vektorraum V gegeben. Dann ist V ein Erzeugendensystem von V.

Beweis. Dies folgt aus Bemerkung (2.71)(b). □

(2.90) Bemerkung. Es seien ein Körper K, ein K-Vektorraum V und Teilmengen S und T von V mit $S \subseteq T$ gegeben. Wenn S ein Erzeugendensystem von V ist, dann ist auch T ein Erzeugendensystem von V.

Beweis. Es sei S ein Erzeugendensystem von V, so dass $V = \langle S\rangle$ gilt. Wegen $S \subseteq T$ ist $\langle S\rangle \subseteq \langle T\rangle$ nach Korollar (2.72). Dann ist aber $V = \langle S\rangle \subseteq \langle T\rangle$, wegen $\langle T\rangle \subseteq V$ also $V = \langle T\rangle$, d.h. T ist ebenfalls ein Erzeugendensystem von V. □

(2.91) Bemerkung. Es seien ein Körper K und ein K-Vektorraum V gegeben. Eine Teilmenge S von V ist genau dann ein Erzeugendensystem von V, wenn λ_S surjektiv ist.

Beweis. Es sei eine Teilmenge S von V gegeben. Nach Bemerkung (2.76) und Lemma (2.80)(b) ist

$$\operatorname{Im}\lambda_S = \sum_{s\in S} Ks = \langle S\rangle.$$

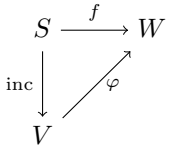
Somit ist S genau dann ein Erzeugendensystem von V, wenn $\operatorname{Im}\lambda_S = V$ ist, d.h. wenn λ_S surjektiv ist. □

Die nachfolgende Proposition besagt, dass Vektorraumhomomorphismen bereits eindeutig durch ihre Werte auf einem Erzeugendensystem festgelegt sind.

(2.92) Proposition. Es seien ein Körper K und ein K-Vektorraum V gegeben.

(a) Es sei ein parametrisiertes Erzeugendensystem $s = (s_i)_{i\in I}$ von V gegeben. Für jeden K-Vektorraum W und jede Familie $w = (w_i)_{i\in I}$ in W gibt es höchstens einen K-Vektorraumhomomorphismus $\varphi\colon V \to W$ mit $w_i = \varphi(s_i)$ für alle $i \in I$.

(b) Es sei ein Erzeugendensystem S von V gegeben. Für jeden K-Vektorraum W und jede Abbildung $f\colon S \to W$ gibt es höchstens einen K-Vektorraumhomomorphismus $\varphi\colon V \to W$ mit $f = \varphi|_S$.



Beweis.

(a) Es seien ein K-Vektorraum W und eine Familie $w = (w_i)_{i\in I}$ in W gegeben. Ferner sei $v \in V$ gegeben. Da s ein Erzeugendensystem von V ist, gibt es ein $a \in K^{(I)}$ mit $v = \sum_{i\in I} a_i s_i$. Wir erhalten

$$\varphi(v) = \varphi(\sum_{i\in I} a_i s_i) = \sum_{i\in I} a_i\,\varphi(s_i) = \sum_{i\in I} a_i w_i.$$

Da $v \in V$ beliebig war, ist φ somit durch w bereits eindeutig bestimmt.

(b) Dies folgt aus (a) und Bemerkung (2.88)(b). □

(2.93) Definition (endlich erzeugter Vektorraum)**.** Es sei ein Körper K gegeben. Ein K-Vektorraum heißt *endlich erzeugt*, falls er ein endliches Erzeugendensystem besitzt.

(2.94) Beispiel. Der $\mathbb{R}$-Vektorraum $\mathbb{R}^3$ ist endlich erzeugt.

Beweis. Nach Beispiel (2.87) ist $\{(1,0,0),(0,1,0),(0,0,1)\}$ ein endliches Erzeugendensystem von $\mathbb{R}^3$. □

Wir werden später beweisen können, dass für einen Körper K und eine unendliche Menge I stets K^I und auch schon $K^{(I)}$ nicht endlich erzeugte K-Vektorräume sind.

Lineare (Un)abhängigkeit

(2.95) Definition (lineare (Un)abhängigkeit)**.** Es seien ein Körper K und ein K-Vektorraum V gegeben.

(a) Eine Familie $s = (s_i)_{i\in I}$ in V heißt *linear unabhängig* über K (oder *K-linear unabhängig* oder *linear unabhängig*), wenn $\lambda_s\colon K^{(I)} \to V$ injektiv ist; ansonsten *linear abhängig* über K (oder *K-linear abhängig* oder *linear abhängig*).

(b) Eine Teilmenge S von V heißt *linear unabhängig* über K (oder *K-linear unabhängig* oder *linear unabhängig*), wenn $\lambda_S\colon K^{(S)} \to V$ injektiv ist; ansonsten *linear abhängig* über K (oder *K-linear abhängig* oder *linear abhängig*).

In einem Vektorraum V über einem Körper K sei eine Familie $s = (s_i)_{i\in I}$ gegeben. Genau dann ist s linear unabhängig, wenn sich jedes Element aus $\langle s\rangle = \sum_{i\in I} Ks_i$ eindeutig als Linearkombination von s zu einem $a \in K^{(I)}$ darstellen lässt. Mit anderen Worten: Genau dann ist s linear unabhängig, wenn aus $\sum_{i\in I} a_i s_i = \sum_{i\in I} b_i s_i$ für $a, b \in K^{(I)}$ (d.h. für $a_i, b_i \in K$ mit $a_i = 0$ und $b_i = 0$ für fast alle $i \in I$) stets $a = b$ (d.h. $a_i = b_i$ für alle $i \in I$) folgt. Insbesondere ist ein n-Tupel $t = (t_j)_{j\in[1,n]}$ in V für ein $n \in \mathbb{N}_0$ genau dann linear unabhängig, wenn aus $\sum_{j\in[1,n]} a_j t_j = \sum_{j\in[1,n]} b_j t_j$ für $a_j, b_j \in K$, $j \in [1,n]$ stets $a_j = b_j$ für $j \in [1,n]$ folgt.

(2.96) Bemerkung (Kriterium für lineare Unabhängigkeit)**.** Es seien ein Körper K, ein K-Vektorraum V und eine Familie $s = (s_i)_{i\in I}$ in V gegeben. Genau dann ist s linear unabhängig, wenn für $a \in K^{(I)}$ aus $\sum_{i\in I} a_i s_i = 0$ stets $a = 0$ folgt.

Beweis. Genau dann ist s linear unabhängig, wenn $\lambda_s\colon K^{(I)} \to V$, $a \mapsto \sum_{i\in I} a_i s_i$ injektiv ist. Nach Bemerkung (2.76) ist λ_s ein K-Vektorraumhomomorphismus. Somit ist λ_s genau dann injektiv, wenn $\operatorname{Ker}\lambda_s = \{0\}$ ist, siehe Lemma (2.63). Insgesamt ist daher s genau dann linear unabhängig, wenn für $a \in \operatorname{Ker}\lambda_s$, d.h. für $a \in K^{(I)}$ mit $\sum_{i\in I} a_i s_i = \lambda_s(a) = 0$, stets $a = 0$ folgt. □

Nach Bemerkung (2.96) ist eine Familie $s = (s_i)_{i\in I}$ in einem Vektorraum V über einem Körper K genau dann linear unabhängig, wenn sich die Null in V nur als Linearkombination von s zu $0 \in K^{(I)}$ darstellen lässt. Mit anderen Worten: Genau dann ist s linear unabhängig, wenn aus $\sum_{i\in i} a_i s_i = 0$ für $a \in K^{(I)}$ (d.h. für $a_i \in K$ mit $a_i = 0$ für fast alle $i \in I$) stets $a = 0$ (d.h. $a_i = 0$ für alle $i \in I$) folgt. Insbesondere ist ein n-Tupel $t = (t_j)_{j\in[1,n]}$ in V für ein $n \in \mathbb{N}_0$ genau dann linear unabhängig, wenn aus $\sum_{j\in[1,n]} a_j t_j = 0$ für $a_j \in K$, $j \in [1,n]$ stets $a_j = 0$ für $j \in [1,n]$ folgt.

(2.97) Beispiel.

(a) In $\mathbb{R}^3$ ist

$$\{(1,0,0),(0,1,0),(0,0,1)\}$$

linear unabhängig.

(b) In $\mathbb{R}^4$ ist

$$\{(3,-2,-3,4),(1,1,-1,1),(-1,-1,1,3),(-2,2,2,1)\}$$

linear abhängig und

$$\{(1,0,-1,0),(0,1,0,0),(0,0,0,1)\}$$

linear unabhängig.

(c) In $\mathbb{F}_3^{2\times 2}$ ist

$$\left\{\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}, \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}, \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}, \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\right\}$$

linear unabhängig.

Beweis.

(a) Es seien $a, b, c \in \mathbb{R}$ mit

$$a(1,0,0) + b(0,1,0) + c(0,0,1) = 0$$

gegeben. Dann ist $(a, b, c) = 0$. Somit ist

$$\{(1,0,0), (0,1,0), (0,0,1)\}$$

linear unabhängig in $\mathbb{R}^3$.

(b) Es ist

$$16(3,-2,-3,4) + (-27)(1,1,-1,1) + (-19)(-1,-1,1,3) + 20(-2,2,2,1) = (0,0,0,0),$$

aber $(16, -27, -19, 20) \neq (0,0,0,0)$. Somit ist

$$\{(3,-2,-3,4), (1,1,-1,1), (-1,-1,1,3), (-2,2,2,1)\}$$

linear abhängig in $\mathbb{R}^4$.
Es seien $a, b, c \in \mathbb{R}$ mit

$$a(1,0,-1,0) + b(0,1,0,0) + c(0,0,0,1) = 0$$

gegeben. Dann haben wir $(a, b, -a, c) = 0 = (0,0,0,0)$, also $a = 0$, $b = 0$, $c = 0$. Somit ist

$$\{(1,0,-1,0), (0,1,0,0), (0,0,0,1)\}$$

linear unabhängig in $\mathbb{R}^4$.

(c) Dies lässt sich analog zu (a) beweisen. □

(2.98) Bemerkung. Es seien ein Körper K und ein K-Vektorraum V gegeben. Dann ist $(\,)$ eine linear unabhängige Familie von V.

Beweis. Es ist $K^{(\emptyset)} = K^{\emptyset} = \{0\}$ und damit $\lambda_\emptyset \colon K^{(\emptyset)} \to V$ notwendigerweise injektiv. □

(2.99) Bemerkung. Es seien ein Körper K, ein K-Vektorraum V, eine Familie $s = (s_i)_{i\in I}$ in V und eine Teilmenge J von I gegeben. Wenn s linear unabhängig ist, dann ist auch $s|_J = (s_j)_{j\in J}$ linear unabhängig.

Beweis. Es sei s linear unabhängig und es sei $a \in K^{(J)}$ mit $\sum_{j\in J} a_j s_j = 0$ gegeben. Dann ist

$$\sum_{j\in J} a_j s_j + \sum_{i\in I\setminus J} 0 s_i = \sum_{j\in J} a_j s_j = 0.$$

Da aber s linear unabhängig ist, folgt $a_j = 0$ für alle $j \in J$. Somit ist auch $s|_J$ linear unabhängig. □

(2.100) Korollar. Es seien ein Körper K, ein K-Vektorraum V und eine Familie $s = (s_i)_{i\in I}$ von V gegeben. Wenn es ein $i \in I$ mit $s_i = 0$ gibt, dann ist s linear abhängig.

Beweis. Es sei $i \in I$ mit $s_i = 0$ gegeben. Dann ist $1^K \cdot 0^V = 0^V$, aber $1^K \neq 0^K$. Somit ist $s|_{\{i\}}$ linear abhängig und damit auch s linear abhängig nach Bemerkung (2.99). □

(2.101) Bemerkung. Es seien ein Körper K, ein K-Vektorraum V, eine Familie $s = (s_i)_{i\in I}$ in V und ein $i \in I$ gegeben. Wenn s_i eine Linearkombination von $s|_{I\setminus\{i\}}$ ist, dann ist s linear abhängig.

Beweis. Es sei s_i eine Linearkombination von $s|_{I\setminus\{i\}}$. Dann gibt es ein $a \in K^{(I\setminus\{i\})}$ mit $s_i = \sum_{j\in I\setminus\{i\}} a_j s_j$ und also mit $\sum_{j\in I\setminus\{i\}} a_j s_j + (-1)s_i = 0$. Wegen $-1 \neq 0$ ist s daher linear abhängig. □

(2.102) Bemerkung. Es seien ein Körper K und ein K-Vektorraum V gegeben.

(a) Eine Familie $s = (s_i)_{i\in I}$ in V ist genau dann linear unabhängig, wenn $\{s_i \mid i \in I\}$ linear unabhängig ist und die Einträge von s verschieden sind.

(b) Eine Teilmenge S von V ist genau dann linear unabhängig, wenn $(s)_{s\in S}$ linear unabhängig ist.

Beweis.

(a) Es sei eine Familie $s = (s_i)_{i\in I}$ in V gegeben. Wenn $\{s_i \mid i \in I\}$ linear unabhängig ist und die Einträge von s verschieden sind, dann ist $I \to \{s_i \mid i \in I\}$, $i \mapsto s_i$ eine Bijektion und daher auch s linear unabhängig.

Es sei umgekehrt $\{s_i \mid i \in I\}$ linear abhängig. Wir wählen eine Teilmenge J von I so, dass es für jedes $i \in I$ ein $j \in J$ mit $s_i = s_j$ gibt, und so, dass die Einträge von $s|_J$ verschieden sind (d.h. wir wählen eine Transversale bzgl. der Bildgleichheit der Abbildung $I \to V$, $i \mapsto s_i$). Dann ist $\{s_j \mid j \in J\} = \{s_i \mid i \in I\}$ linear abhängig und $J \to \{s_j \mid j \in J\}$, $j \mapsto s_j$ eine Bijektion, also auch $s|_J$ linear abhängig. Nach Bemerkung (2.99) folgt die lineare Abhängigkeit von s.

Schließlich seien die Einträge von s nicht verschieden, d.h. es gebe $i, i' \in I$ mit $i \neq i'$ und $s_i = s_{i'}$. Dann gilt $1s_i + (-1)s_{i'} = 0$, es ist also $s|_{\{i,i'\}}$ linear abhängig und damit auch s nach Bemerkung (2.99).

Im Umkehrschluss gilt daher: Wenn s linear unabhängig in V ist, dann ist auch $\{s_i \mid i \in I\}$ linear unabhängig und die Einträge von s sind verschieden.

(b) Es sei eine Teilmenge S von V gegeben. Da die Einträge von $(s)_{s\in S}$ stets verschieden sind, ist $(s)_{s\in S}$ nach (a) genau dann linear unabhängig, wenn $\{s \mid s \in S\} = S$ linear unabhängig ist. □

(2.103) Beispiel. In $\mathbb{R}^3$ ist $\{(1,0,0),(0,1,0),(1,0,0)\}$ linear unabhängig und $((1,0,0),(0,1,0),(1,0,0))$ linear abhängig.

(2.104) Bemerkung. Es seien ein Körper K und ein K-Vektorraum V gegeben. Genau dann ist (v) linear unabhängig, wenn $v \neq 0$ ist.

Beweis. Wenn (v) linear unabhängig ist, dann ist $v \neq 0$ nach Korollar (2.100). Es sei also umgekehrt $v \neq 0$. Nach Lemma (2.44) folgt dann aus $av = 0$ stets $a = 0$. Somit ist (v) nach Bemerkung (2.96) linear unabhängig. □

(2.105) Proposition. Es seien ein Körper K, ein K-Vektorraum V und eine Familie $s = (s_i)_{i\in I}$ in V gegeben.

(a) Genau dann ist s linear abhängig, wenn es ein $i \in I$ so gibt, dass s_i eine Linearkombination von $s|_{I\setminus\{i\}}$ ist.

(b) Es sei ein $i \in I$ so gegeben, dass $s|_{I\setminus\{i\}}$ linear unabhängig ist. Genau dann ist s linear abhängig, wenn s_i eine Linearkombination von $s|_{I\setminus\{i\}}$ ist.

Beweis.

(a) Zunächst sei s linear abhängig, so dass es ein $a \in K^{(I)}\setminus\{0\}$ mit $\sum_{j\in I} a_j s_j = 0$ gibt. Wegen $a \neq 0$ ist $a_i \neq 0$ für ein $i \in I$. Aus $0 = \sum_{j\in I} a_j s_j = \sum_{j\in I\setminus\{i\}} a_j s_j + a_i s_i$ folgt nun

$$s_i = -a_i^{-1} \sum_{j\in I\setminus\{i\}} a_i s_i = \sum_{j\in I\setminus\{i\}} (-a_i^{-1} a_j) s_j,$$

d.h. s_i ist eine Linearkombination von $s|_{I\setminus\{i\}}$.

Gibt es umgekehrt ein $i \in I$ derart, dass s_i eine Linearkombination von $s|_{I\setminus\{i\}}$ ist, so ist s linear abhängig nach Bemerkung (2.101).

(b) Zunächst sei s_i keine Linearkombination von $s|_{I\setminus\{i\}}$. Um zu zeigen, dass s linear unabhängig ist, sei $a \in K^{(I)}$ mit $\sum_{j\in I} a_j s_j = 0$ gegeben. Dann gilt $\sum_{j\in I\setminus\{i\}} a_j s_j + a_i s_i = 0$, also

$$a_i s_i = -\sum_{j\in I\setminus\{i\}} a_j s_j = \sum_{j\in I\setminus\{i\}} (-a_j) s_j.$$

Da s_i keine Linearkombination von $s|_{I\setminus\{i\}}$ ist, folgt $a_i = 0$. Somit haben wir $\sum_{j\in I\setminus\{i\}} a_j s_j = 0$ und die lineare Unabhängigkeit von $s|_{I\setminus\{i\}}$ liefert $a_j = 0$ für alle $j \in I \setminus \{i\}$. Insgesamt ist s daher linear unabhängig.

Ist umgekehrt s_i eine Linearkombination von $s|_{j\in I\setminus\{i\}}$, so ist s linear abhängig nach Bemerkung (2.101). □

Basen

(2.106) Definition (Basis)**.** Es seien ein Körper K und ein K-Vektorraum V gegeben.

(a) Eine Familie $s = (s_i)_{i\in I}$ in V heißt (*parametrisierte*) *Basis* über K (oder (*parametrisierte*) *K-Basis* oder (*parametrisierte*) *Basis*) von V, wenn $\lambda_s\colon K^{(I)} \to V$ bijektiv ist.

(b) Eine Teilmenge S von V heißt *Basis* über K (oder *K-Basis* oder *Basis*) von V, wenn $\lambda_S\colon K^{(S)} \to V$ bijektiv ist.

In einem Vektorraum V über einem Körper K sei eine Familie $s = (s_i)_{i\in I}$ gegeben. Genau dann ist s eine parametrisierte Basis von V, wenn sich jeder Vektor in V eindeutig als Linearkombination von s schreiben lässt. Mit anderen Worten: Genau dann ist s eine parametrisierte Basis, wenn für jedes $v \in V$ ein $a \in K^{(I)}$ (d.h. $a_i \in K$ mit $a_i = 0$ für fast alle $i \in I$) mit $v = \sum_{i\in I} a_i s_i$ existiert und wenn aus $\sum_{i\in I} a_i s_i = \sum_{i\in I} b_i s_i$ für $a, b \in K^{(I)}$ stets $a = b$ (d.h. $a_i = b_i$ für alle $i \in I$) folgt. Insbesondere ist ein n-Tupel $t = (t_j)_{j\in[1,n]}$ in V für ein $n \in \mathbb{N}_0$ genau dann eine parametrisierte Basis von V, wenn für jedes $v \in V$ stets $a_j \in K$ für $j \in [1, n]$ mit $v = \sum_{j\in[1,n]} a_j t_j$ existieren und wenn aus $\sum_{j\in[1,n]} a_j t_j = \sum_{j\in[1,n]} b_j t_j$ für $a_j, b_j \in K$, $j \in [1, n]$ stets $a_j = b_j$ für $j \in [1, n]$ folgt.

(2.107) Bemerkung. Es seien ein Körper K und ein K-Vektorraum V gegeben.

(a) Eine Familie $s = (s_i)_{i\in I}$ in V ist genau dann eine Basis von V, wenn $\{s_i \mid i \in I\}$ eine Basis von V ist und die Einträge von s verschieden sind.

(b) Eine Teilmenge S von V ist genau dann eine Basis von V, wenn $(s)_{s\in S}$ eine Basis von V ist.

Beweis.

(a) Dies folgt aus Bemerkung (2.88)(a) und Bemerkung (2.102)(a).

(b) Dies folgt aus Bemerkung (2.88)(b) und Bemerkung (2.102)(b). □

(2.108) Bemerkung. Es seien ein Körper K, ein K-Vektorraum V und eine Teilmenge S von V gegeben. Die folgenden Bedingungen sind äquivalent.

(a) Es ist S eine Basis von V.

(b) Es ist S ein linear unabhängiges Erzeugendensystem von V.

(c) Es ist $\lambda_S\colon K^{(S)} \to V$ ein K-Vektorraumisomorphismus.

Beweis. Genau dann ist S eine Basis von V, wenn $\lambda_S\colon K^{(S)} \to V$ bijektiv, d.h. injektiv und surjektiv, ist. Nun ist λ_S nach Definition (2.95)(b) aber genau dann injektiv, wenn S linear unabhängig ist, sowie nach Bemerkung (2.91) genau dann surjektiv, wenn S ein Erzeugendensystem von V ist. Insgesamt ist S genau dann eine Basis von V, wenn S ein linear unabhängiges Erzeugendensystem von V ist. Somit sind Bedingung (a) und Bedingung (b) äquivalent.
Nach Bemerkung (2.76) ist $\lambda_S\colon K^{(S)} \to V$ stets ein Homomorphismus. Dies bedeutet nach Bemerkung (2.40) aber, dass λ_S genau dann bijektiv ist, wenn es ein Isomorphismus ist. Folglich sind auch Bedingung (a) und Bedingung (c) äquivalent.
Insgesamt sind Bedingung (a), Bedingung (b) und Bedingung (c) äquivalent. □

(2.109) Beispiel.

(a) Es ist

$$\{(1,0,0),(0,1,0),(0,0,1)\}$$

eine Basis von $\mathbb{R}^3$.

(b) Es ist $\{(1,0,-1,0),(0,1,0,0),(0,0,0,1)\}$ eine Basis des Unterraums

$$\langle(3,-2,-3,4),(1,1,-1,1),(-1,-1,1,3),(-2,2,2,1)\rangle$$

von $\mathbb{R}^4$.

(c) Es ist

$$\left\{\begin{pmatrix}1&0\\0&0\end{pmatrix},\begin{pmatrix}0&1\\0&0\end{pmatrix},\begin{pmatrix}0&0\\1&0\end{pmatrix},\begin{pmatrix}0&0\\0&1\end{pmatrix}\right\}$$

eine Basis von $\mathbb{F}_3^{2\times 2}$.

Beweis.

(a) Dies folgt aus Beispiel (2.87)(a), Beispiel (2.97)(a) und Bemerkung (2.108).

(b) Dies folgt aus Beispiel (2.87)(b), Beispiel (2.97)(b) und Bemerkung (2.108).

(c) Dies folgt aus Beispiel (2.87)(c), Beispiel (2.97)(c) und Bemerkung (2.108). □

(2.110) Bemerkung. Es sei ein Körper K gegeben. Dann ist $\emptyset$ eine Basis von $\{0\}$.

Beweis. Es ist $\emptyset$ ein Erzeugendensystem von $\{0\}$ nach Korollar (2.71)(a). Ferner ist $\emptyset$ linear unabhängig nach Bemerkung (2.98) und Bemerkung (2.102)(b). Folglich ist $\emptyset$ eine Basis von $\{0\}$ nach Bemerkung (2.108). □

Nach Proposition (2.92) wissen wir, dass Vektorraumhomomorphismen durch ihre Werte auf Erzeugendensystemen eindeutig bestimmt sind. Nun zeigen wir, dass auf einer Basis sich sogar jede Vorgabe von Werten zu einem Vektorraumhomomorphismus fortsetzen lässt.

(2.111) Proposition. Es seien ein Körper K und ein K-Vektorraum V gegeben.

(a) Es sei eine parametrisierte Basis $s = (s_i)_{i\in I}$ von V gegeben. Für jeden K-Vektorraum W und jede Familie $w = (w_i)_{i\in I}$ in W gibt es genau einen K-Vektorraumhomomorphismus $\varphi\colon V \to W$ mit $w_i = \varphi(s_i)$ für alle $i \in I$, gegeben durch

$$\varphi = \lambda_w \circ \lambda_s^{-1}.$$

Für $v \in V$, $a \in K^{(I)}$ mit $v = \lambda_s(a)$ ist

$$\varphi(v) = \sum_{i\in I} a_i w_i.$$

(b) Es sei eine Basis S von V gegeben. Für jeden K-Vektorraum W und jede Abbildung $f\colon S \to W$ gibt es genau einen K-Vektorraumhomomorphismus $\varphi\colon V \to W$ mit $f = \varphi|_S$, gegeben durch

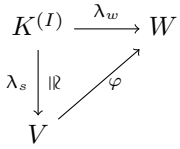
$$\varphi(v) = \sum_{s\in S} a_s\, f(s)$$

für $v \in V$, $a \in K^{(S)}$ mit $v = \lambda_S(a)$.

$$\begin{array}{ccc} S & \xrightarrow{f} & W \\ {\scriptstyle \mathrm{inc}}\downarrow & \nearrow_{\varphi} & \\ V & & \end{array}$$

Beweis.

(a) Es seien ein K-Vektorraum W und eine Familie $w = (w_i)_{i\in I}$ in W gegeben. Nach Proposition (2.92)(a) gibt es höchstens einen Homomorphismus $\varphi\colon V \to W$ mit $w_i = \varphi(s_i)$ für alle $i \in I$. Wir müssen also lediglich die Existenz eines solchen Homomorphismus zeigen. Es ist s eine Basis von V, also $\lambda_s\colon K^{(I)} \to V$, $a \mapsto \sum_{i\in I} a_i s_i$ ein Isomorphismus nach Bemerkung (2.108). Ferner ist $\lambda_w\colon K^{(I)} \to W$, $a \mapsto \sum_{i\in I} a_i f(s_i)$ ein Homomorphismus nach Bemerkung (2.76). Aus Bemerkung (2.37)(a) folgt nun, dass dann auch $\varphi := \lambda_w \circ \lambda_s^{-1}$ ein Homomorphismus ist.



Für $v \in V$, $a \in K^{(I)}$ mit $v = \lambda_s(a)$ gilt

$$\varphi(v) = \lambda_w(\lambda_s^{-1}(v)) = \lambda_w(a) = \sum_{i\in I} a_i w_i.$$

Insbesondere gilt für $i \in I$ stets $s_i = \lambda_s((\delta_{i,j})_{j\in I})$ und damit

$$\varphi(s_i) = \sum_{j\in I} \delta_{i,j} w_j = w_i.$$

(b) Dies folgt aus (a) und Bemerkung (2.107)(b). □

(2.112) Beispiel. Es gibt genau einen $\mathbb{F}_5$-Vektorraumhomomorphismus $\varphi\colon \mathbb{F}_5^{2\times 2} \to \mathbb{F}_5^{2\times 1}$ mit

$$\varphi(\begin{pmatrix}1&0\\0&0\end{pmatrix}) = \begin{pmatrix}1\\2\end{pmatrix},\ \varphi(\begin{pmatrix}0&1\\0&0\end{pmatrix}) = \begin{pmatrix}0\\-1\end{pmatrix},\ \varphi(\begin{pmatrix}0&0\\1&0\end{pmatrix}) = \begin{pmatrix}0\\0\end{pmatrix},\ \varphi(\begin{pmatrix}0&0\\0&1\end{pmatrix}) = \begin{pmatrix}2\\-2\end{pmatrix},$$

gegeben durch

$$\varphi(\begin{pmatrix}a&b\\c&d\end{pmatrix}) = \begin{pmatrix}a+2d\\2a-b-2d\end{pmatrix}$$

für $a, b, c, d \in \mathbb{F}_5$.

Beweis. Nach Beispiel (2.109)(c) ist

$$\{\begin{pmatrix}1&0\\0&0\end{pmatrix}, \begin{pmatrix}0&1\\0&0\end{pmatrix}, \begin{pmatrix}0&0\\1&0\end{pmatrix}, \begin{pmatrix}0&0\\0&1\end{pmatrix}\}$$

eine Basis von $\mathbb{F}_5^{2\times 2}$. Somit gibt es nach Proposition (2.111)(b) genau einen Homomorphismus $\varphi\colon \mathbb{F}_5^{2\times 2} \to \mathbb{F}_5^{2\times 1}$ mit

$$\varphi(\begin{pmatrix}1&0\\0&0\end{pmatrix}) = \begin{pmatrix}1\\2\end{pmatrix},\ \varphi(\begin{pmatrix}0&1\\0&0\end{pmatrix}) = \begin{pmatrix}0\\-1\end{pmatrix},\ \varphi(\begin{pmatrix}0&0\\1&0\end{pmatrix}) = \begin{pmatrix}0\\0\end{pmatrix},\ \varphi(\begin{pmatrix}0&0\\0&1\end{pmatrix}) = \begin{pmatrix}2\\-2\end{pmatrix},$$

gegeben durch

$$\begin{aligned}\varphi(\begin{pmatrix}a&b\\c&d\end{pmatrix}) &= \varphi(a\begin{pmatrix}1&0\\0&0\end{pmatrix} + b\begin{pmatrix}0&1\\0&0\end{pmatrix} + c\begin{pmatrix}0&0\\1&0\end{pmatrix} + d\begin{pmatrix}0&0\\0&1\end{pmatrix})\\ &= a\begin{pmatrix}1\\2\end{pmatrix} + b\begin{pmatrix}0\\-1\end{pmatrix} + c\begin{pmatrix}0\\0\end{pmatrix} + d\begin{pmatrix}2\\-2\end{pmatrix} = \begin{pmatrix}a+2d\\2a-b-2d\end{pmatrix}\end{aligned}$$

für $a, b, c, d \in \mathbb{F}_5$. □

(2.113) Proposition. Es seien ein Körper K, Vektorräume V und W über K, eine parametrisierte Basis $s = (s_i)_{i\in I}$ von V und eine Familie $w = (w_i)_{i\in I}$ in W gegeben. Ferner bezeichne $\varphi\colon V \to W$ den eindeutig bestimmten K-Vektorraumhomomorphismus mit $\varphi(s_i) = w_i$ für alle $i \in I$.

(a) Genau dann ist φ surjektiv, wenn w ein Erzeugendensystem von W ist.

(b) Genau dann ist φ injektiv, wenn w linear unabhängig in W ist.

(c) Genau dann ist φ ein Isomorphismus, wenn w eine Basis von W ist.

Beweis. Nach Proposition (2.111)(a) ist $\varphi = \lambda_w \circ \lambda_s^{-1}$, wobei λ_s^{-1} ein Isomorphismus und damit insbesondere bijektiv ist.

(a) Genau dann ist φ surjektiv, wenn λ_w surjektiv ist, nach Bemerkung (2.91) also genau dann, wenn w ein Erzeugendensystem von W ist.

(b) Genau dann ist φ injektiv, wenn λ_w injektiv ist, d.h. wenn w linear unabhängig in W ist.

(c) Nach Bemerkung (2.40) ist φ genau dann ein Isomorphismus, wenn φ bijektiv ist. Dies gilt aber genau dann, wenn λ_w bijektiv ist, d.h. wenn w eine Basis von W ist. □

(2.114) Lemma. Es seien ein Körper K, ein K-Vektorraum V und eine Teilmenge S von V gegeben. Die folgenden Bedingungen sind äquivalent.

(a) Es ist S eine Basis von V.

(b) Es ist S eine bzgl. Inklusion maximale linear unabhängige Teilmenge von V.

(c) Es ist S ein bzgl. Inklusion minimales Erzeugendensystem von V.

Beweis. Es gelte zunächst Bedingung (a), d.h. es sei S eine Basis von V. Dann ist S insbesondere eine linear unabhängige Teilmenge von V nach Bemerkung (2.108). Wegen der Surjektivität von $\lambda_S\colon K^{(S)} \to V$ ist ferner jedes $v \in V \setminus S$ eine Linearkombination von S. Dies impliziert nach Bemerkung (2.101) aber bereits die lineare Abhängigkeit von $S \cup \{v\}$ für alle $v \in V \setminus S$ (und damit insbesondere die lineare Abhängigkeit jeder Teilmenge T von V mit $S \subset T$ nach Bemerkung (2.99) und Bemerkung (2.102)(b)). Folglich ist S eine bzgl. Inklusion maximale linear unabhängige Teilmenge von V, d.h. Bedingung (b) ist erfüllt.
Als nächstes gelte Bedingung (b), d.h. es sei S eine bzgl. Inklusion maximale linear unabhängige Teilmenge von V. Für $v \in V \setminus S$ ist dann $S \cup \{v\}$ eine linear abhängige Teilmenge von V wegen der Maximalität von S, also $v \in \sum_{s\in S} Ks = \langle S\rangle$ nach Proposition (2.105)(b) und Lemma (2.80)(b). Somit ist $V \setminus S \subseteq \langle S\rangle$. Da nach Bemerkung (2.70) aber auch $S \subseteq \langle S\rangle$ ist, haben wir insgesamt $V = \langle S\rangle$, d.h. S ist ein Erzeugendensystem von V.
Um zu zeigen, dass S ein bzgl. Inklusion minimales Erzeugendensystem von V ist, sei ein $s \in S$ gegeben. Wegen der linearen Unabhängigkeit von S ist dann s keine Linearkombination von $S \setminus \{s\}$ nach Proposition (2.105)(a), also $s \notin \sum_{t\in S\setminus\{s\}} Kt = \langle S \setminus \{s\}\rangle$ nach Lemma (2.80)(b). Insbesondere ist $V \neq \langle S \setminus \{s\}\rangle$, d.h. $S \setminus \{s\}$ ist kein Erzeugendensystem von V. Mit Korollar (2.72) folgt, dass jede echte Teilmenge T von S kein Erzeugendensystem von V ist. Folglich ist S ein minimales Erzeugendensystem von V, d.h. Bedingung (c) ist erfüllt.
Schließlich gelte Bedingung (c), d.h. es sei S ein bzgl. Inklusion minimales Erzeugendensystem von V. Für alle $s \in S$ ist dann $S \setminus \{s\}$ kein Erzeugendensystem von V, d.h. es ist $\langle S \setminus \{s\}\rangle \subset V = \langle S\rangle$ und damit s keine Linearkombination von $S \setminus \{s\}$ nach Proposition (2.82). Dies impliziert nach Proposition (2.105)(a) aber bereits die lineare Unabhängigkeit von S. Somit ist S ein linear unabhängiges Erzeugendensystem und damit eine Basis von V nach Bemerkung (2.108), d.h. Bedingung (a) ist erfüllt.
Insgesamt sind Bedingung (a), Bedingung (b) und Bedingung (c) äquivalent. □

(2.115) Proposition. Es seien ein Körper K, ein K-Vektorraumhomomorphismus $\varphi\colon V \to W$ und eine parametrisierte Basis $s = (s_i)_{i\in I}$ von V gegeben. Ferner sei J eine Teilmenge von I so gegeben, dass $s|_J$ eine Basis von $\operatorname{Ker}\varphi$ ist. Dann ist $\varphi \circ s|_{I\setminus J} = (\varphi(s_i))_{i\in I\setminus J}$ eine parametrisierte Basis von $\operatorname{Im}\varphi$.

Beweis. Auf Grund der Surjektivität von $\varphi|^{\operatorname{Im}\varphi}\colon V \to \operatorname{Im}\varphi$ ist $(\varphi(s_i))_{i\in I}$ nach Proposition (2.113)(a) ein Erzeugendensystem von $\operatorname{Im}\varphi$. Da aber $\varphi(s_j) = 0$ für alle $j \in J$, ist sogar $(\varphi(s_i))_{i\in I\setminus J}$ ein Erzeugendensystem von $\operatorname{Im}\varphi$ nach Proposition (2.82).
Um zu zeigen, dass $(\varphi(s_i))_{i\in I\setminus J}$ linear unabhängig ist, sei ein $a \in K^{(I\setminus J)}$ mit $\sum_{i\in I\setminus J} a_i\,\varphi(s_i) = 0$ gegeben. Wir erhalten

$$0 = \sum_{i\in I\setminus J} a_i\,\varphi(s_i) = \varphi\Big(\sum_{i\in I\setminus J} a_i s_i\Big),$$

d.h. es ist $\sum_{i\in I\setminus J} a_i s_i \in \operatorname{Ker}\varphi$. Da $s|_J$ als Basis insbesondere ein Erzeugendensystem von $\operatorname{Ker}\varphi$ ist, gibt es ein $b \in K^{(J)}$ mit $\sum_{i\in I\setminus J} a_i s_i = \sum_{j\in J} b_j s_j$. Es folgt

$$0 = \sum_{i\in I\setminus J} a_i s_i - \sum_{j\in J} b_j s_j = \sum_{i\in I\setminus J} a_i s_i + \sum_{j\in J} (-b_j) s_j,$$

also $a_i = 0$ für $i \in I \setminus J$ und $b_j = 0$ für $j \in J$ auf Grund der linearen Unabhängigkeit von s. Folglich ist $(\varphi(s_i))_{i\in I\setminus J}$ linear unabhängig.
Insgesamt ist $(\varphi(s_i))_{i\in I\setminus J}$ ein linear unabhängiges Erzeugendensystem von $\operatorname{Im}\varphi$, nach Bemerkung (2.108) also eine Basis von $\operatorname{Im}\varphi$. □

(2.116) Korollar. Es seien ein Körper K und ein K-Vektorraumisomorphismus $\varphi\colon V \to W$ gegeben. Für jede parametrisierte Basis $s = (s_i)_{i\in I}$ von V ist $(\varphi(s_i))_{i\in I}$ eine Basis von W.

Beweis. Es sei eine parametrisierte Basis $s = (s_i)_{i\in I}$ von V gegeben. Da φ ein K-Vektorraumisomorphismus ist, gilt $\operatorname{Ker}\varphi = \{0\}$ und $\operatorname{Im}\varphi = W$ nach Korollar (2.64). Folglich ist $(s_j)_{j\in\emptyset} = (\,)$ eine Basis von $\operatorname{Ker}\varphi$ nach Bemerkung (2.110) und somit $(\varphi(s_i))_{i\in I\setminus\emptyset} = (\varphi(s_i))_{i\in I}$ eine Basis von $\operatorname{Im}\varphi = W$ nach Proposition (2.115). □

Standardbasis

(2.117) Beispiel. Es seien eine Menge I und ein Körper K gegeben. Dann ist $\mathrm{e} = (\mathrm{e}_i)_{i\in I}$ definiert durch

$$\mathrm{e}_i = (\delta_{i,j})_{j\in I}$$

eine parametrisierte Basis von $K^{(I)}$.

Beweis. Für $a \in K^{(I)}$ gilt

$$\lambda_{\mathrm{e}}(a) = \sum_{i\in I} a_i \mathrm{e}_i = \sum_{i\in I} a_i (\delta_{i,j})_{j\in I} = (\sum_{i\in I} a_i \delta_{i,j})_{j\in I} = (a_j)_{j\in I} = a,$$

d.h. es ist $\lambda_{\mathrm{e}} = \mathrm{id}_{K^{(I)}}$. Insbesondere ist λ_{e} eine Bijektion und damit e eine Basis von $K^{(I)}$. □

(2.118) Definition (Standardbasis)**.** Es seien eine Menge I und ein Körper K gegeben. Die Basis $\mathrm{e} = \mathrm{e}^{K^{(I)}} = (\mathrm{e}_i^{K^{(I)}})_{i\in I}$ aus Beispiel (2.117) heißt *Standardbasis* von $K^{(I)}$.

In Beispiel (2.109)(a), (c) haben wir Standardbasen von $\mathbb{R}^3$ bzw. $\mathbb{F}_3^{2\times 2}$ (aufgefasst als Mengen) betrachtet.
Die Standardbasis von $K^n = K^{([1,n])}$ ist gegeben durch

$$\mathrm{e} = (\mathrm{e}_1, \ldots, \mathrm{e}_n) = ((1,0,\ldots,0,0), \ldots, (0,0,\ldots,0,1)).$$

(2.119) Notation. Es seien $n \in \mathbb{N}_0$ und ein Körper K gegeben.

(a) Für $i \in [1,n]$ schreiben wir $\mathrm{e}_i = \mathrm{e}_i^{K^{n\times 1}} := \mathrm{e}_{i,1}^{K^{n\times 1}}$.

(b) Für $i \in [1,n]$ schreiben wir $\mathrm{e}_i = \mathrm{e}_i^{K^{1\times n}} := \mathrm{e}_{1,i}^{K^{1\times n}}$.

Aufgaben

Aufgabe 68 (Erzeugnis)**.** Es seien ein Körper K, ein K-Vektorraumhomomorphismus $\varphi\colon V \to W$ und eine Familie $s = (s_i)_{i\in I}$ in V gegeben. Zeigen Sie, dass

$$\varphi(\langle s_i \mid i \in I\rangle) = \langle \varphi(s_i) \mid i \in I\rangle$$

ist.

Aufgabe 69 (Erzeugendensysteme)**.** Es sei ein Körper K gegeben und es sei $\varphi\colon K^{2\times 2} \to K^{2\times 2}$ definiert durch

$$\varphi(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) := \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

für $a, b, c, d \in K$. Zeigen Sie, dass φ ein K-Vektorraumhomomorphismus ist und bestimmen Sie Erzeugendensysteme von $\operatorname{Ker}\varphi$ und $\operatorname{Im}\varphi$ mit möglichst wenig Elementen.

Aufgabe 70 (lineare Unabhängigkeit)**.** Es sei ein Körper K gegeben.

(a) Es seien ein K-Vektorraum V, ein K-Vektorraumhomomorphismus $\varphi\colon V \to V$ und ein $v \in V$ gegeben. Ferner sei $n := \min\{k \in \mathbb{N}_0 \mid \varphi^k(v) = 0\}$. Zeigen Sie, dass $(\varphi^k(v))_{k\in[0,n-1]}$ linear unabhängig ist.

(b) Für welche $(a, b, c) \in K^3$ ist

$$\left\{\begin{pmatrix}1\\a\\a^2\end{pmatrix}, \begin{pmatrix}1\\b\\b^2\end{pmatrix}, \begin{pmatrix}1\\c\\c^2\end{pmatrix}\right\}$$

linear unabhängig in $K^{3\times 1}$?

Aufgabe 71 (lineare Unabhängigkeit von irrationalen Zahlen)**.** Zeigen Sie:

(a) Es ist

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

ein $\mathbb{Q}$-Untervektorraum von $\mathbb{R}$.

(b) Es ist $\sqrt{3} \notin \mathbb{Q}[\sqrt{2}]$.

(c) Es ist $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ linear unabhängig in $\mathbb{R}$ über $\mathbb{Q}$.

Aufgabe 72 (lineare Unabhängigkeit für Abbildungen)**.**

(a) Es seien ein Körper K, ein K-Vektorraumhomomorphismus $\varphi\colon V \to W$ und eine Familie $s = (s_i)_{i\in I}$ in V gegeben. Zeigen Sie: Wenn $(\varphi(s_i))_{i\in I}$ linear unabhängig in W ist, dann ist $(s_i)_{i\in I}$ linear unabhängig in V.

(b) Es seien eine Menge X, ein n-Tupel $x = (x_i)_{i\in[1,n]}$ in X und ein Körper K gegeben. Zeigen Sie, dass $\varphi\colon \mathrm{Map}(X, K) \to K^n$, $f \mapsto (f(x_i))_{i\in[1,n]}$ ein K-Vektorraumhomomorphismus ist.

(c) Zeigen Sie, dass $(x \mapsto 1, x \mapsto x, x \mapsto x^2)$ linear unabhängig in $\mathrm{Map}(\mathbb{R}, \mathbb{R})$ ist.

(d) Zeigen Sie, dass $(\sin, \cos)$ linear unabhängig in $\mathrm{Map}(\mathbb{R}, \mathbb{R})$ ist.

5 Dimension

Existenz von Basen

(2.120) Satz (Basisauswahlergänzungssatz)**.** Es seien ein Körper K und ein endlich erzeugter K-Vektorraum V gegeben. Für jede linear unabhängige Teilmenge S in V und jedes endliche Erzeugendensystem T von V gibt es eine Teilmenge T' von T so, dass $S \cup T'$ eine Basis von V ist.

Beweis. Es sei eine linear unabhängige Teilmenge S von V und ein endliches Erzeugendensystem T von V gegeben. Wegen der Endlichkeit von T gibt es eine bzgl. Inklusion maximale Teilmenge T' von T so, dass $S \cup T'$ eine linear unabhängige Teilmenge von V ist. Wir wollen zeigen, dass $S \cup T'$ ein Erzeugendensystem von V ist. Für $t \in T \setminus T'$ ist $S \cup T' \cup \{t\}$ wegen der Maximalität von $S \cup T'$ eine linear abhängige Teilmenge von V und damit $t \in \langle S \cup T'\rangle$ nach Proposition (2.105)(b) und Lemma (2.80)(b). Somit ist $T \setminus T' \subseteq \langle S \cup T'\rangle$. Nach Bemerkung (2.70) ist aber auch $T' \subseteq \langle S \cup T'\rangle$, also $T = (T \setminus T') \cup T' \subseteq \langle S \cup T'\rangle$ und folglich $V = \langle T\rangle \subseteq \langle S \cup T'\rangle$. Somit ist $S \cup T'$ in der Tat ein Erzeugendensystem von V, und auf Grund der linearen Unabhängigkeit also sogar eine Basis von V nach Bemerkung (2.108). □

(2.121) Korollar (Basisauswahlsatz)**.** Es seien ein Körper K und ein endlich erzeugter K-Vektorraum V gegeben. Für jedes endliche Erzeugendensystem S von V gibt es eine Teilmenge S' von S so, dass S' eine Basis von V ist.

Beweis. Es sei ein endliches Erzeugendensystem S von V gegeben. Da $\emptyset$ nach Bemerkung (2.98) und Bemerkung (2.102)(b) eine linear unabhängige Teilmenge von V ist, gibt es nach Satz (2.120) eine Teilmenge S' von S so, dass $S' = \emptyset \cup S'$ eine Basis von V ist. □

Der Basisauswahlsatz (2.121) besagt also, dass sich aus jedem endlichen Erzeugendensystem eines endlich erzeugten Vektorraums eine Basis auswählen lässt.

(2.122) Korollar. Es sei ein Körper K und ein endlich erzeugter K-Vektorraum V gegeben. Dann gibt es eine endliche Basis von V.

Beweis. Da V endlich erzeugt ist, gibt es ein endliches Erzeugendensystem S von V. Nach dem Basisauswahlsatz (2.121) gibt es eine Teilmenge S' von S so, dass S' eine Basis von V ist. Die Endlichkeit von S impliziert die Endlichkeit von S'. □

(2.123) Korollar (Basisergänzungssatz)**.** Es seien ein Körper K und ein endlich erzeugter K-Vektorraum V gegeben. Für jede linear unabhängige Teilmenge S von V gibt es eine Basis S' von V so, dass S eine Teilmenge von S' ist.

Beweis. Es sei eine linear unabhängige Teilmenge S von V gegeben. Da V endlich erzeugt ist, gibt es ein endliches Erzeugendensystem T von V. Nach Satz (2.120) gibt es eine Teilmenge T' von T so, dass $S' := S \cup T'$ eine Basis von V ist. □

Der Basisergänzungssatz (2.123) besagt also, dass jede linear unabhängige Teilmenge eines endlich erzeugten Vektorraums zu einer Basis dieses Vektorraums ergänzt werden kann.

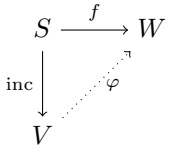
(2.124) Korollar. Es seien ein Körper K, ein endlich erzeugter K-Vektorraum V und ein K-Untervektorraum U von V gegeben. Für jede Basis S von U gibt es eine Basis S' von V so, dass S eine Teilmenge von S' ist.

Beweis. Es sei eine Basis S von U gegeben. Dann ist S linear unabhängig in U und damit auch in V. Nach dem Basisergänzungssatz (2.123) gibt es eine Basis S' von V mit $S \subseteq S'$. □

(2.125) Korollar. Es seien ein Körper K und ein endlich erzeugter K-Vektorraum V gegeben.

(a) Es sei eine linear unabhängige Familie $s = (s_i)_{i \in I}$ in V gegeben. Für jeden K-Vektorraum W und jede Familie $w = (w_i)_{i \in I}$ in W gibt es einen K-Vektorraumhomomorphismus $\varphi\colon V \to W$ mit $w_i = \varphi(s_i)$ für alle $i \in I$.

(b) Es sei eine linear unabhängige Teilmenge S von V gegeben. Für jeden K-Vektorraum W und jede Abbildung $f\colon S \to W$ gibt es einen K-Vektorraumhomomorphismus $\varphi\colon V \to W$ mit $f = \varphi|_S$.



Beweis.

(a) Siehe Aufgabe 74.

(b) Dies folgt aus (a) und Bemerkung (2.102)(b). □

Eindeutigkeit von Basen

(2.126) Lemma (Austauschlemma von Steinitz)**.** Es seien ein Körper K, ein K-Vektorraum V, ein Erzeugendensystem T von V, ein $s \in V$ und ein $a \in K^{(T)}$ mit $s = \sum_{t \in T} a_t t$ gegeben. Für alle $t \in T$ mit $a_t \neq 0$ ist $T \setminus \{t\} \cup \{s\}$ ein Erzeugendensystem von V.

Beweis. Es sei $t \in T$ mit $a_t \neq 0$ gegeben. Nach Lemma (2.80)(b) ist dann

$$t = a_t^{-1}(-\sum_{t' \in T \setminus \{t\}} a_{t'} t' + s) = \sum_{t' \in T \setminus \{t\}} (-a_t^{-1} a_{t'}) t' + a_t^{-1} s$$

eine Linearkombination von $T \setminus \{t\} \cup \{s\}$. Da T ein Erzeugendensystem von V ist, gilt dies auch für $T \cup \{s\}$ nach Bemerkung (2.90). Wir erhalten

$$V = \langle T \cup \{s\} \rangle = \langle (T \cup \{s\}) \setminus \{t\} \rangle = \langle T \setminus \{t\} \cup \{s\} \rangle$$

nach Proposition (2.82), d.h. $T \setminus \{t\} \cup \{s\}$ ist ein Erzeugendensystem von V. □

(2.127) Satz (Steinitzscher Austauschsatz)**.** Es seien ein Körper K und ein K-Vektorraum V gegeben. Für jede endliche linear unabhängige Teilmenge S von V und jedes Erzeugendensystem T von V gibt es eine Teilmenge S' von T mit $|S'| = |S|$ so, dass $T \setminus S' \cup S$ ein Erzeugendensystem von V ist.

Beweis. Es sei ein Erzeugendensystem T von V gegeben. Durch Induktion nach $|S|$ zeigen wir, dass es für jede endliche linear unabhängige Teilmenge S von V eine Teilmenge S' von T mit $|S'| = |S|$ so gibt, dass $T \setminus S' \cup S$ ein Erzeugendensystem von V ist.
Ist $|S| = 0$, so ist $S = \emptyset$ und es ist $T \setminus \emptyset \cup \emptyset = T$ ein Erzeugendensystem von V.
Es sei also eine endliche linear unabhängige Teilmenge S von V mit $|S| \geq 1$ gegeben und es sei angenommen, dass es für jede linear unabhängige Teilmenge U von V mit $|U| < |S|$ eine Teilmenge U' von T mit $|U'| = |U|$ so gibt, dass $T \setminus U' \cup U$ ein Erzeugendensystem von V ist. Wegen $|S| \geq 1$ gibt es ein Element $s_0 \in S$. Da $S \setminus \{s_0\}$ nach Bemerkung (2.99) linear unabhängig und $|S \setminus \{s_0\}| = |S| - 1 < |S|$ ist, gibt es nach Induktionsvoraussetzung eine Teilmenge S'' von T mit $|S''| = |S \setminus \{s_0\}| = |S| - 1$ so, dass $T \setminus S'' \cup (S \setminus \{s_0\})$ ein Erzeugendensystem von V ist. Nach Bemerkung (2.91) ist s_0 eine Linearkombination von $T \setminus S'' \cup (S \setminus \{s_0\})$, d.h. es gibt ein $a \in K^{(T \setminus S'' \cup (S \setminus \{s_0\}))}$ mit

$$s_0 = \sum_{t \in T \setminus S''} a_t t + \sum_{s \in S \setminus \{s_0\}} a_s s.$$

Wegen der linearen Unabhängigkeit von S ist s_0 nach Bemerkung (2.101) keine Linearkombination von $S \setminus \{s_0\}$. Folglich gibt es ein $t_0 \in T \setminus S''$ mit $a_{t_0} \neq 0$. Wir setzen $S' := S'' \cup \{t_0\}$. Nach dem Austauschlemma (2.126) ist mit $T \setminus S'' \cup (S \setminus \{s_0\})$ dann auch $T \setminus (S'' \cup \{t_0\}) \cup S = T \setminus S' \cup S$ ein Erzeugendensystem von V.
Nach dem Induktionsprinzip folgt, dass es für jede endliche linear unabhängige Teilmenge S von V eine Teilmenge S' von T mit $|S'| = |S|$ so gibt, dass $T \setminus S' \cup S$ ein Erzeugendensystem von V ist. □

(2.128) Korollar. Es seien ein Körper K und ein K-Vektorraum V gegeben. Für jede endliche linear unabhängige Teilmenge S von V und jedes Erzeugendensystem T von V gilt

$$|S| \leq |T|.$$

Beweis. Es sei eine endliche linear unabhängige Teilmenge S von V und ein Erzeugendensystem T von V gegeben. Nach dem Steinitzschen Austauschsatz (2.127) gibt es eine Teilmenge S' von T mit $|S'| = |S|$ so, dass $T \setminus S' \cup S$ ein Erzeugendensystem von V ist. Insbesondere gilt

$$|S| = |S'| \leq |T|.$$ □

(2.129) Korollar. Es seien ein Körper K, ein K-Vektorraum V und eine endliche Basis S von V gegeben.

(a) Für jedes Erzeugendensystem T von V gilt $|T| \geq |S|$.

(b) Für jede linear unabhängige Teilmenge T von V gilt $|T| \leq |S|$.

Beweis.

(a) Es sei ein Erzeugendensystem T von V gegeben. Nach Bemerkung (2.108) ist S als Basis linear unabhängig. Da S endlich ist, folgt $|S| \leq |T|$ nach Korollar (2.128).

(b) Es sei eine linear unabhängige Teilmenge T in V gegeben. Nach Bemerkung (2.108) ist S als Basis ein Erzeugendensystem von V. Jede endliche Teilmenge T_0 von T ist linear unabhängig nach Bemerkung (2.99), es gilt also $|T_0| \leq |S|$ nach Korollar (2.128). Dies impliziert aber schon, dass T selbst endlich ist und $|T| \leq |S|$ gilt. □

(2.130) Korollar. Es seien ein Körper K, ein endlich erzeugter K-Vektorraum V und Basen S und T von V gegeben. Dann sind S und T endlich und es gilt

$$|S| = |T|.$$

Beweis. Da V endlich erzeugt ist, gibt es eine endliche Basis X von V.
Nach Bemerkung (2.108) sind Basen linear unabhängige Erzeugendensysteme. Die Endlichkeit von X impliziert $|S| \geq |X|$ nach Korollar (2.129)(a) sowie $|S| \leq |X|$ nach Korollar (2.129)(b). Insgesamt haben wir also $|S| = |X|$ und damit insbesondere die Endlichkeit von S.
Analog zeigt man, dass T endlich und $|T| = |X|$ ist. Es folgt

$$|S| = |X| = |T|.$$ □

(2.131) Korollar. Es seien ein Körper K, ein endlich erzeugter K-Vektorraum V und eine Teilmenge S von V gegeben. Die folgenden Bedingungen sind äquivalent.

(a) Es ist S eine Basis von V.

(b) Es ist S ein bzgl. Kardinalität minimales Erzeugendensystem von V.

(c) Es ist S eine bzgl. Kardinalität maximale linear unabhängige Teilmenge von V.

Beweis. Wenn S eine Basis von V ist, so ist S endlich nach Korollar (2.130) und somit ein bzgl. Kardinalität minimales Erzeugendensystem von V nach Bemerkung (2.108) und Korollar (2.129)(a). Ist umgekehrt S ein bzgl. Kardinalität minimales Erzeugendensystem von V, so ist S insbesondere ein bzgl. Inklusion minimales Erzeugendensystem von V und damit eine Basis von V nach Lemma (2.114). Dies zeigt die Äquivalenz von Bedingung (a) und Bedingung (b).
Wenn S eine Basis von V ist, so ist S endlich nach Korollar (2.130) und somit eine bzgl. Kardinalität maximale linear unabhängige Teilmenge von V nach Bemerkung (2.108) und Korollar (2.129)(b). Ist umgekehrt S eine bzgl. Kardinalität maximale linear unabhängige Teilmenge von V, so ist S insbesondere eine bzgl. Inklusion maximale linear unabhängige Teilmenge von V und damit eine Basis von V nach Lemma (2.114). Dies zeigt die Äquivalenz von Bedingung (a) und Bedingung (c).
Insgesamt sind Bedingung (a), Bedingung (b) und Bedingung (c) äquivalent. □

Dimension eines endlich erzeugten Vektorraums

Nach Korollar (2.122) hat jeder endlich erzeugte Vektorraum eine endliche Basis, und nach Korollar (2.130) sind die Kardinalitäten von verschiedenen Basen gleich. Man sagt, dass diese Kardinalität eine *Invariante* des Vektorraums ist: Sie ist unabhängig von der betrachteten Basis und hängt nur vom Vektorraum ab. Wir wollen ihr einen Namen geben:

(2.132) Definition (Dimension)**.** Es seien ein Körper K und ein endlich erzeugter K-Vektorraum V gegeben. Für eine Basis S von V heißt

$$\dim V = \dim_K V := |S|$$

die *Dimension* von V über K (oder die *K-Dimension* von V).

(2.133) Beispiel. Es sei ein Körper K gegeben.

(a) Für jede endliche Menge I ist

$$\dim_K K^I = |I|.$$

(b) Für $n \in \mathbb{N}_0$ ist

$$\dim_K K^n = n.$$

(c) Für $m, n \in \mathbb{N}_0$ ist

$$\dim_K K^{m\times n} = mn.$$

Beweis.

(a) Nach Beispiel (2.117) ist die Standardbasis $\mathrm{e} = (\mathrm{e}_i)_{i\in I}$ eine parametrisierte Basis von $K^{(I)} = K^I$. Da $I \mapsto K^I$, $i \mapsto \mathrm{e}_i$ injektiv ist, folgt

$$\dim K^I = |\{\mathrm{e}_i \mid i \in I\}| = |I|.$$

(b) Nach (a) ist

$$\dim K^n = \dim K^{[1,n]} = |[1, n]| = n.$$

(c) Nach (a) ist

$$\dim K^{m\times n} = \dim K^{[1,m]\times[1,n]} = |[1,m]\times[1,n]| = |[1,m]|\,|[1,n]| = mn. \qquad \square$$

Nach Korollar (2.122) hat jeder endlich erzeugte Vektorraum eine endliche Basis. Da jede Basis eines Vektorraums insbesondere ein Erzeugendensystem ist, folgt umgekehrt aus der Existenz einer endlichen Basis, dass der Vektorraum endlich erzeugt ist. Da die Dimension eines endlich erzeugten Vektorraums gerade die Anzahl der Elemente einer endlichen Basis ist, vereinbaren wir folgende Terminologie:

(2.134) Definition ((un)endlichdimensional)**.** Es seien ein Körper K und ein K-Vektorraum V gegeben.

(a) Wir sagen, dass V *endlichdimensional* (über K) ist, wenn V endlich erzeugt ist. Ist V nicht endlichdimensional, so sagen wir, dass V *unendlichdimensional* (über K) ist.

(b) Es sei $n \in \mathbb{N}_0$ gegeben. Wir sagen, dass V ein *n-dimensionaler* K-Vektorraum ist, wenn V endlichdimensional und $\dim_K V = n$ ist.

(2.135) Bemerkung. Es seien ein Körper K, ein endlichdimensionaler K-Vektorraum V und eine Teilmenge S von V gegeben.

(a) Wenn S ein Erzeugendensystem von V ist, so ist $|S| \geq \dim_K V$.

(b) Wenn S linear unabhängig in V ist, so ist $|S| \leq \dim_K V$.

Beweis. Nach Korollar (2.122) gibt es eine endliche Basis T von V.

(a) Wenn S ein Erzeugendensystem von V ist, so gilt $|S| \geq |T| = \dim V$ nach Korollar (2.129)(a).

(b) Wenn S linear unabhängig in V ist, so gilt $|S| \leq |T| = \dim V$ nach Korollar (2.129)(b). $\square$

(2.136) Korollar. Es seien ein Körper K, ein endlichdimensionaler K-Vektorraum V und eine Teilmenge S von V gegeben. Die folgenden Bedingungen sind äquivalent.

(a) Es ist S eine Basis von V.

(b) Es ist S ein Erzeugendensystem von V und $|S| = \dim_K V$.

(c) Es ist S linear unabhängig in V und $|S| = \dim_K V$.

Beweis. Dies folgt aus Bemerkung (2.135) und Korollar (2.131). $\square$

Klassifikation endlichdimensionaler Vektorräume

(2.137) Satz. Es seien ein Körper K und endlichdimensionale K-Vektorräume V und W gegeben. Genau dann ist

$$V \cong W,$$

wenn

$$\dim_K V = \dim_K W$$

ist.

Beweis. Es sei $n := \dim V$.
Zunächst gelte $V \cong W$, so dass es einen Isomorphismus $\varphi\colon V \to W$ gibt. Da $\dim V = n$ ist, gibt es eine parametrisierte Basis $s = (s_i)_{i\in[1,n]}$ von V. Nach Korollar (2.116) ist $(\varphi(s_i))_{i\in[1,n]}$ eine parametrisierte Basis von W. Insbesondere gilt $\dim V = n = \dim W$.
Nun gelte umgekehrt $\dim V = \dim W$, so dass auch $\dim W = n$ ist. Es seien eine parametrisierte Basis $s = (s_i)_{i\in[1,n]}$ von V und eine parametrisierte Basis $t = (t_i)_{i\in[1,n]}$ von W gegeben. Nach Proposition (2.111)(a) gibt es genau einen K-Vektorraumhomomorphismus $\varphi\colon V \to W$ mit $\varphi(s_i) = t_i$ für alle $i \in I$, und nach Proposition (2.113)(c) ist φ ein Isomorphismus. Insbesondere gilt $V \cong W$. $\square$

(2.138) Korollar (Klassifikation endlichdimensionaler Vektorräume)**.** Es seien $n \in \mathbb{N}_0$, ein Körper K und ein endlichdimensionaler K-Vektorraum V gegeben. Genau dann ist

$$\dim_K V = n,$$

wenn

$$V \cong K^n$$

ist.

Beweis. Nach Beispiel (2.133)(b) ist $\dim K^n = n$. Somit gilt genau dann $\dim V = n$, wenn $\dim V = \dim K^n$ ist, was nach Satz (2.137) aber äquivalent zu $V \cong K^n$ ist. □

Dimension von Untervektorräumen

(2.139) Proposition. Es seien ein Körper K, ein endlichdimensionaler K-Vektorraum V und ein K-Untervektorraum U von V gegeben. Dann ist U endlichdimensional und es gilt

$$\dim_K U \leq \dim_K V.$$

Ferner gilt genau dann $U = V$, wenn

$$\dim_K U = \dim_K V$$

ist.

Beweis. Jede linear unabhängige Teilmenge S von U ist auch linear unabhängig in V, erfüllt also $|S| \leq \dim V$ nach Bemerkung (2.135)(b) und ist somit insbesondere endlich.
Es sei nun S eine bzgl. Kardinalität maximale linear unabhängige Teilmenge von U gegeben. Dann ist S insbesondere eine bzgl. Inklusion maximale linear unabhängige Teilmenge von V und damit eine Basis von V nach Lemma (2.114). Wegen der Endlichkeit von S ist U endlichdimensional und es gilt $\dim U = |S| \leq \dim V$. Wenn $U = V$ ist, so insbesondere auch $\dim U = \dim V$. Es gelte also umgekehrt $\dim U = \dim V$. Dann ist $|S| = \dim U = \dim V$ und damit S eine Basis von V nach (2.136)(a). Insbesondere ist S ein Erzeugendensystem von V nach Bemerkung (2.108) und damit $U = \langle S \rangle = V$. □

(2.140) Proposition. Es seien ein Körper K, ein endlichdimensionaler K-Vektorraum V und K-Untervektorräume U_1 und U_2 von V gegeben. Dann gilt

$$\dim_K(U_1 + U_2) = \dim_K U_1 + \dim_K U_2 - \dim_K(U_1 \cap U_2).$$

Beweis. Siehe Aufgabe 77. □

Rang und Defekt

(2.141) Proposition (Rangsatz)**.** Es seien ein Körper K, ein endlichdimensionaler K-Vektorraum V und ein K-Vektorraumhomomorphismus $\varphi\colon V \to W$ gegeben. Dann sind $\operatorname{Ker}\varphi$ und $\operatorname{Im}\varphi$ endlichdimensional und es gilt

$$\dim_K V = \dim_K(\operatorname{Ker}\varphi) + \dim_K(\operatorname{Im}\varphi).$$

Beweis. Siehe Aufgabe 78. □

(2.142) Definition (Rang)**.** Es seien ein Körper K und ein K-Vektorraumhomomorphismus $\varphi\colon V \to W$ so gegeben, dass V oder W endlichdimensional ist. Der *Rang* von φ ist definiert als

$$\operatorname{rk}\varphi = \operatorname{rk}_K\varphi := \dim_K(\operatorname{Im}\varphi).$$

(2.143) Definition (Defekt)**.** Es seien ein Körper K, ein endlichdimensionaler K-Vektorraum V und ein K-Vektorraumhomomorphismus $\varphi\colon V \to W$ gegeben. Der *Defekt* von φ ist definiert als

$$\operatorname{def}\varphi = \operatorname{def}_K\varphi := \dim_K(\operatorname{Ker}\varphi).$$

(2.144) Bemerkung (Rangsatz)**.** Es seien ein Körper K, ein endlichdimensionaler K-Vektorraum V und ein K-Vektorraumhomomorphismus $\varphi\colon V \to W$ gegeben. Dann gilt

$$\dim_K V = \operatorname{def}\varphi + \operatorname{rk}\varphi.$$

Beweis. Nach Proposition (2.141) gilt

$$\dim V = \dim(\operatorname{Ker}\varphi) + \dim(\operatorname{Im}\varphi) = \operatorname{def}\varphi + \operatorname{rk}\varphi. \qquad \square$$

Aufgaben

Aufgabe 73 (Basisauswahl, **3 Punkte**)**.** Es sei U der $\mathbb{F}_3$-Untervektorraum von $\mathbb{F}_3^{6\times 1}$ gegeben durch

$$U = \left\langle \begin{pmatrix} -1 \\ 1 \\ 1 \\ 1 \\ -1 \\ -1 \end{pmatrix}, \begin{pmatrix} -1 \\ -1 \\ 1 \\ 1 \\ 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ -1 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ -1 \\ 1 \\ -1 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ -1 \\ 1 \\ -1 \\ 0 \end{pmatrix} \right\rangle.$$

Bestimmen Sie eine Basis von U.

Aufgabe 74 (Fortsetzungen von Vektorraumhomomorphismen auf linear unabhängigen Familien)**.** Es seien ein Körper K, ein endlich erzeugter K-Vektorraum V und eine linear unabhängige Familie $s = (s_i)_{i\in I}$ in V gegeben. Zeigen Sie: Für jeden K-Vektorraum W und jede Familie $w = (w_i)_{i\in I}$ in W gibt es einen K-Vektorraumhomomorphismus $\varphi\colon V \to W$ mit $w_i = \varphi(s_i)$ für alle $i \in I$.

Aufgabe 75 (Fortsetzen von Vektorraumhomomorphismen)**.** Für $i \in [1,5]$ seien $x_i \in \mathbb{R}^4$, $y_i \in \mathbb{R}^3$ gegeben durch

$$x_1 := (1,1,0,0),\ x_2 := (3,4,0,-1),\ x_3 := (0,0,2,1),\ x_4 := (0,1,2,0),\ x_5 := (-2,1,1,1),$$
$$y_1 := (0,1,0),\ y_2 := (1,1,-1),\ y_3 := (2,2,3),\ y_4 := (1,-1,-1),\ y_5 := (1,6,4).$$

Entscheiden Sie in den folgenden Fällen jeweils, ob es einen $\mathbb{R}$-Vektorraumhomomorphismus φ mit den geforderten Eigenschaften gibt.

(a) Existiert ein Homomorphismus $\varphi\colon \mathbb{R}^4 \to \mathbb{R}^3$ mit $\varphi(x_1) = y_1$, $\varphi(x_2) = y_2$, $\varphi(x_3) = y_3$, $\varphi(x_4) = y_4$?

(b) Existiert ein Homomorphismus $\varphi\colon \mathbb{R}^3 \to \mathbb{R}^4$ mit $\varphi(y_1) = x_1$, $\varphi(y_2) = x_2$, $\varphi(y_3) = x_3$?

(c) Existiert ein Homomorphismus $\varphi\colon \mathbb{R}^4 \to \mathbb{R}^3$ mit $\varphi(x_1) = y_1$, $\varphi(x_2) = y_4$, $\varphi(x_3) = y_5$, $\varphi(x_4) = y_3$?

(d) Existiert ein Homomorphismus $\varphi\colon \mathbb{R}^4 \to \mathbb{R}^4$ mit $\varphi(x_1) = x_5$, $\varphi(x_5) = x_1$?

(e) Existiert ein Homomorphismus $\varphi\colon \mathbb{R}^3 \to \mathbb{R}^3$ mit $\varphi(y_1) = y_2$, $\varphi(y_2) = y_1$, $\varphi(y_3) = y_4$?

Bestimmen Sie in den Fällen, in welchen φ existiert und eindeutig bestimmt ist, Basen von $\operatorname{Im}\varphi$ und $\operatorname{Ker}\varphi$.

Aufgabe 76 (Vektorräume über endlichen Körpern)**.** Es sei K ein endlicher Körper und es sei V ein n-dimensionaler K-Vektorraum für ein $n \in \mathbb{N}_0$. Wieviele Elemente besitzt V?

Aufgabe 77 (Dimension der inneren Summe)**.** Es seien ein Körper K, ein endlichdimensionaler K-Vektorraum V und K-Untervektorräume U_1 und U_2 von V gegeben. Zeigen Sie, dass

$$\dim_K(U_1 + U_2) = \dim_K U_1 + \dim_K U_2 - \dim_K(U_1 \cap U_2)$$

gilt.

Aufgabe 78 (Rangsatz)**.** Es seien ein Körper K, ein endlichdimensionaler K-Vektorraum V und ein K-Vektorraumhomomorphismus $\varphi\colon V \to W$ gegeben. Zeigen Sie, dass $\operatorname{Ker}\varphi$ und $\operatorname{Im}\varphi$ endlichdimensional sind und

$$\dim_K V = \dim_K(\operatorname{Ker}\varphi) + \dim_K(\operatorname{Im}\varphi)$$

gilt.

6 Matrix-Kalkül

Vektorraum der Homomorphismen

(2.145) Bemerkung. Es seien ein Körper K und K-Vektorräume V und W gegeben. Die Menge $\mathrm{Map}(V,W)$ wird ein K-Vektorraum mit Addition gegeben durch

$$(f+g)(v) = f(v) + g(v)$$

für $v \in V$, $f, g \in \mathrm{Map}(V,W)$ und Skalarmultiplikation gegeben durch

$$(af)(v) = af(v)$$

für $v \in V$, $a \in K$, $f \in \mathrm{Map}(V,W)$.

Beweis. Dies ist im Wesentlichen nur eine Umformulierung von Aufgabe 59(a): Jedes Element $f \in \mathrm{Map}(V,W)$, also jede Abbildung $f\colon V \to W$, liefert eine Familie f in W über V via $f_i = f(i)$, also ein Element $f \in W^V$; und umgekehrt. □

(2.146) Proposition. Es seien ein Körper K und K-Vektorräume V, W, X gegeben.

(a) Für $\varphi \in \mathrm{Hom}(V,W)$, $\psi, \psi' \in \mathrm{Hom}(W,X)$ gilt

$$(\psi + \psi') \circ \varphi = \psi \circ \varphi + \psi' \circ \varphi.$$

Für $\varphi, \varphi' \in \mathrm{Hom}(V,W)$, $\psi \in \mathrm{Hom}(W,X)$ gilt

$$\psi \circ (\varphi + \varphi') = \psi \circ \varphi + \psi \circ \varphi'.$$

(b) Für $a \in K$, $\varphi \in \mathrm{Hom}(V,W)$, $\psi \in \mathrm{Hom}(W,X)$ gilt

$$(a\psi) \circ \varphi = \psi \circ (a\varphi) = a(\psi \circ \varphi).$$

Beweis.

(a) Für $\varphi \in \mathrm{Hom}(V,W)$, $\psi, \psi' \in \mathrm{Hom}(W,X)$ gilt

$$((\psi + \psi') \circ \varphi)(v) = (\psi + \psi')(\varphi(v)) = \psi(\varphi(v)) + \psi'(\varphi(v)) = (\psi \circ \varphi + \psi' \circ \varphi)(v)$$

für alle $v \in V$ und damit $\psi \circ (\varphi + \varphi') = \psi \circ \varphi + \psi \circ \varphi'$. Für $\varphi, \varphi' \in \mathrm{Hom}(V,W)$, $\psi \in \mathrm{Hom}(W,X)$ gilt

$$(\psi \circ (\varphi + \varphi'))(v) = \psi((\varphi + \varphi')(v)) = \psi(\varphi(v) + \varphi'(v)) = \psi(\varphi(v)) + \psi(\varphi'(v)) = (\psi \circ \varphi + \psi \circ \varphi')(v)$$

für alle $v \in V$ und damit $\psi \circ (\varphi + \varphi') = \psi \circ \varphi + \psi \circ \varphi'$.

(b) Für $a \in K$, $\varphi \in \mathrm{Hom}(V,W)$, $\psi \in \mathrm{Hom}(W,X)$ gilt

$$\begin{aligned}((a\psi) \circ \varphi)(v) &= (a\psi)(\varphi(v)) = a\psi(\varphi(v)) = (a(\psi \circ \varphi))(v),\\ (\psi \circ (a\varphi))(v) &= \psi((a\varphi)(v)) = \psi(a\varphi(v)) = a\psi(\varphi(v)) = (a(\psi \circ \varphi))(v)\end{aligned}$$

für alle $v \in V$ und damit $(a\psi) \circ \varphi = \psi \circ (a\varphi) = a(\psi \circ \varphi)$. □

(2.147) Proposition. Es seien ein Körper K und K-Vektorräume V und W gegeben. Dann ist $\mathrm{Hom}_K(V,W)$ ein K-Untervektorraum von $\mathrm{Map}(V,W)$.

Beweis. Für $\varphi, \psi \in \mathrm{Hom}_K(V,W)$ gilt

$$\begin{aligned}(\varphi + \psi)(v + v') &= \varphi(v + v') + \psi(v + v') = \varphi(v) + \varphi(v') + \psi(v) + \psi(v') = \varphi(v) + \psi(v) + \varphi(v') + \psi(v')\\ &= (\varphi + \psi)(v) + (\varphi + \psi)(v'),\\ (\varphi + \psi)(bv) &= \varphi(bv) + \psi(bv) = b\varphi(v) + b\psi(v) = b(\varphi + \psi)(v)\end{aligned}$$

für $b \in K$, $v, v' \in V$, d.h. $\varphi + \psi \in \mathrm{Hom}_K(V,W)$ nach Bemerkung (2.36). Ferner ist

$$0(v+v') = 0 = 0+0 = 0(v) + 0(v'),$$
$$0(bv) = 0 = b0 = b0(v)$$

für $b \in K$, $v, v' \in V$, d.h. $0 \in \mathrm{Hom}_K(V,W)$ nach Bemerkung (2.36). Für $a \in K$, $\varphi \in \mathrm{Hom}_K(V,W)$ gilt schließlich

$$(a\varphi)(v+v') = a\varphi(v+v') = a(\varphi(v)+\varphi(v')) = a\varphi(v) + a\varphi(v') = (a\varphi)(v) + (a\varphi)(v'),$$
$$(a\varphi)(bv) = a\varphi(bv) = ab\varphi(v) = ba\varphi(v) = b(a\varphi)(v)$$

für $b \in K$, $v, v' \in V$, d.h. $a\varphi \in \mathrm{Hom}_K(V,W)$ nach Bemerkung (2.36).
Nach dem Untervektorraumkriterium (2.52) ist $\mathrm{Hom}_K(V,W)$ ein Untervektorraum von $\mathrm{Map}(V,W)$. □

(2.148) Bemerkung. Es seien ein Körper K und ein K-Vektorraum V gegeben. Die abelsche Gruppe $\mathrm{Hom}(V,V)$ wird ein Ring mit Multiplikation gegeben durch Komposition.

Beweis. Nach Beispiel (1.44)(e) bildet die unterliegende Menge von $\mathrm{Hom}(V,V)$ zusammen mit der Komposition ein Monoid. Die Distributivgesetze folgen aus Proposition (2.146)(a). □

Matrizen und Homomorphismen

Wir wollen nun Homomorphismen zwischen Vektorräumen mit Hilfe von Basen effizient beschreiben. Nach Proposition (2.111) wissen wir, dass Vektorraumhomomorphismen eindeutig durch ihre Werte auf einer Basis bestimmt sind und dass jede Vorgabe von solchen Werten auf einer Basis auch zu einem Vektorraumhomomorphismus fortsetzt. Noch etwas genauer haben wir folgendes Resultat:

(2.149) Proposition. Es seien ein Körper K, Vektorräume V und W über K sowie eine parametrisierte Basis $s = (s_j)_{j\in J}$ gegeben. Die Abbildungen

$$\mathrm{Hom}_K(V,W) \to W^J,\ \varphi \mapsto (\varphi(s_j))_{j\in J},$$
$$W^J \to \mathrm{Hom}_K(V,W),\ w \mapsto \lambda_w \circ \lambda_s^{-1}$$

sind sich gegenseitig invertierbare K-Vektorraumisomorphismen.

Beweis. Da s eine Basis von V ist, sind

$$\Phi\colon \mathrm{Hom}_K(V,W) \to W^J,\ \varphi \mapsto (\varphi(s_j))_{j\in J},$$
$$\Psi\colon W^J \to \mathrm{Hom}_K(V,W),\ w \mapsto \lambda_w \circ \lambda_s^{-1}$$

nach Proposition (2.111)(a) sich gegenseitig invertierbare Abbildungen. Nun gilt

$$\Phi(\varphi+\psi) = ((\varphi+\psi)(s_j))_{j\in J} = (\varphi(s_j)+\psi(s_j))_{j\in J} = (\varphi(s_j))_{j\in J} + (\psi(s_j))_{j\in J} = \Phi(\varphi) + \Phi(\psi)$$

für $\varphi, \psi \in \mathrm{Hom}(V,W)$ sowie

$$\Phi(a\varphi) = ((a\varphi)(s_j))_{j\in J} = (a\varphi(s_j))_{j\in J} = a(\varphi(s_j))_{j\in J} = a\,\Phi(\varphi).$$

für $a \in K$, $\varphi \in \mathrm{Hom}(V,W)$. Folglich ist Φ nach Bemerkung (2.36) und Bemerkung (2.40) ein Isomorphismus. Wegen $\Psi = \Phi^{-1}$ ist dann aber auch Ψ ein Isomorphismus. □

Haben wir also endlichdimensionale Vektorräume V und W über einem Körper K sowie eine parametrisierte Basis $s = (s_j)_{j\in[1,n]}$ von V gegeben, wobei $n \in \mathbb{N}_0$, so liefert Proposition (2.149) einen Isomorphismus

$$W^n \to \mathrm{Hom}_K(V,W).$$

Andererseits liefert jede parametrisierte Basis $t = (t_j)_{j\in[1,m]}$ von W, wobei $m \in \mathbb{N}_0$, nach Bemerkung (2.108) den Isomorphismus

$$\lambda_t\colon K^m \to W,$$

welcher widerum einen Isomorphismus

$$(K^m)^n \to W^n,\ (b_j)_{j\in[1,n]} \mapsto (\lambda_t(b_j))_{j\in[1,n]}$$

induziert. Schließlich sind die Vektorraumstrukturen auf $(K^m)^n$ und $K^{m\times n}$ gerade so definiert, dass

$$K^{m\times n} \to (K^m)^n,\ A \mapsto ((A_{i,j})_{i\in[1,m]})_{j\in[1,n]}$$

ein Isomorphismus wird. Durch Komposition dieser Isomorphismen und ihrer Inversen erhalten wir Isomorphismen $K^{m\times n} \to \mathrm{Hom}_K(V,W)$ und $\mathrm{Hom}_K(V,W) \to K^{m\times n}$, welche wir nun näher beleuchten wollen. Diese Isomorphismen stellen somit einen Zusammenhang zwischen Elementen von $\mathrm{Hom}_K(V,W)$, also Vektorraumhomomorphismen von V nach W, und Elementen von $K^{m\times n}$, also $(m\times n)$-Matrizen mit Einträgen in K, dar. Sie erlauben uns, Vektorraumhomomorphismen durch Matrizen zu kodieren.

(2.150) Definition (durch Matrix dargestellter Vektorraumhomomorphismus)**.** Es sei ein Körper K gegeben.

(a) Es seien endlichdimensionale K-Vektorräume V und W, eine parametrisierte Basis $s = (s_j)_{j\in[1,n]}$ von V und eine parametrisierte Basis $t = (t_i)_{i\in[1,m]}$ von W gegeben. Für $A \in K^{m\times n}$ heißt der eindeutige K-Vektorraumhomomorphismus $\varphi_{A,s,t}\colon V \to W$ mit

$$\varphi_{A,s,t}(s_j) = \sum_{i\in[1,m]} A_{i,j}t_i$$

für $j \in [1,n]$ der durch A bzgl. der Basen s und t *dargestellte K-Vektorraumhomomorphismus.*

(b) Es seien $m,n \in \mathbb{N}_0$ gegeben. Für $A \in K^{m\times n}$ heißt

$$\varphi_A := \varphi_{A,\mathrm{e},\mathrm{e}}\colon K^{n\times 1} \to K^{m\times 1}$$

die *Standardinterpretation* von A.

(2.151) Proposition. Es seien ein Körper K und endlichdimensionale K-Vektorräume V und W gegeben. Für jede parametrisierte Basis $s = (s_j)_{j\in[1,n]}$ von V und jede parametrisierte Basis $t = (t_i)_{i\in[1,m]}$ von W ist

$$\varphi_{-,s,t}\colon K^{m\times n} \to \mathrm{Hom}_K(V,W),\ A \mapsto \varphi_{A,s,t}$$

ein K-Vektorraumisomorphismus.

Beweis. Zunächst ist

$$\Psi_1\colon K^{m\times n} \to (K^m)^n,\ A \mapsto ((A_{i,j})_{i\in[1,m]})_{j\in[1,n]}$$

ein Isomorphismus. Nach Bemerkung (2.108) liefert die Basis t den Isomorphismus

$$\lambda_t\colon K^m \to W,\ b \mapsto \sum_{i\in[1,m]} b_i t_i$$

welcher widerum einen Isomorphismus

$$\Psi_2\colon (K^m)^n \to W^n,\ (b_j)_{j\in[1,n]} \mapsto (\lambda_t(b_j))_{j\in[1,n]}$$

induziert. Schließlich haben wir nach Proposition (2.149) den Isomorphismus

$$\Psi_3\colon W^n \to \mathrm{Hom}_K(V,W),\ w \mapsto \lambda_w \circ \lambda_s^{-1}.$$

Dabei ist $\Psi_3(w)\colon V \to W$ für $w \in W^n$ der eindeutige Homomorphismus mit $(\Psi_3(w))(s_j) = w_j$ für $j \in [1,n]$. Für $A \in K^{m\times n}$ gilt nun

$$\Psi_2(\Psi_1(A)) = \Psi_2(((A_{i,j})_{i\in[1,m]})_{j\in[1,n]}) = (\lambda_t((A_{i,j})_{i\in[1,m]}))_{j\in[1,n]} = (\sum_{i\in[1,m]} A_{i,j}t_i)_{j\in[1,n]},$$

es ist also $\Psi_3(\Psi_2(\Psi_1(A))) = \Psi_3((\sum_{i\in[1,m]} A_{i,j}t_i)_{j\in[1,n]})$ der eindeutige Homomorphismus mit

$$(\Psi_3(\Psi_2(\Psi_1(A))))(s_j) = \sum_{i\in[1,m]} A_{i,j}t_i$$

und damit $\Psi_3(\Psi_2(\Psi_1(A))) = \varphi_{A,s,t}$. Folglich ist

$$\varphi_{-,s,t} = \Psi_3 \circ \Psi_2 \circ \Psi_1$$

ein Isomorphismus. □

(2.152) Korollar. Es seien ein Körper K und endlichdimensionale K-Vektorräume V und W gegeben. Dann ist

$$\dim_K \mathrm{Hom}_K(V,W) = (\dim_K V)(\dim_K W).$$

Beweis. Es ist $\mathrm{Hom}_K(V,W) \cong K^{m\times n}$ nach Proposition (2.151) und damit

$$\dim_K \mathrm{Hom}_K(V,W) = \dim_K K^{m\times n} = mn = nm = (\dim_K V)(\dim_K W)$$

nach Satz (2.137) und Beispiel (2.133)(c). □

(2.153) Definition (Darstellungsmatrix)**.** Es seien ein Körper K, endlichdimensionale K-Vektorräume V und W, eine parametrisierte Basis $s = (s_j)_{j\in[1,n]}$ von V und eine parametrisierte Basis $t = (t_i)_{i\in[1,m]}$ von W gegeben. Wir bezeichnen mit

$$\mathrm{M}_t^s \colon \mathrm{Hom}_K(V,W) \to K^{m\times n},\ \varphi \mapsto \mathrm{M}_t^s(\varphi)$$

den zu $\varphi_{-,s,t} \colon K^{m\times n} \to \mathrm{Hom}_K(V,W)$, $A \mapsto \varphi_{A,s,t}$ inversen K-Vektorraumisomorphismus. Für einen K-Vektorraumhomomorphismus $\varphi \colon V \to W$ heißt $\mathrm{M}_t^s(\varphi)$ die *Darstellungsmatrix* (oder *Abbildungsmatrix*) von φ zu den Basen s und t.

(2.154) Bemerkung. Es seien ein Körper K, endlichdimensionale K-Vektorräume V und W, ein K-Vektorraumhomomorphismus $\varphi \colon V \to W$, eine parametrisierte Basis $s = (s_j)_{j\in[1,n]}$ von V und eine parametrisierte Basis $t = (t_i)_{i\in[1,m]}$ von W gegeben.

(a) Für $j \in [1,n]$ gilt

$$\varphi(s_j) = \sum_{i\in[1,m]} (\mathrm{M}_t^s(\varphi))_{i,j}t_i.$$

(b) Es sei $A \in K^{m\times n}$ so gegeben, dass $\varphi(s_j) = \sum_{i\in[1,m]} A_{i,j}t_i$ für $j \in [1,n]$ gilt. Dann ist

$$\mathrm{M}_t^s(\varphi) = A.$$

Beweis.

(a) Wegen $\varphi_{-,s,t} \circ \mathrm{M}_t^s = \mathrm{id}_{\mathrm{Hom}_K(V,W)}$ ist $\varphi = \varphi_{\mathrm{M}_t^s(\varphi),s,t}$, also

$$\varphi(s_j) = (\varphi_{\mathrm{M}_t^s(\varphi),s,t})(s_j) = \sum_{i\in[1,m]} (\mathrm{M}_t^s(\varphi))_{i,j}t_i$$

für $j \in [1,n]$.

(b) Nach Definition (2.150)(a) ist $\varphi = \varphi_{A,s,t}$. Wegen $\mathrm{M}_t^s \circ \varphi_{-,s,t} = \mathrm{id}_{K^{m\times n}}$ folgt

$$\mathrm{M}_t^s(\varphi) = \mathrm{M}_t^s(\varphi_{A,s,t}) = A.$$ □

(2.155) Korollar. Es seien $m,n \in \mathbb{N}_0$ und ein Körper K gegeben. Für $A \in K^{m\times n}$ gilt

$$\mathrm{M}_{\mathrm{e}^{K^{m\times 1}}}^{\mathrm{e}^{K^{n\times 1}}}(\varphi_A) = A.$$

Beweis. Für $j \in [1,n]$ ist $\varphi_A(\mathrm{e}_j) = \sum_{i\in[1,m]} A_{i,j}\mathrm{e}_i$. Somit folgt $\mathrm{M}_{\mathrm{e}}^{\mathrm{e}}(\varphi_A) = A$ nach Bemerkung (2.154)(b). □

Bemerkung (2.154) sagt uns, wie wir die Einträge der Darstellungsmatrix $\mathrm{M}_t^s(\varphi)$ eines Vektorraumhomomorphismus $\varphi\colon V \to W$ bzgl. parametrisierter Basen $s = (s_j)_{j\in[1,n]}$ und $t = (t_i)_{i\in[1,m]}$ ermitteln: Es sei $j \in [1,n]$ gegeben. Zunächst bilden wir den Basisvektor s_j unter φ ab. Dann stellen wir das Bild $\varphi(s_j)$ als Linearkombination in $t = (t_i)_{i\in[1,m]}$ dar (diese Darstellung existiert und ist eindeutig, da t eine Basis von W ist). Der Koeffizient von t_i bildet den Eintrag von $\mathrm{M}_t^s(\varphi)$ an der Stelle (i,j). Wir schreiben sämtliche Koeffizienten also in die j-te Spalte von $\mathrm{M}_t^s(\varphi)$.

(2.156) Beispiel.

(a) Die Darstellungsmatrix von $\varphi\colon K^2 \to K^3$, $(x_1,x_2) \mapsto (x_1+x_2, x_1-x_2, x_2)$ bzgl. der Standardbasen e^{K^2} und e^{K^3} ist

$$\mathrm{M}_{\mathrm{e}^{K^3}}^{\mathrm{e}^{K^2}}(\varphi) = \begin{pmatrix} 1 & 1 \\ 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

(b) Die Darstellungsmatrix von $\varphi\colon \mathbb{R}^3 \to \mathbb{R}^2$, $(x_1,x_2,x_3) \mapsto (x_1+x_2+x_3, 2x_1+3x_2+4x_3)$ bzgl. der Standardbasen $\mathrm{e}^{\mathbb{R}^3}$ und $\mathrm{e}^{\mathbb{R}^2}$ ist

$$\mathrm{M}_{\mathrm{e}^{\mathbb{R}^2}}^{\mathrm{e}^{\mathbb{R}^3}}(\varphi) = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 3 & 4 \end{pmatrix}.$$

(c) Die Darstellungsmatrix von $\varphi\colon K^{3\times 2} \to K^{2\times 3}$, $A \mapsto A^{\mathrm{tr}}$ bzgl. der Basen

$$s = (\mathrm{e}_{1,1}^{K^{3\times 2}}, \mathrm{e}_{1,2}^{K^{3\times 2}}, \mathrm{e}_{2,1}^{K^{3\times 2}}, \mathrm{e}_{2,2}^{K^{3\times 2}}, \mathrm{e}_{3,1}^{K^{3\times 2}}, \mathrm{e}_{3,2}^{K^{3\times 2}}),$$
$$t = (\mathrm{e}_{1,1}^{K^{2\times 3}}, \mathrm{e}_{1,2}^{K^{2\times 3}}, \mathrm{e}_{1,3}^{K^{2\times 3}}, \mathrm{e}_{2,1}^{K^{2\times 3}}, \mathrm{e}_{2,2}^{K^{2\times 3}}, \mathrm{e}_{2,3}^{K^{2\times 3}})$$

ist

$$\mathrm{M}_t^s(\varphi) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Beweis.

(a) Es ist

$$\varphi(\mathrm{e}_1) = (1,1,0) = \mathrm{e}_1 + \mathrm{e}_2 = 1\mathrm{e}_1 + 1\mathrm{e}_2 + 0\mathrm{e}_3,$$
$$\varphi(\mathrm{e}_2) = (1,-1,1) = \mathrm{e}_1 - \mathrm{e}_2 + \mathrm{e}_3 = 1\mathrm{e}_1 + (-1)\mathrm{e}_2 + 1\mathrm{e}_3,$$

und damit

$$\mathrm{M}_{\mathrm{e}^{K^3}}^{\mathrm{e}^{K^2}}(\varphi) = \begin{pmatrix} 1 & 1 \\ 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

(b) Es ist

$$\varphi(\mathrm{e}_1) = (1,2) = \mathrm{e}_1 + 2\mathrm{e}_2,$$
$$\varphi(\mathrm{e}_2) = (1,3) = \mathrm{e}_1 + 3\mathrm{e}_2,$$
$$\varphi(\mathrm{e}_3) = (1,4) = \mathrm{e}_1 + 4\mathrm{e}_2,$$

und damit

$$\mathrm{M}_{\mathrm{e}^{\mathbb{R}^2}}^{\mathrm{e}^{\mathbb{R}^3}}(\varphi) = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 3 & 4 \end{pmatrix}.$$

(c) Es ist

$$\begin{aligned}
\varphi(\mathrm{e}_{1,1}^{K^{3\times 2}}) &= (\mathrm{e}_{1,1}^{K^{3\times 2}})^{\mathrm{tr}} = \mathrm{e}_{1,1}^{K^{2\times 3}},\\
\varphi(\mathrm{e}_{1,2}^{K^{3\times 2}}) &= (\mathrm{e}_{1,2}^{K^{3\times 2}})^{\mathrm{tr}} = \mathrm{e}_{2,1}^{K^{2\times 3}},\\
\varphi(\mathrm{e}_{2,1}^{K^{3\times 2}}) &= (\mathrm{e}_{2,1}^{K^{3\times 2}})^{\mathrm{tr}} = \mathrm{e}_{1,2}^{K^{2\times 3}},\\
\varphi(\mathrm{e}_{2,2}^{K^{3\times 2}}) &= (\mathrm{e}_{2,2}^{K^{3\times 2}})^{\mathrm{tr}} = \mathrm{e}_{2,2}^{K^{2\times 3}},\\
\varphi(\mathrm{e}_{3,1}^{K^{3\times 2}}) &= (\mathrm{e}_{3,1}^{K^{3\times 2}})^{\mathrm{tr}} = \mathrm{e}_{1,3}^{K^{2\times 3}},\\
\varphi(\mathrm{e}_{3,2}^{K^{3\times 2}}) &= (\mathrm{e}_{3,2}^{K^{3\times 2}})^{\mathrm{tr}} = \mathrm{e}_{2,3}^{K^{2\times 3}},
\end{aligned}$$

und damit

$$\mathrm{M}_t^s(\varphi) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \qquad \square$$

In Beispiel (2.156)(c) können wir nicht direkt mit den Standardbasen $\mathrm{e}^{K^{3\times 2}} = (\mathrm{e}_{i,j}^{K^{3\times 2}})_{(i,j)\in[1,3]\times[1,2]}$ und $\mathrm{e}^{K^{2\times 3}} = (\mathrm{e}_{i,j}^{K^{2\times 3}})_{(i,j)\in[1,2]\times[1,3]}$ arbeiten, da diese nicht durch $[1,6]$ indiziert sind. Zum Bilden der Darstellungsmatrizen benötigen wir jedoch die Indizierung durch $[1,6]$, da es sich hierbei um eine total geordnete Menge handelt (es ist $1 < 2 < \cdots < 6$). Aus diesem Grund haben wir zuerst die Basen s und t gebildet. Betrachten wir statt t die Basis $t' = (\mathrm{e}_{1,1}^{K^{2\times 3}}, \mathrm{e}_{2,1}^{K^{2\times 3}}, \mathrm{e}_{1,2}^{K^{2\times 3}}, \mathrm{e}_{2,2}^{K^{2\times 3}}, \mathrm{e}_{1,3}^{K^{2\times 3}}, \mathrm{e}_{2,3}^{K^{2\times 3}})$ von $K^{2\times 3}$, so erhalten wir die Darstellungsmatrix

$$\mathrm{M}_{t'}^s(\varphi) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Matrixmultiplikation

Es seien Vektorraumhomorphismen $\varphi\colon V \to W$ und $\psi\colon W \to X$ zwischen endlichdimensionalen Vektorräumen sowie eine parametrisierte Basis $s = (s_k)_{k\in[1,p]}$ von V, eine parametrisierte Basis $t = (t_j)_{j\in[1,n]}$ von W und eine parametrisierte Basis $u = (u_i)_{i\in[1,m]}$ von X gegeben. Wir können die Darstellungsmatrizen $\mathrm{M}_t^s(\varphi)$ und $\mathrm{M}_u^t(\psi)$ bilden. Da nach Bemerkung (a) das Kompositum $\psi \circ \varphi\colon V \to X$ auch ein Vektorraumhomomorphismus ist, können wir außerdem die Darstellungsmatrix $\mathrm{M}_u^s(\psi\circ\varphi)$ bilden. Da φ und ψ nur von ihren Darstellungsmatrizen abhängen, gilt dies auch für das Komposition $\psi\circ\varphi$ und damit auch für die Darstellungsmatrix $\mathrm{M}_u^s(\psi\circ\varphi)$. Es stellt sich die Frage, wie sich die Darstellungsmatrix des Kompositums $\mathrm{M}_u^s(\psi\circ\varphi)$ aus den Darstellungsmatrizen $\mathrm{M}_t^s(\varphi)$ und $\mathrm{M}_u^t(\psi)$ berechnen lässt. Für $k \in [1,p]$ gilt

$$\begin{aligned}
\psi(\varphi(s_k)) &= \psi\Big(\sum_{j\in[1,n]} (\mathrm{M}_t^s(\varphi))_{j,k} t_j\Big) = \sum_{j\in[1,n]} (\mathrm{M}_t^s(\varphi))_{j,k}\psi(t_j) = \sum_{j\in[1,n]} (\mathrm{M}_t^s(\varphi))_{j,k} \sum_{i\in[1,m]} (\mathrm{M}_u^t(\psi))_{i,j} u_i\\
&= \sum_{i\in[1,m]} \Big(\sum_{j\in[1,n]} (\mathrm{M}_u^t(\psi))_{i,j}(\mathrm{M}_t^s(\varphi))_{j,k}\Big) u_i,
\end{aligned}$$

so dass wir also

$$\mathrm{M}_u^s(\psi\circ\varphi) = \Big(\sum_{j\in[1,n]} (\mathrm{M}_u^t(\psi))_{i,j}(\mathrm{M}_t^s(\varphi))_{j,k}\Big)_{i\in[1,m],k\in[1,p]}$$

haben. Wir wollen im Folgenden eine Multiplikation zwischen Matrizen einführen, welche gerade der Komposition von Vektorraumhomomorphismen entspricht.

Bzgl. dieser Multiplikation von Matrizen sollte es außerdem Matrizen geben, welche sich ähnlich wie die Identitäten unter den Vektorraumhomomorphismen verhalten. Haben wir einen Vektorraum V und eine parametrisierte Basis $s = (s_j)_{j\in[1,n]}$ von V gegeben, so gilt

$$\mathrm{id}_V(s_j) = \sum_{i\in[1,m]} \delta_{i,j} s_i$$

und damit

$$\mathrm{M}_s^s(\mathrm{id}_V) = (\delta_{i,j})_{i,j\in[1,n]}.$$

(2.157) Definition (Matrixmultiplikation)**.** Es sei ein Körper K gegeben.

(a) Es seien $m, n, p \in \mathbb{N}_0$ gegeben. Für $A \in K^{n\times p}$, $B \in K^{m\times n}$ heißt $BA \in K^{m\times p}$ gegeben durch

$$BA = B \cdot A = (\sum_{j\in[1,n]} B_{i,j}A_{j,k})_{i\in[1,m],k\in[1,p]}$$

das *Matrixprodukt* von B und A.

(b) Es sei $n \in \mathbb{N}_0$ gegeben. Die Matrix $\mathrm{E}_n \in K^{n\times n}$ gegeben durch

$$\mathrm{E}_n = (\delta_{i,j})_{i,j\in[1,n]}$$

heißt *Einheitsmatrix* (genauer *n-te Einheitsmatrix* oder *n-te Identitätsmatrix*) über K.

Das Matrixprodukt BA von B mit A ist also nur definiert, falls die Anzahl der Spalten von B gleich der Anzahl der Zeilen von A ist. Dies ist ein Analogon zur Komposition von Abbildungen: Das Kompositum $g \circ f$ von g mit f ist nur definiert, falls die Startmenge von g gleich der Zielmenge von f ist.
Um den Eintrag an einer Stelle (i, k) von BA zu berechnen, müssen wir die i-te Zeile $B_{i,-}$ von B und die k-te Spalte $A_{-,k}$ von A betrachten. Dann bilden wir die Produkte $B_{i,j}A_{j,k}$ für alle j, d.h. wir gehen $B_{i,-}$ von links nach rechts und $A_{-,k}$ von oben nach unten durch und bilden $B_{i,1}A_{1,k}$, $B_{i,2}A_{2,k}$, usw. Die Summe all dieser Produkte ist dann gerade der Eintrag von BA an der Stelle (i, k).

(2.158) Beispiel.

(a) Es seien $A \in \mathbb{Q}^{4\times 2}$, $B \in \mathbb{Q}^{3\times 4}$ gegeben durch

$$A = \begin{pmatrix} 1 & 4 \\ 2 & 3 \\ 3 & 2 \\ 4 & 1 \end{pmatrix},\ B = \begin{pmatrix} 0 & 1 & 2 & 3 \\ -1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}.$$

Dann ist

$$BA = \begin{pmatrix} 20 & 10 \\ 3 & -3 \\ 3 & 7 \end{pmatrix}.$$

(b) Es ist $\mathrm{E}_3 \in \mathbb{Q}^{3\times 3}$ gegeben durch

$$\mathrm{E}_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Beweis.

(a) Es ist

$$\begin{aligned} BA &= \begin{pmatrix} 0 & 1 & 2 & 3 \\ -1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 4 \\ 2 & 3 \\ 3 & 2 \\ 4 & 1 \end{pmatrix} = \begin{pmatrix} 0\cdot 1+1\cdot 2+2\cdot 3+3\cdot 4 & 0\cdot 4+1\cdot 3+2\cdot 2+3\cdot 1 \\ (-1)\cdot 1+0\cdot 2+0\cdot 3+1\cdot 4 & (-1)\cdot 4+0\cdot 3+0\cdot 2+1\cdot 1 \\ 1\cdot 1+1\cdot 2+0\cdot 3+0\cdot 4 & 1\cdot 4+1\cdot 3+0\cdot 2+0\cdot 1 \end{pmatrix} \\ &= \begin{pmatrix} 20 & 10 \\ 3 & -3 \\ 3 & 7 \end{pmatrix}. \end{aligned}$$

□

(2.159) Proposition. Es sei ein Körper K gegeben.

(a) Es seien endlichdimensionale K-Vektorräume V, W, X, Vektorraumhomomorphismen $\varphi\colon V \to W$ und $\psi\colon W \to X$ über K, eine parametrisierte Basis $s = (s_k)_{k\in[1,p]}$ von V, eine parametrisierte Basis $t = (t_j)_{j\in[1,n]}$ von W und eine parametrisierte Basis $u = (u_i)_{i\in[1,m]}$ von X gegeben. Dann gilt

$$\mathrm{M}_u^s(\psi \circ \varphi) = \mathrm{M}_u^t(\psi)\,\mathrm{M}_t^s(\varphi).$$

(b) Es seien ein endlichdimensionaler K-Vektorraum V und eine parametrisierte Basis $s = (s_j)_{j\in[1,n]}$ von V gegeben. Dann gilt

$$\mathrm{M}_s^s(\mathrm{id}_V) = \mathrm{E}_n.$$

Beweis.

(a) Nach Bemerkung (2.154) gilt

$$\begin{aligned}\psi(\varphi(s_k)) &= \psi\Big(\sum_{j\in[1,n]} (\mathrm{M}_t^s(\varphi))_{j,k} t_j\Big) = \sum_{j\in[1,n]} (\mathrm{M}_t^s(\varphi))_{j,k}\,\psi(t_j) = \sum_{j\in[1,n]} (\mathrm{M}_t^s(\varphi))_{j,k} \sum_{i\in[1,m]} (\mathrm{M}_u^t(\psi))_{i,j} u_i \\ &= \sum_{i\in[1,m]} \Big(\sum_{j\in[1,n]} (\mathrm{M}_u^t(\psi))_{i,j} (\mathrm{M}_t^s(\varphi))_{j,k}\Big) u_i\end{aligned}$$

und damit

$$\mathrm{M}_u^s(\psi \circ \varphi) = \Big(\sum_{j\in[1,n]} (\mathrm{M}_u^t(\psi))_{i,j} (\mathrm{M}_t^s(\varphi))_{j,k}\Big)_{i\in[1,m],k\in[1,p]} = \mathrm{M}_u^t(\psi)\,\mathrm{M}_t^s(\varphi).$$

(b) Es gilt

$$\mathrm{id}_V(s_j) = \sum_{i\in[1,m]} \delta_{i,j} s_i$$

und damit

$$\mathrm{M}_s^s(\mathrm{id}_V) = \mathrm{E}_n$$

nach Bemerkung (2.154)(b). □

(2.160) Korollar. Es sei ein Körper K gegeben.

(a) Es seien endlichdimensionale K-Vektorräume V, W, X, eine parametrisierte Basis $s = (s_k)_{k\in[1,p]}$ von V, eine parametrisierte Basis $t = (t_j)_{j\in[1,n]}$ von W und eine parametrisierte Basis $u = (u_i)_{i\in[1,m]}$ von X gegeben. Für $A \in K^{n\times p}$, $B \in K^{m\times n}$ gilt

$$\varphi_{BA,s,u} = \varphi_{B,t,u} \circ \varphi_{A,s,t}.$$

(b) Es seien ein endlichdimensionaler K-Vektorraum V und eine parametrisierte Basis $s = (s_j)_{j\in[1,n]}$ von V gegeben. Dann gilt

$$\varphi_{\mathrm{E}_n,s,s} = \mathrm{id}_V.$$

Beweis.

(a) Nach Proposition (2.159)(a) gilt für $A \in K^{n\times p}$, $B \in K^{m\times n}$ stets

$$\mathrm{M}_u^s(\varphi_{BA,s,u}) = BA = \mathrm{M}_u^t(\varphi_{B,t,u})\,\mathrm{M}_t^s(\varphi_{A,s,t}) = \mathrm{M}_u^s(\varphi_{B,t,u} \circ \varphi_{A,s,t})$$

und damit

$$\varphi_{BA,s,u} = \varphi_{B,t,u} \circ \varphi_{A,s,t}.$$

(b) Nach Proposition (2.159)(b) gilt

$$\mathrm{M}_s^s(\varphi_{\mathrm{E}_n,s,s}) = \mathrm{E}_n = \mathrm{M}_s^s(\mathrm{id}_V)$$

und damit

$$\varphi_{\mathrm{E}_n,s,s} = \mathrm{id}_V.$$ □

(2.161) Proposition. Es sei ein Körper K gegeben.

(a) Es seien $m, n, p, q \in \mathbb{N}_0$ gegeben. Für $A \in K^{p\times q}$, $B \in K^{n\times p}$, $C \in K^{m\times n}$ gilt

$$C(BA) = (CB)A.$$

(b) Es seien $m, n \in \mathbb{N}_0$ gegeben. Für $A \in K^{m\times n}$ gilt

$$\mathrm{E}_m A = A\mathrm{E}_n = A.$$

(c) Es seien $m, n, p \in \mathbb{N}_0$ gegeben. Für $A, A' \in K^{n\times p}$, $B \in K^{m\times n}$ gilt

$$B(A + A') = BA + BA'.$$

Für $A \in K^{n\times p}$, $B, B' \in K^{m\times n}$ gilt

$$(B + B')A = BA + B'A.$$

(d) Es seien $m, n, p \in \mathbb{N}_0$ gegeben. Für $a \in K$, $A \in K^{n\times p}$, $B \in K^{m\times n}$ gilt

$$(aB)A = B(aA) = a(BA).$$

Beweis.

(a) Nach Korollar (2.155) und Proposition (2.159)(a) gilt für $A \in K^{p\times q}$, $B \in K^{n\times p}$, $C \in K^{m\times n}$ stets

$$\begin{aligned} C(BA) &= \mathrm{M}_\mathrm{e}^\mathrm{e}(\varphi_C)\,(\mathrm{M}_\mathrm{e}^\mathrm{e}(\varphi_B)\,\mathrm{M}_\mathrm{e}^\mathrm{e}(\varphi_A)) = \mathrm{M}_\mathrm{e}^\mathrm{e}(\varphi_C)\,\mathrm{M}_\mathrm{e}^\mathrm{e}(\varphi_B \circ \varphi_A) = \mathrm{M}_\mathrm{e}^\mathrm{e}(\varphi_C \circ (\varphi_B \circ \varphi_A)) \\ &= \mathrm{M}_\mathrm{e}^\mathrm{e}((\varphi_C \circ \varphi_B) \circ \varphi_A) = \mathrm{M}_\mathrm{e}^\mathrm{e}(\varphi_C \circ \varphi_B)\,\mathrm{M}_\mathrm{e}^\mathrm{e}(\varphi_A) = (\mathrm{M}_\mathrm{e}^\mathrm{e}(\varphi_C)\,\mathrm{M}_\mathrm{e}^\mathrm{e}(\varphi_B))\,\mathrm{M}_\mathrm{e}^\mathrm{e}(\varphi_A) = (CB)A. \end{aligned}$$

(b) Siehe Aufgabe 83(a).

(c) Siehe Aufgabe 83(b).

(d) Siehe Aufgabe 83(c). □

(2.162) Korollar. Es seien $n \in \mathbb{N}_0$ und ein Körper K gegeben. Die abelsche Gruppe $K^{n\times n}$ wird ein Ring mit Multiplikation gegeben durch Matrixmultiplikation. Die Eins von $K^{n\times n}$ ist gegeben durch

$$1^{K^{n\times n}} = \mathrm{E}_n.$$

Beweis. Dies folgt aus Proposition (2.161)(a), (b), (c). □

Ein $A \in K^{n\times n}$ ist invertierbar, falls ein $B \in K^{n\times n}$ mit $AB = BA = \mathrm{E}_n$ existiert. In diesem Fall ist das Inverse zu A eindeutig bestimmt und wird mit $A^{-1} = B$ bezeichnet.

(2.163) Definition (allgemeine lineare Matrixgruppe)**.** Es seien $n \in \mathbb{N}_0$ und ein Körper K gegeben. Die Gruppe

$$\mathrm{GL}_n(K) := (K^{n\times n})^\times$$

heißt *allgemeine lineare Gruppe* (oder *volle lineare Gruppe*) vom Grad n über K.

(2.164) Bemerkung. Es seien ein Körper K, endlichdimensionale K-Vektorräume V und W, ein K-Vektorraumisomorphismus $\varphi\colon V \to W$, eine parametrisierte Basis $s = (s_j)_{j\in[1,n]}$ von V und eine parametrisierte Basis $t = (t_i)_{i\in[1,n]}$ von W gegeben. Dann ist $\mathrm{M}_t^s(\varphi)$ invertierbar und es gilt

$$(\mathrm{M}_t^s(\varphi))^{-1} = \mathrm{M}_s^t(\varphi^{-1}).$$

Beweis. Es gilt

$$\mathrm{M}_s^t(\varphi^{-1})\,\mathrm{M}_t^s(\varphi) = \mathrm{M}_s^s(\varphi^{-1}\circ\varphi) = \mathrm{M}_s^s(\mathrm{id}_V) = \mathrm{E}_n,$$
$$\mathrm{M}_t^s(\varphi)\,\mathrm{M}_s^t(\varphi^{-1}) = \mathrm{M}_t^t(\varphi\circ\varphi^{-1}) = \mathrm{M}_t^t(\mathrm{id}_W) = \mathrm{E}_n.$$

Folglich ist $\mathrm{M}_t^s(\varphi)$ invertierbar mit $(\mathrm{M}_t^s(\varphi))^{-1} = \mathrm{M}_s^t(\varphi^{-1})$. □

(2.165) Bemerkung. Es seien ein Körper K, endlichdimensionale K-Vektorräume V und W, eine parametrisierte Basis $s = (s_j)_{j\in[1,n]}$ von V und eine parametrisierte Basis $t = (t_i)_{i\in[1,n]}$ gegeben. Für $A \in \mathrm{GL}_n(K)$ ist $\varphi_{A,s,t}\colon V \to W$ ein Isomorphismus mit

$$\varphi_{A,s,t}^{-1} = \varphi_{A^{-1},t,s}.$$

Beweis. Es sei ein invertierbares $A \in K^{m\times n}$ gegeben. Dann gilt

$$\varphi_{A^{-1},t,s}\circ\varphi_{A,s,t} = \varphi_{A^{-1}A,s,s} = \varphi_{\mathrm{E}_n,s,s} = \mathrm{id}_V,$$
$$\varphi_{A,s,t}\circ\varphi_{A^{-1},t,s} = \varphi_{AA^{-1},t,t} = \varphi_{\mathrm{E}_n,t,t} = \mathrm{id}_W.$$

Folglich ist $\varphi_{A,s,t}\colon V \to W$ ein Isomorphismus mit $\varphi_{A,s,t}^{-1} = \varphi_{A^{-1},t,s}$. □

Koordinatenspalten

(2.166) Definition (Koordinatenspalte)**.** Es seien ein Körper K, ein endlichdimensionaler K-Vektorraum V und eine parametrisierte Basis $s = (s_j)_{j\in[1,n]}$ von V gegeben. Wir bezeichnen mit

$$\kappa_s\colon V \to K^{n\times 1},\ v \mapsto \kappa_s(v)$$

den zu $K^{n\times 1} \to V,\ a \mapsto \sum_{j\in[1,n]} a_j s_j$ inversen K-Vektorraumisomorphismus. Für $v \in V$ heißt $\kappa_s(v)$ die *Koordinatenspalte* (oder der *Koordinatenvektor*) von v zur Basis s.

(2.167) Beispiel. Es sei ein Körper K gegeben. Die Koordinatenspalte von $x \in K^2$ bzgl. $s = ((1,0),(1,1))$ ist

$$\kappa_s(x) = \begin{pmatrix} x_1 - x_2 \\ x_2 \end{pmatrix}.$$

Beweis. Es ist

$$x = (x_1, x_2) = (x_1 - x_2)(1,0) + x_2(1,1)$$

und damit

$$\kappa_s(x) = \begin{pmatrix} x_1 - x_2 \\ x_2 \end{pmatrix}.$$ □

(2.168) Bemerkung. Es seien $n \in \mathbb{N}_0$ und ein Körper K gegeben. Für $x \in K^{n\times 1}$ gilt

$$\kappa_{\mathrm{e}_{K^{n\times 1}}}(x) = x.$$

Beweis. Es ist $x = \sum_{j\in[1,n]} x_j \mathrm{e}_j$ und damit

$$\kappa_{\mathrm{e}}(x) = x.$$ □

(2.169) Bemerkung. Es seien ein Körper K, ein endlichdimensionaler K-Vektorraum V und eine parametrisierte Basis $s = (s_j)_{j\in[1,n]}$ von V gegeben. Für $v \in V$ ist

$$\kappa_s(v) = \mathrm{M}_s^{(1)}(\rho_v),$$

wobei $\rho_v \colon K \to V$, $a \mapsto av$.

Beweis. Es sei $v \in V$ gegeben und es sei $\rho_v \colon K \to V$, $a \mapsto av$. Dann gilt

$$\rho_v(1) = v = \sum_{j\in[1,n]} (\kappa_s(v))_j s_j$$

und somit $\mathrm{M}_s^{(1)}(\rho_v) = \kappa_s(v)$ nach Bemerkung (2.154)(b). □

(2.170) Proposition. Es seien ein Körper K, endlichdimensionale K-Vektorräume V und W, ein K-Vektorraumhomomorphismus $\varphi \colon V \to W$, eine parametrisierte Basis $s = (s_j)_{j\in[1,n]}$ von V und eine parametrisierte Basis $t = (t_i)_{i\in[1,m]}$ von W gegeben. Für $v \in V$ gilt

$$\kappa_t(\varphi(v)) = \mathrm{M}_t^s(\varphi)\,\kappa_s(v).$$

Beweis. Es sei $v \in V$ gegeben und es sei $\rho_v \colon K \to V$, $a \mapsto av$ und $\rho_{\varphi(v)} \colon K \to W$, $a \mapsto a\,\varphi(v)$. Dann ist $\rho_{\varphi(v)} = \varphi \circ \rho_v$. Nach Bemerkung (2.169) und Proposition (2.159)(a) folgt

$$\mathrm{M}_t^s(\varphi)\,\kappa_s(v) = \mathrm{M}_t^s(\varphi)\,\mathrm{M}_s^{(1)}(\rho_v) = \mathrm{M}_t^{(1)}(\varphi \circ \rho_v) = \mathrm{M}_t^{(1)}(\rho_{\varphi(v)}) = \kappa_t(\varphi(v)).$$ □

(2.171) Korollar. Es seien ein Körper K, endlichdimensionale K-Vektorräume V und W, ein K-Vektorraumhomomorphismus $\varphi \colon V \to W$, eine parametrisierte Basis $s = (s_j)_{j\in[1,n]}$ von V und eine parametrisierte Basis $t = (t_i)_{i\in[1,m]}$ von W gegeben. Für $j \in [1,n]$ gilt

$$(\mathrm{M}_t^s(\varphi))_{-,j} = \kappa_t(\varphi(s_j)).$$

Beweis. Nach Proposition (2.170) gilt

$$\kappa_t(\varphi(s_j)) = \mathrm{M}_t^s(\varphi)\,\kappa_s(s_j) = \mathrm{M}_t^s(\varphi)\,\mathrm{e}_j = (\mathrm{M}_t^s(\varphi))_{-,j}$$

für $j \in [1,n]$. □

(2.172) Korollar. Es seien $m, n \in \mathbb{N}_0$, ein Körper K und $A \in K^{m\times n}$ gegeben. Für $x \in K^{n\times 1}$ gilt

$$\varphi_A(x) = Ax.$$

Beweis. Nach Proposition (2.170) gilt

$$\varphi_A(x) = \kappa_{\mathrm{e}}(\varphi_A(x)) = \mathrm{M}_{\mathrm{e}}^{\mathrm{e}}(\varphi_A)\,\kappa_{\mathrm{e}}(x) = Ax.$$ □

(2.173) Korollar. Es seien ein Körper K, endlichdimensionale K-Vektorräume V und W, ein K-Vektorraumhomomorphismus $\varphi \colon V \to W$, eine parametrisierte Basis $s = (s_j)_{j\in[1,n]}$ von V und eine parametrisierte Basis $t = (t_i)_{i\in[1,m]}$ von W gegeben. Dann gilt

$$\kappa_t \circ \varphi = \varphi_{\mathrm{M}_t^s(\varphi)} \circ \kappa_s.$$

$$\begin{array}{ccc} V & \xrightarrow[\cong]{\kappa_s} & K^{n\times 1} \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi_{\mathrm{M}_t^s(\varphi)}} \\ W & \xrightarrow[\cong]{\kappa_t} & K^{m\times 1} \end{array}$$

Beweis. Nach Proposition (2.170) und Korollar (2.172) gilt

$$\kappa_t(\varphi(v)) = \mathrm{M}_t^s(\varphi)\,\kappa_s(v) = \varphi_{\mathrm{M}_t^s(\varphi)}(\kappa_s(v))$$

für alle $v \in V$, also $\kappa_t \circ \varphi = \varphi_{\mathrm{M}_t^s(\varphi)} \circ \kappa_s$. □

Basiswechsel

(2.174) Definition (Basiswechselmatrix)**.** Es seien ein Körper K, ein endlichdimensionaler K-Vektorraum V und parametrisierte Basen $s = (s_j)_{j\in[1,n]}$ und $s' = (s'_j)_{j\in[1,n]}$ von V gegeben. Die Darstellungsmatrix $\mathrm{M}_s^{s'}(\mathrm{id}_V)$ heißt *Basiswechselmatrix* (oder *Transformationsmatrix*) zu den Basen s und s'.

(2.175) Beispiel. Es sei ein Körper K gegeben. Die Basiswechselmatrix zu den Basen e^{K^2} und $s = ((1,0),(1,1))$ von K^2 ist

$$\mathrm{M}_{\mathrm{e}}^{s}(\mathrm{id}_{K^2}) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Beweis. Es ist

$$s_1 = (1,0) = \mathrm{e}_1,$$
$$s_2 = (1,1) = \mathrm{e}_1 + \mathrm{e}_2,$$

und damit

$$\mathrm{M}_{\mathrm{e}}^{s}(\mathrm{id}_{K^2}) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$ □

(2.176) Bemerkung. Es seien ein Körper K, ein endlichdimensionaler K-Vektorraum V und parametrisierte Basen $s = (s_j)_{j\in[1,n]}$ und $s' = (s'_j)_{j\in[1,n]}$ von V gegeben. Die Basiswechselmatrix $\mathrm{M}_s^{s'}(\mathrm{id}_V)$ ist invertierbar mit

$$(\mathrm{M}_s^{s'}(\mathrm{id}_V))^{-1} = \mathrm{M}_{s'}^{s}(\mathrm{id}_V)$$

Beweis. Dies folgt aus Bemerkung (2.164). □

(2.177) Proposition. Es sei ein Körper K gegeben.

(a) Es seien ein endlichdimensionaler K-Vektorraum V und parametrisierte Basen $s = (s_j)_{j\in[1,n]}$ und $s' = (s'_j)_{j\in[1,n]}$ von V gegeben. Für $v \in V$ gilt

$$\kappa_{s'}(v) = (\mathrm{M}_s^{s'}(\mathrm{id}_V))^{-1}\kappa_s(v).$$

(b) Es seien endlichdimensionale K-Vektorräume V und W, ein K-Vektorraumhomomorphismus $\varphi\colon V \to W$, parametrisierte Basen $s = (s_j)_{j\in[1,n]}$ und $s' = (s'_j)_{j\in[1,n]}$ von V und parametrisierte Basen $t = (t_i)_{i\in[1,m]}$ und $t' = (t'_i)_{i\in[1,m]}$ von W gegeben. Dann gilt

$$\mathrm{M}_{t'}^{s'}(\varphi) = (\mathrm{M}_t^{t'}(\mathrm{id}_W))^{-1}\,\mathrm{M}_t^{s}(\varphi)\,\mathrm{M}_s^{s'}(\mathrm{id}_V).$$

Beweis.

(a) Nach Proposition (2.170) und Bemerkung (2.176) gilt

$$\kappa_{s'}(v) = \kappa_{s'}(\mathrm{id}_V(v)) = \mathrm{M}_{s'}^{s}(\mathrm{id}_V)\,\kappa_{s'}(v) = (\mathrm{M}_s^{s'}(\mathrm{id}_V))^{-1}\kappa_s(v).$$

(b) Nach Proposition (2.159)(a) und Bemerkung (2.176) gilt

$$\mathrm{M}_{t'}^{s'}(\varphi) = \mathrm{M}_{t'}^{s'}(\mathrm{id}_W \circ \varphi \circ \mathrm{id}_V) = \mathrm{M}_{t'}^{t}(\mathrm{id}_W)\,\mathrm{M}_t^{s}(\varphi)\,\mathrm{M}_s^{s'}(\mathrm{id}_V) = (\mathrm{M}_t^{t'}(\mathrm{id}_W))^{-1}\,\mathrm{M}_t^{s}(\varphi)\,\mathrm{M}_s^{s'}(\mathrm{id}_V).$$ □

Ein Vektorraumendomorphismus eines Vektorraums V ist ein Vektorraumhomomorphismus von V nach V.

(2.178) Korollar. Es seien ein Körper K, ein endlichdimensionaler K-Vektorraum V, ein K-Vektorraumendomorphismus $\varphi\colon V \to V$ und parametrisierte Basen $s = (s_j)_{j\in[1,n]}$ und $s' = (s'_j)_{j\in[1,n]}$ von V gegeben. Dann gilt

$$\mathrm{M}_{s'}^{s'}(\varphi) = (\mathrm{M}_s^{s'}(\mathrm{id}_V))^{-1}\,\mathrm{M}_s^{s}(\varphi)\,\mathrm{M}_s^{s'}(\mathrm{id}_V).$$

Beweis. Dies folgt aus Proposition (2.177)(b). □

(2.179) Beispiel. Es seien $A \in \mathbb{R}^{2\times 2}$ und $s = (s_1, s_2)$ in $\mathbb{R}^{2\times 1}$ gegeben durch

$$A = \frac{1}{5}\begin{pmatrix} -3 & 4 \\ 4 & 3 \end{pmatrix},\ s = (\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} -2 \\ 1 \end{pmatrix}).$$

Dann ist

$$\mathrm{M}_s^s(\varphi_A) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Beweis. Es ist

$$\mathrm{M}_{\mathrm{e}}^s(\mathrm{id}_{\mathbb{R}^{2\times 1}}) = \begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix}.$$

Wegen

$$\begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}\begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix}$$

gilt

$$(\mathrm{M}_{\mathrm{e}}^s(\mathrm{id}_{\mathbb{R}^{2\times 1}}))^{-1} = \begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix}^{-1} = \frac{1}{5}\begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}$$

und damit

$$\begin{aligned}\mathrm{M}_s^s(\varphi_A) &= (\mathrm{M}_{\mathrm{e}}^s(\mathrm{id}_{\mathbb{R}^{2\times 1}}))^{-1}\,\mathrm{M}_{\mathrm{e}}^{\mathrm{e}}(\varphi_A)\,\mathrm{M}_{\mathrm{e}}^s(\mathrm{id}_{\mathbb{R}^{2\times 1}}) = \frac{1}{5}\begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}\frac{1}{5}\begin{pmatrix} -3 & 4 \\ 4 & 3 \end{pmatrix}\begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix} \\ &= \frac{1}{5}\begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}\frac{1}{5}\begin{pmatrix} 5 & 10 \\ 10 & -5 \end{pmatrix} = \frac{1}{5}\begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 2 & -1 \end{pmatrix} = \frac{1}{5}\begin{pmatrix} 5 & 0 \\ 0 & -5 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\end{aligned}$$

nach Korollar (2.178). □

Quasieinheitsmatrizen

(2.180) Definition (Quasieinheitsmatrix)**.** Es seien $m, n, r \in \mathbb{N}_0$ mit $r \leq \min(m, n)$ und ein Körper K gegeben. Die Matrix $\mathrm{Q}_r \in K^{m\times n}$ gegeben durch

$$\mathrm{Q}_r := \begin{pmatrix} \mathrm{E}_r & 0 \\ 0 & 0 \end{pmatrix}$$

heißt *Quasieinheitsmatrix*.

(2.181) Beispiel. Es ist $\mathrm{Q}_2 \in \mathbb{Q}^{3\times 4}$ gegeben durch

$$\mathrm{Q}_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

(2.182) Satz. Es seien ein Körper K und endlichdimensionale K-Vektorräume V und W gegeben. Für jeden K-Vektorraumhomomorphismus $\varphi\colon V \to W$ gibt es eine parametrisierte Basis $s = (s_j)_{j\in[1,\dim_K V]}$ von V und eine parametrisierte Basis $t = (t_i)_{i\in[1,\dim_K W]}$ von W so, dass

$$\mathrm{M}_t^s(\varphi) = \mathrm{Q}_{\dim_K(\mathrm{Im}\,\varphi)}$$

ist.

Beweis. Nach Proposition (2.139) ist $\operatorname{Ker}\varphi$ ein endlichdimensionaler Untervektorraum von V mit $\dim(\operatorname{Ker}\varphi) \leq \dim V$, es ist $\operatorname{Im}\varphi$ ein endlichdimensionaler Untervektorraum von W mit $\dim(\operatorname{Im}\varphi) \leq \dim W$, und es gilt

$$\dim V = \dim(\operatorname{Ker}\varphi) + \dim(\operatorname{Im}\varphi).$$

Nach Korollar (2.124) gibt es daher eine parametrisierte Basis $s = (s_j)_{j\in[1,\dim V]}$ von V derart, dass $(s_j)_{j\in[\dim V-\dim(\operatorname{Ker}\varphi)+1,\dim V]}$ eine parametrisierte Basis von $\operatorname{Ker}\varphi$ ist. Es ist $(\varphi(s_k))_{k\in[1,\dim(\operatorname{Im}\varphi)]}$ eine Basis von $\operatorname{Im}\varphi$ nach Proposition (2.115). Nach Korollar (2.124) gibt es eine parametrisierte Basis $t = (t_i)_{i\in[1,\dim W]}$ von W mit $t_k = \varphi(s_k)$ für $k \in [1, \dim(\operatorname{Im}\varphi)]$.
Für $j \in [1, \dim V]$ gilt nun

$$\varphi(s_j) = \begin{cases} t_j, & \text{falls } j \in [1, \dim(\operatorname{Im}\varphi)], \\ 0, & \text{falls } j \in [\dim(\operatorname{Im}\varphi)+1, \dim V] \end{cases}$$

und damit

$$\mathrm{M}_t^s(\varphi) = \begin{pmatrix} \mathrm{E}_r & 0 \\ 0 & 0 \end{pmatrix} = \mathrm{Q}_{\dim_K(\operatorname{Im}\varphi)}. \qquad \square$$

Aufgaben

Aufgabe 79 (lineare Gleichungssysteme und Homomorphismen)**.** Es seien $m, n \in \mathbb{N}_0$, ein Körper K und ein $A \in K^{m\times n}$ gegeben.

(a) Zeigen Sie: Für $b \in K^{m\times 1}$ ist $\operatorname{Sol}(A,b) = \varphi_A^{-1}(\{b\})$. Insbesondere ist $\operatorname{Sol}_0(A) = \operatorname{Ker}\varphi_A$.

(b) Zeigen Sie, dass $\operatorname{Sol}_0(A)$ ein K-Untervektorraum von $K^{n\times 1}$ ist.

(c) Es seien $b \in K^{m\times 1}$ und $\bar{x} \in \operatorname{Sol}(A,b)$, d.h. eine Lösung $\bar{x}$ des linearen Gleichungssystems zur erweiterten Koeffizientenmatrix $\left(A \mid b\right)$, gegeben. Zeigen Sie, dass

$$\operatorname{Sol}(A,b) = \bar{x} + \operatorname{Sol}_0(A)$$

ist.

(d) Für $b \in K^{m\times 1}$ sind die folgenden Bedingungen sind äquivalent.

(i) Das lineare Gleichungssystem zur erweiterten Koeffizientenmatrix $\left(A \mid b\right)$ besitzt eine Lösung.

(ii) Es ist $b \in \operatorname{Im}\varphi_A$.

(iii) Es ist $\mathrm{C}(\left(A \mid b\right)) = \mathrm{C}(A)$.

Aufgabe 80 (Kern, Fasern und Linearkombinationen)**.** Es seien $A \in \mathbb{F}_5^{4\times 5}$, $b_1, b_2 \in \mathbb{F}_5^{4\times 1}$, $c \in \mathbb{F}_5^{5\times 1}$, $S \subseteq \mathbb{F}_5^{5\times 1}$ gegeben durch

$$A := \begin{pmatrix} 1 & 0 & 1 & -2 & 1 \\ 1 & 2 & 0 & -1 & 0 \\ -1 & -2 & 0 & 1 & 2 \\ 1 & -1 & -1 & 0 & -2 \end{pmatrix}, \; b_1 := \begin{pmatrix} 2 \\ 1 \\ 1 \\ -1 \end{pmatrix}, \; b_2 := \begin{pmatrix} 2 \\ -1 \\ 0 \\ -2 \end{pmatrix}, \; c := \begin{pmatrix} 1 \\ 1 \\ -2 \\ 1 \\ 1 \end{pmatrix},$$

$$S := \left\{ \begin{pmatrix} 1 \\ 0 \\ 1 \\ -2 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ 0 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ -2 \\ 0 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ -1 \\ 0 \\ -2 \end{pmatrix} \right\}.$$

(a) Bestimmen Sie eine Basis von $\operatorname{Ker}\varphi_A$.

(b) Ist $b_i \in \operatorname{Im}\varphi_A$ für $i \in \{1,2\}$? Falls ja, berechnen Sie die Faser $\varphi_A^{-1}(\{b_i\})$.

(c) Ist c eine Linearkombination von S?

Aufgabe 81 (Darstellungsmatrix)**.** Es seien $A \in \mathbb{Q}^{3\times 4}$, $s = (s_1, s_2, s_3, s_4)$ in $\mathbb{Q}^{4\times 1}$ und $t = (t_1, t_2, t_3)$ in $\mathbb{Q}^{3\times 1}$ gegeben durch

$$A = \begin{pmatrix} -5 & -4 & -7 & -6 \\ -4 & 0 & -12 & -8 \\ -1 & 2 & -7 & -4 \end{pmatrix},\ s = (\begin{pmatrix} -8 \\ 5 \\ 3 \\ -1 \end{pmatrix}, \begin{pmatrix} 8 \\ -7 \\ -5 \\ 4 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix}, \begin{pmatrix} -4 \\ 3 \\ 2 \\ -1 \end{pmatrix}),\ t = (\begin{pmatrix} 5 \\ 4 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ -4 \\ -3 \end{pmatrix}, \begin{pmatrix} -1 \\ -2 \\ -1 \end{pmatrix}).$$

(a) Zeigen Sie, dass s eine Basis von $\mathbb{Q}^{4\times 1}$ und t eine Basis von $\mathbb{Q}^{3\times 1}$ ist.

(b) Bestimmen Sie die Darstellungsmatrix $\mathrm{M}_t^s(\varphi_A)$ von $\varphi_A \colon \mathbb{Q}^{4\times 1} \to \mathbb{Q}^{3\times 1}$ bzgl. der Basen s und t.

Aufgabe 82 (Matrixmultiplikation)**.** Es seien die folgenden Matrizen mit Einträgen in $\mathbb{Q}$ gegeben.

$$A = \begin{pmatrix} 1 & -3 & 7 & -2 \end{pmatrix},\ B = \begin{pmatrix} 0 & 1 \\ 2 & -3 \\ 4 & 2 \\ -2 & 5 \end{pmatrix},\ C = \begin{pmatrix} 5 \\ 1 \\ 3 \end{pmatrix},\ D = \begin{pmatrix} -1 & 0 \\ 2 & 1 \end{pmatrix},\ E = \begin{pmatrix} -1 & 5 & 0 \\ 0 & -3 & 1 \end{pmatrix}.$$

(a) Berechnen Sie alle definierten Produkte der gegebenen Matrizen (auch Produkte aus mehr als zwei Faktoren, sofern definiert), welche folgender Zusatzbedingung genügen: In keinem Produkt soll eine Einheitsmatrix oder eine Nullmatrix als echtes „Teilprodukt“ vorkommen. (Denn ist für Matrizen X und Y etwa XY eine Einheitsmatrix, so auch $XYXY$, $XYXYXY$, ...)

(b) Es seien $n \in \mathbb{N}$ und ein Körper K gegeben. Eine Matrix $N \in K^{n\times n}$ heißt *nilpotent*, falls es ein $k \in \mathbb{N}$ mit $N^k = 0$ gibt.

Zeigen Sie, dass das Produkt aus (a) mit der größten Anzahl an Faktoren nilpotent ist.

Aufgabe 83 (Rechenregeln für die Matrixmultiplikation)**.** Es sei ein Körper K gegeben.

(a) Es seien $m, n \in \mathbb{N}_0$ gegeben. Zeigen Sie: Für $A \in K^{m\times n}$ gilt

$$\mathrm{E}_m A = A\mathrm{E}_n = A.$$

(b) Es seien $m, n, p \in \mathbb{N}_0$ gegeben. Zeigen Sie: Für $A, A' \in K^{n\times p}$, $B \in K^{m\times n}$ gilt

$$B(A + A') = BA + BA'.$$

Für $A \in K^{n\times p}$, $B, B' \in K^{m\times n}$ gilt

$$(B + B')A = BA + B'A.$$

(c) Es seien $m, n, p \in \mathbb{N}_0$ gegeben. Zeigen Sie: Für $a \in K$, $A \in K^{n\times p}$, $B \in K^{m\times n}$ gilt

$$B(aA) = (aB)A = a(BA).$$

Aufgabe 84 (Basiswechsel)**.** Es seien Basen $s = (s_1, s_2, s_3)$ und $s' = (s'_1, s'_2, s'_3)$ von $\mathbb{R}^{3\times 1}$ gegeben durch

$$s = (\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}),\ s' = (\begin{pmatrix} 1 \\ \sqrt{2} \\ -\sqrt{2} \end{pmatrix}, \begin{pmatrix} \sqrt{2} \\ 3 \\ -2+\sqrt{2} \end{pmatrix}, \begin{pmatrix} -\sqrt{2} \\ -2+\sqrt{2} \\ 5 \end{pmatrix}).$$

Ferner sei ein $\mathbb{R}$-Vektorraumendomorphismus $\varphi \colon \mathbb{R}^{3\times 1} \to \mathbb{R}^{3\times 1}$ gegeben durch

$$\varphi(a_1 \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + a_2 \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + a_3 \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}) = b_1 \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + b_2 \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + b_3 \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

für $a_1, a_2, a_3 \in \mathbb{R}$, wobei

$$\begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} = \begin{pmatrix} 3+2\sqrt{2} & -1+\sqrt{2} & \sqrt{2} \\ 3-7\sqrt{2} & 9-4\sqrt{2} & 2-3\sqrt{2} \\ -26+4\sqrt{2} & -14+10\sqrt{2} & -8+2\sqrt{2} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}.$$

Berechnen Sie die Darstellungsmatrix A von φ bzgl. s (und s), die Basiswechselmatrix zum Basiswechsel von s zu s' und deren Inverse, die Darstellungsmatrix von φ bzgl. s' (und s') sowie Basen von $\operatorname{Ker}\varphi$ und $\operatorname{Im}\varphi$.
Zur Kontrolle. Die Summe der Einträge von $\mathrm{M}_{s'}^{s'}(\varphi)$ ist 5.

Aufgabe 85 (Matrixkalkül in abstrakten Vektorräumen)**.** Es seien ein Körper K, Vektorräume V und W über K, eine Basis $s = (s_1, s_2, s_3)$ von V und eine Basis $t = (t_1, t_2, t_3, t_4)$ von W gegeben. Ferner sei $\varphi\colon V \to W$ der eindeutige K-Vektorraumhomomorphismus mit

$$\varphi(s_1) = -2t_1 + t_3 + 2t_4,\ \varphi(s_2) = t_2 + t_3 + t_4,\ \varphi(s_3) = -2t_1 - t_2 + t_4.$$

Schließlich seien $s' = (s'_1, s'_2, s'_3)$ in V und $t' = (t'_1, t'_2, t'_3, t'_4)$ in W gegeben durch

$$s' = (s_1, -s_1 + s_2, -s_1 + s_2 + s_3),\ t' = (-2t_1 + t_3 + 2t_4, 2t_1 + t_2 - t_4, t_1, t_4).$$

(a) Bestimmen Sie die Darstellungsmatrix von φ bzgl. s und t.

(b) Zeigen Sie, dass s' eine Basis von V und t' eine Basis von W ist.

(c) Berechnen Sie die Darstellungsmatrix von φ bzgl. s' und t'.

(d) Bestimmen Sie $\dim_K(\operatorname{Ker}\varphi)$ und $\dim_K(\operatorname{Im}\varphi)$.

Aufgabe 86 (invertierbare Matrizen als Basiswechselmatrizen)**.** Es seien ein Körper K, ein endlichdimensionaler K-Vektorraum V und eine parametrisierte Basis $s = (s_j)_{j\in[1,n]}$ von V gegeben. Zeigen Sie, dass es für alle $A \in \mathrm{GL}_n(K)$ genau eine parametrisierte Basis $s' = (s'_j)_{j\in[1,n]}$ von V mit $A = \mathrm{M}_s^{s'}(\mathrm{id}_V)$ gibt.

Aufgabe 87 ((schief-)symmetrische Matrizen)**.** Es seien $n \in \mathbb{N}$ und ein Körper K gegeben. Für $A \in K^{n\times n}$ ist die *transponierte Matrix* $A^{\mathrm{tr}} \in K^{n\times n}$ definiert durch $A^{\mathrm{tr}}_{i,j} = A_{j,i}$ für $i, j \in [1, n]$. Ferner setzen wir $K^{n\times n}_{\mathrm{sym}} := \{A \in K^{n\times n} \mid A^{\mathrm{tr}} = A\}$ und $K^{n\times n}_{\mathrm{skew}} := \{A \in K^{n\times n} \mid A^{\mathrm{tr}} = -A\}$.

(a) Zeigen Sie, dass $K^{n\times n}_{\mathrm{sym}}$ und $K^{n\times n}_{\mathrm{skew}}$ Untervektorräume von $K^{n\times n}$ sind.

(b) Bestimmen Sie eine Basis S von $\mathbb{Q}^{3\times 3}_{\mathrm{sym}}$ und eine Basis T von $\mathbb{Q}^{3\times 3}_{\mathrm{skew}}$. Zeigen Sie, dass $S \cup T$ (für Ihre Wahl von S und T) eine Basis von $\mathbb{Q}^{3\times 3}$ ist.

(c) Bestimmen Sie eine Basis S von $(\mathbb{F}_2)^{3\times 3}_{\mathrm{sym}}$ und eine Basis T von $(\mathbb{F}_2)^{3\times 3}_{\mathrm{skew}}$. Ist $S \cup T$ eine Basis von $(\mathbb{F}_2)^{3\times 3}$?

Aufgabe 88 (Elementarmatrizen)**.**

(a) Es seien $m, n \in \mathbb{N}_0$ und ein Körper K gegeben. Zeigen Sie: Für jeden Zeilenoperator ρ auf $K^{m\times n}$ ist $\rho(\mathrm{E}_m) \in \mathrm{GL}_m(K)$ und für $A \in K^{m\times n}$ gilt

$$\rho(A) = \rho(\mathrm{E}_m)A.$$

(b) Es sei $A \in \mathbb{F}_5^{3\times 4}$ gegeben durch

$$A = \begin{pmatrix} 2 & 2 & 1 & -1 \\ -1 & -2 & 1 & -1 \\ 1 & -2 & 0 & 2 \end{pmatrix}.$$

Berechnen Sie $P \in \mathrm{GL}_3(\mathbb{F}_5)$ so, dass PA in reduzierter Zeilenstufenform ist.

7 Äquivalenz und der Rang von Matrizen

Äquivalenz von Matrizen

(2.183) Definition (Äquivalenz von Matrizen)**.** Es seien $m, n \in \mathbb{N}_0$ und ein Körper K gegeben. Für $A, B \in K^{m\times n}$ sagen wir, dass A *äquivalent* zu B ist, wenn es $P \in \mathrm{GL}_n(K)$, $Q \in \mathrm{GL}_m(K)$ mit

$$Q^{-1}AP = B$$

gibt.

(2.184) Bemerkung. Es seien $m, n \in \mathbb{N}_0$ und ein Körper K gegeben. Äquivalenz von Matrizen ist eine Äquivalenzrelation auf $K^{m\times n}$.

Beweis. Es seien $A, B, C \in K^{m\times n}$ so gegeben, dass A äquivalent zu B und B äquivalent zu C ist. Dann gibt es $P, R \in \mathrm{GL}_n(K)$ und $Q, S \in \mathrm{GL}_m(K)$ mit $Q^{-1}AP = B$ und $S^{-1}BR = C$. Es folgt

$$(QS)^{-1}A(PR) = S^{-1}Q^{-1}APR = S^{-1}BR = C,$$

also A äquivalent zu C. Folglich ist Äquivalenz von Matrizen transitiv.
Für $A \in K^{m\times n}$ gilt $\mathrm{E}_m^{-1}A\mathrm{E}_n = A$, also A äquivalent zu A. Folglich ist Äquivalenz von Matrizen reflexiv.
Es seien $A, B \in K^{m\times n}$ so gegeben, dass A äquivalent zu B ist. Dann gibt es $P \in \mathrm{GL}_n(K)$, $Q \in \mathrm{GL}_m(K)$ mit $Q^{-1}AP = B$. Es folgt $(Q^{-1})^{-1}BP^{-1} = A$, also B äquivalent zu A. Folglich ist Äquivalenz von Matrizen symmetrisch.
Insgesamt ist Äquivalenz von Matrizen eine Äquivalenzrelation auf $K^{m\times n}$. □

(2.185) Bemerkung. Es seien ein Körper K, endlichdimensionale K-Vektorräume V und W, ein K-Vektorraumhomomorphismus $\varphi\colon V \to W$, parametrisierte Basen $s = (s_j)_{j\in[1,n]}$ und $s' = (s'_j)_{j\in[1,n]}$ von V und parametrisierte Basen $t = (t_i)_{i\in[1,m]}$ und $t' = (t'_i)_{i\in[1,m]}$ von W gegeben. Dann ist $\mathrm{M}_t^s(\varphi)$ äquivalent zu $\mathrm{M}_{t'}^{s'}(\varphi)$.

Beweis. Nach Proposition (2.177)(b) gilt

$$\mathrm{M}_{t'}^{s'}(\varphi) = (\mathrm{M}_t^{t'}(\mathrm{id}_V))^{-1}\,\mathrm{M}_t^s(\varphi)\,\mathrm{M}_s^{s'}(\mathrm{id}_V).$$

Insbesondere ist $\mathrm{M}_t^s(\varphi)$ äquivalent zu $\mathrm{M}_{t'}^{s'}(\varphi)$. □

(2.186) Bemerkung. Es seien $m, n \in \mathbb{N}_0$, ein Körper K und $A, B \in K^{m\times n}$ gegeben. Genau dann ist A äquivalent zu B, wenn es $P \in \mathrm{GL}_n(K)$, $Q \in \mathrm{GL}_m(K)$ mit

$$QAP = B$$

gibt.

Unser Ziel ist es, $(m \times n)$-Matrizen für $m, n \in \mathbb{N}_0$ bis auf Äquivalenz zu charakterisieren. Wir gehen also der Frage nach, wie die Elemente von $K^{m\times n}$ modulo Äquivalenz von Matrizen aussehen.

Spaltenraum

(2.187) Definition (Spaltenraum)**.** Es seien $m, n \in \mathbb{N}_0$, ein Körper K und $A \in K^{m\times n}$ gegeben. Der K-Untervektorraum

$$\mathrm{C}(A) := \mathrm{Im}\,\varphi_A$$

von $K^{m\times 1}$ heißt *Spaltenraum* von A.

Für $m, n \in \mathbb{N}$, $A \in K^{m\times n}$ gilt also

$$\mathrm{C}(A) = \mathrm{Im}\,\varphi_A = \{\varphi_A(x) \mid x \in K^{n\times 1}\} = \{Ax \mid x \in K^{n\times 1}\}.$$

(2.188) Bemerkung. Es seien $m, n \in \mathbb{N}_0$, ein Körper K und ein $A \in K^{m\times n}$ gegeben. Dann ist

$$\mathrm{C}(A) = \langle A_{-,j} \mid j \in [1, n]\rangle.$$

Beweis. Siehe Aufgabe 89. □

(2.189) Bemerkung. Es seien $m, n, p \in \mathbb{N}_0$, ein Körper K und $A \in K^{n\times p}$, $B \in K^{m\times n}$ gegeben. Dann ist $\mathrm{C}(BA)$ ein K-Untervektorraum von $\mathrm{C}(B)$.

Beweis. Nach Korollar (2.172) ist

$$\mathrm{C}(BA) = \mathrm{Im}\,\varphi_{BA} = \mathrm{Im}(\varphi_B \circ \varphi_A) \subseteq \mathrm{Im}\,\varphi_B = \mathrm{C}(B).$$

Da sowohl $\mathrm{C}(BA)$ als auch $\mathrm{C}(B)$ Untervektorräume von $K^{m\times 1}$ sind, ist folglich $\mathrm{C}(BA)$ ein Untervektorraum von $\mathrm{C}(B)$. □

(2.190) Korollar. Es seien $m, n \in \mathbb{N}_0$, ein Körper K und $A \in K^{m\times n}$, $P \in \mathrm{GL}_n(K)$ gegeben. Dann ist

$$\mathrm{C}(AP) = \mathrm{C}(A).$$

Beweis. Nach Bemerkung (2.189) gilt $\mathrm{C}(AP) \leq \mathrm{C}(A)$ und $\mathrm{C}(A) = \mathrm{C}(APP^{-1}) \leq \mathrm{C}(AP)$, also $\mathrm{C}(AP) = \mathrm{C}(A)$. □

(2.191) Bemerkung. Es seien $m, n \in \mathbb{N}_0$, ein Körper K und $A \in K^{m\times n}$, $P \in \mathrm{GL}_m(K)$ gegeben. Dann ist

$$\varphi_P|^{\mathrm{C}(PA)}_{\mathrm{C}(A)} \colon \mathrm{C}(A) \to \mathrm{C}(PA)$$

ein wohldefinierter K-Vektorraumisomorphismus.

Beweis. Auf Grund der Invertierbarkeit von P ist $\varphi_P \colon K^{m\times 1} \to K^{m\times 1}$, $y \mapsto Py$ ein Isomorphismus. Nach Korollar (2.172) ist

$$\varphi_P(\mathrm{C}(A)) = \varphi_P(\mathrm{Im}\,\varphi_A) = \mathrm{Im}(\varphi_P \circ \varphi_A) = \mathrm{Im}(\varphi_{PA}) = \mathrm{C}(PA),$$

so dass $\varphi_P \colon K^{m\times 1} \to K^{m\times 1}$ zu einem surjektiven Homomorphismus $\varphi_P|^{\mathrm{C}(PA)}_{\mathrm{C}(A)} \colon \mathrm{C}(A) \to \mathrm{C}(PA)$ einschränkt. Die Injektivität von φ_P impliziert ferner die Injektivität von $\varphi_P|^{\mathrm{C}(PA)}_{\mathrm{C}(A)}$. Insgesamt ist $\varphi_P|^{\mathrm{C}(PA)}_{\mathrm{C}(A)}$ bijektiv und daher ein Isomorphismus nach Bemerkung (2.40). □

Rang einer Matrix

(2.192) Definition (Rang)**.** Es seien $m, n \in \mathbb{N}_0$, ein Körper K und eine Matrix $A \in K^{m\times n}$ gegeben. Der *Rang* (oder *Spaltenrang*) von A ist definiert als

$$\mathrm{rk}\, A := \mathrm{rk}\, \varphi_A.$$

(2.193) Bemerkung. Es seien $m, n \in \mathbb{N}_0$ und ein Körper K gegeben. Für $A \in K^{m\times n}$ gilt

$$\mathrm{rk}\, A = \dim_K \mathrm{C}(A).$$

Beweis. Für $A \in K^{m\times n}$ gilt

$$\mathrm{rk}\, A = \mathrm{rk}\, \varphi_A = \dim(\mathrm{Im}\,\varphi_A) = \dim \mathrm{C}(A).$$ □

(2.194) Beispiel. Es seien $m, n, r \in \mathbb{N}_0$ mit $r \leq \min(m, n)$ und ein Körper K gegeben. Es ist

$$\mathrm{rk}\, \mathrm{Q}_r = r.$$

(2.195) Proposition. Es seien $m, n, p \in \mathbb{N}_0$ und ein Körper K gegeben. Für $A \in K^{n\times p}$, $B \in K^{m\times n}$ gilt

$$\mathrm{rk}(BA) \leq \min(\mathrm{rk}\, B, \mathrm{rk}\, A).$$

Beweis. Siehe Aufgabe 91. □

(2.196) Bemerkung. Es seien $n \in \mathbb{N}_0$, ein Körper K und ein $A \in K^{n\times n}$ gegeben. Genau dann ist A invertierbar, wenn

$$\mathrm{rk}\, A = n$$

ist.

Beweis. Nach Bemerkung (2.164) und Korollar (2.172) ist A genau dann invertierbar, wenn $\varphi_A \colon K^{n\times 1} \to K^{n\times 1}$, $x \mapsto Ax$ ein Isomorphismus ist, nach Korollar (2.64) also genau dann, wenn $\mathrm{Ker}\,\varphi_A = \{0\}$ und $\mathrm{Im}\,\varphi_A = K^{n\times 1}$ ist. Nach Proposition (2.139) ist dies äquivalent zu $\dim(\mathrm{Ker}\,\varphi_A) = 0$ und $\dim(\mathrm{Im}\,\varphi_A) = n$. Nun ist jedoch

$$n = \dim K^{n\times 1} = \dim(\mathrm{Ker}\,\varphi_A) + \dim(\mathrm{Im}\,\varphi_A),$$

es gilt also genau dann $\dim(\mathrm{Ker}\,\varphi_A) = 0$, wenn $\dim(\mathrm{Im}\,\varphi_A) = n$ ist. Wegen $\mathrm{rk}\, A = \dim(\mathrm{Im}\,\varphi_A)$ ist folglich A genau dann invertierbar, wenn $\mathrm{rk}\, A = n$ ist. □

(2.197) Korollar. Es seien $n \in \mathbb{N}_0$, ein Körper K und ein $A \in K^{n\times n}$ gegeben. Die folgenden Bedingungen sind äquivalent.

(a) Es ist A invertierbar.

(b) Es existiert ein zu A linksinverses Element in $K^{n\times n}$ bzgl. der Matrixmultiplikation.

(c) Es existiert ein zu A rechtsinverses Element in $K^{n\times n}$ bzgl. der Matrixmultiplikation.

Beweis. Wenn Bedingung (a) gilt, so auch insbesondere Bedingung (b). Es gelte also Bedingung (b), d.h. es existiere ein zu A linksinverses Element B in $K^{n\times n}$ bzgl. der Matrixmultiplikation. Dann gilt $BA = \mathrm{E}_n$, nach Proposition (2.195) also

$$n = \operatorname{rk} \mathrm{E}_n = \operatorname{rk}(BA) \leq \operatorname{rk} A.$$

Da aber stets auch $\operatorname{rk} A \leq n$ ist, folgt $\operatorname{rk} A = n$. Nach Bemerkung (2.196) ist A invertierbar, d.h. Bedingung (a) gilt.
Die Äquivalenz von Bedingung (a) und Bedingung (c) lässt sich analog zeigen.
Insgesamt sind Bedingung (a), Bedingung (b) und Bedingung (c) äquivalent. □

Korollar (2.197) liefert uns eine Methode zur Berechnung der Inversen einer Matrix $A \in K^{n\times n}$ über einem Körper K mittels Gauß-Algorithmus. Für alle $j \in [1, n]$ gilt $A(A^{-1})_{-,j} = (\mathrm{E}_n)_{-,j} = \mathrm{e}_j$. Um die Spalten von A^{-1} zu berechnen, müssen wir also für jedes $j \in [1, n]$ das lineare Gleichungssystem zur erweiterten Koeffizientenmatrizen $\left(A \mid \mathrm{e}_j\right)$ lösen. Macht man dies simultan indem man die Matrix $\left(A \mid \mathrm{E}_n\right)$ auf reduzierte Zeilenstufenform $\left(\mathrm{E}_n \mid B\right)$ bringt, so hat man $A^{-1} = B$ berechnet.

(2.198) Beispiel. Es seien ein Körper K und $A \in K^{3\times 3}$ gegeben durch

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

Dann ist

$$A^{-1} = \begin{pmatrix} -1 & 1 & 1 \\ 1 & 0 & -1 \\ 1 & -1 & 0 \end{pmatrix}.$$

Beweis. Wir werden elementare Zeilenoperationen auf die Matrix $\left(A \mid \mathrm{E}_3\right)$ an:

$$\left(\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right) \xmapsto{\mathrm{add}_{1,2,-1}} \left(\begin{array}{ccc|ccc} 0 & 0 & 1 & 1 & -1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right) \xmapsto{\mathrm{add}_{3,1,-1}} \left(\begin{array}{ccc|ccc} 0 & 0 & 1 & 1 & -1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & -1 & 1 & 1 \end{array}\right)$$

$$\xmapsto{\mathrm{add}_{2,3,-1}} \left(\begin{array}{ccc|ccc} 0 & 0 & 1 & 1 & -1 & 0 \\ 0 & 1 & 0 & 1 & 0 & -1 \\ 1 & 0 & 0 & -1 & 1 & 1 \end{array}\right) \xmapsto{\mathrm{sw}_{1,3}} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 1 & -1 & 0 \end{array}\right)$$

Folglich ist

$$A^{-1} = \begin{pmatrix} -1 & 1 & 1 \\ 1 & 0 & -1 \\ 1 & -1 & 0 \end{pmatrix}.$$ □

Klassifikation von Matrizen modulo Äquivalenz

(2.199) Satz. Es seien $m, n \in \mathbb{N}_0$, ein Körper K und ein $A \in K^{m\times n}$ gegeben. Dann ist A äquivalent zu $\mathrm{Q}_{\operatorname{rk} A}$.

Beweis. Nach Satz (2.182) gibt es eine parametrisierte Basis $s = (s_j)_{j\in[1,n]}$ von $K^{n\times 1}$ und eine parametrisierte Basis $t = (t_i)_{i\in[1,m]}$ von $K^{m\times 1}$ mit

$$\mathrm{M}_t^s(\varphi_A) = \mathrm{Q}_{\dim(\operatorname{Im}\varphi_A)}.$$

Wir setzen $P := \mathrm{M}_{\mathrm{e}}^s(\mathrm{id}_{K^{n\times 1}})$ und $Q := \mathrm{M}_{\mathrm{e}}^t(\mathrm{id}_{K^{m\times 1}})$. Dann ist $P \in \mathrm{GL}_n(K)$, $Q \in \mathrm{GL}_m(K)$ nach Bemerkung (2.176) und es gilt

$$Q^{-1}AP = (\mathrm{M}_{\mathrm{e}}^t(\mathrm{id}_{K^{m\times 1}}))^{-1}\,\mathrm{M}_{\mathrm{e}}^{\mathrm{e}}(\varphi_A)\,\mathrm{M}_{\mathrm{e}}^s(\mathrm{id}_{K^{n\times 1}}) = \mathrm{M}_t^s(\varphi_A) = \mathrm{Q}_{\dim(\operatorname{Im}\varphi_A)} = \mathrm{Q}_{\operatorname{rk} A}$$

nach Proposition (2.177)(b). Folglich ist A äquivalent zu $\mathrm{Q}_{\operatorname{rk} A}$. □

(2.200) Satz. Es seien $m, n \in \mathbb{N}_0$, ein Körper K und $A, B \in K^{m\times n}$ gegeben. Genau dann ist A äquivalent zu B, wenn

$$\operatorname{rk} A = \operatorname{rk} B$$

ist.

Beweis. Zunächst sei A äquivalent zu B, so dass es $P \in \mathrm{GL}_n(K)$, $Q \in \mathrm{GL}_m(K)$ mit $Q^{-1}AP = B$ gibt. Nach Korollar (2.190) und Bemerkung (2.191) ist

$$\mathrm{C}(A) = \mathrm{C}(AP) \cong \mathrm{C}(Q^{-1}AP) = \mathrm{C}(B),$$

also

$$\operatorname{rk} A = \dim \mathrm{C}(A) = \dim \mathrm{C}(B) = \operatorname{rk} B$$

nach Satz (2.137).
Nun sei umgekehrt $\operatorname{rk} A = \operatorname{rk} B$. Nach Satz (2.199) ist A äquivalent zu $\mathrm{Q}_{\operatorname{rk} A}$ und B äquivalent zu $\mathrm{Q}_{\operatorname{rk} B}$. Da nun aber $\operatorname{rk} A = \operatorname{rk} B$ ist, folgt $\mathrm{Q}_{\operatorname{rk} A} = \mathrm{Q}_{\operatorname{rk} B}$, und da Äquivalenz von Matrizen eine Äquivalenzrelation auf $K^{m\times n}$ ist, ist A folglich äquivalent zu B. □

(2.201) Korollar (Klassifikation von Matrizen modulo Äquivalenz)**.** Es seien $m, n, r \in \mathbb{N}_0$, ein Körper K und ein $A \in K^{m\times n}$ gegeben. Genau dann ist

$$\operatorname{rk} A = r,$$

wenn A äquivalent zu Q_r ist.

Beweis. Es ist $\operatorname{rk} \mathrm{Q}_r = r$. Somit gilt genau dann $\operatorname{rk} A = r$, wenn $\operatorname{rk} A = \operatorname{rk} \mathrm{Q}_r$ ist, was nach Satz (2.200) aber genau dann gilt, wenn A äquivalent zu Q_r ist. □

(2.202) Korollar. Es seien $m, n \in \mathbb{N}_0$, ein Körper K und ein $A \in K^{m\times n}$ gegeben. Dann ist

$$\operatorname{rk} A = \dim_K(\operatorname{Im}\psi_A),$$

wobei $\psi_A \colon K^{1\times m} \to K^{1\times n}$, $x \mapsto xA$.

Beweisskizze. Es ist $\operatorname{rk} A = \dim \mathrm{C}(A) = \dim(\operatorname{Im}\varphi_A)$ mit $\varphi_A \colon K^{n\times 1} \to K^{m\times 1}$, also der Multiplikation von A an Spalten. Die Abbildung ψ_A ist die Multiplikation von A an Zeilen. Jede Aussage, welche wir in diesem Abschnitt bewiesen haben, besitzt ein Analogon für Zeilen statt Spalten. Das Analogon zu Korollar (2.201) besagt: Für $r \in \mathbb{N}_0$ ist genau dann $\dim(\operatorname{Im}\psi_A) = r$, wenn A äquivalent zu Q_r ist.
Nach Satz (2.199) ist aber A äquivalent zu $\mathrm{Q}_{\operatorname{rk} A}$, so dass das Analogon zu Korollar (2.201) bereits

$$\dim(\operatorname{Im}\psi_A) = \operatorname{rk} A$$

impliziert. □

Aufgaben

Aufgabe 89 (Spaltenraum)**.** Es seien $m, n \in \mathbb{N}_0$, ein Körper K und $A \in K^{m\times n}$ gegeben. Zeigen Sie, dass

$$\mathrm{C}(A) = \langle A_{-,j} \mid j \in [1,n] \rangle$$

ist.

Aufgabe 90 (Lösbarkeit linearer Gleichungssysteme)**.** Es seien $m, n \in \mathbb{N}_0$, ein Körper K und $A \in K^{m\times n}$ gegeben. Zeigen Sie: Für $b \in K^{m\times 1}$ sind die folgenden Bedingungen sind äquivalent.

(a) Das lineare Gleichungssystem zur erweiterten Koeffizientenmatrix $\big(A \mid b\big)$ besitzt eine Lösung.

(b) Es ist $b \in \operatorname{Im} \varphi_A$.

(c) Es ist $\mathrm{C}(\big(A \mid b\big)) = \mathrm{C}(A)$.

Aufgabe 91 (Rang-Ungleichung)**.** Es seien $m, n, p \in \mathbb{N}_0$ und ein Körper K gegeben. Zeigen Sie: Für $A \in K^{n\times p}$, $B \in K^{m\times n}$ gilt

$$\operatorname{rk}(BA) \leq \min(\operatorname{rk} B, \operatorname{rk} A).$$

8 Determinante

Alternierende Multilinearformen

(2.203) Definition (alternierende Multilinearform)**.** Es seien $n \in \mathbb{N}$ und ein Körper K gegeben. Eine *alternierende Multilinearform* (*bzgl. der Spalten*) auf $K^{n\times n}$ ist eine Abbildung $d\colon K^{n\times n} \to K$ so, dass folgende Axiome gelten.

- *Multilinearität in den Spalten.* Für $k \in [1,n]$ und jede Familie $x = (x_j)_{j\in[1,n]\setminus\{k\}}$ in $K^{n\times 1}$ ist

  $$K^{n\times 1} \to K,\ y \mapsto d(\begin{pmatrix} x_1 & \dots & x_{k-1} & y & x_{k+1} & \dots & x_n \end{pmatrix})$$

  ein K-Vektorraumhomomorphismus.

- *Alternierend in den Spalten.* Für jedes n-Tupel $x = (x_j)_{j\in[1,n]}$ in $K^{n\times 1}$ und $k, l \in [1,n]$ mit $k \neq l$, $x_k = x_l$ ist

  $$d(\begin{pmatrix} x_1 & \dots & x_n \end{pmatrix}) = 0.$$

Es seien $n \in \mathbb{N}$ und ein Körper K gegeben. Die Multilinearität einer alternierenden Multilinearform d auf $K^{n\times n}$ bedeutet, dass für $k \in [1,n]$ und jede Familie $x = (x_j)_{j\in[1,n]\setminus\{k\}}$ in $K^{n\times 1}$ sowie alle $a \in K$, $y, z \in K^{n\times 1}$ stets

$$\begin{aligned}
&d(\begin{pmatrix} x_1 & \dots & x_{k-1} & y+z & x_{k+1} & \dots & x_n \end{pmatrix}) \\
&= d(\begin{pmatrix} x_1 & \dots & x_{k-1} & y & x_{k+1} & \dots & x_n \end{pmatrix}) + d(\begin{pmatrix} x_1 & \dots & x_{k-1} & z & x_{k+1} & \dots & x_n \end{pmatrix}), \\
&d(\begin{pmatrix} x_1 & \dots & x_{k-1} & ay & x_{k+1} & \dots & x_n \end{pmatrix}) = ad(\begin{pmatrix} x_1 & \dots & x_{k-1} & y & x_{k+1} & \dots & x_n \end{pmatrix}).
\end{aligned}$$

gilt. Insbesondere haben wir

$$\begin{aligned}
&d(\begin{pmatrix} x_1 & \dots & x_{k-1} & 0 & x_{k+1} & \dots & x_n \end{pmatrix}) = 0, \\
&d(\begin{pmatrix} x_1 & \dots & x_{k-1} & -y & x_{k+1} & \dots & x_n \end{pmatrix}) = -d(\begin{pmatrix} x_1 & \dots & x_{k-1} & y & x_{k+1} & \dots & x_n \end{pmatrix}).
\end{aligned}$$

(2.204) Bemerkung. Es seien $n \in \mathbb{N}$, ein Körper K, eine alternierende Multilinearform d auf $K^{n\times n}$ und ein n-Tupel $x = (x_j)_{j\in[1,n]}$ in $K^{n\times 1}$ gegeben. Für $k, l \in [1,n]$ mit $k \neq l$ und $a \in K$ gilt

$$d(\begin{pmatrix} x_1 & \dots & x_n \end{pmatrix}) = d(\begin{pmatrix} x_1 & \dots & x_{k-1} & x_k + ax_l & x_{k+1} & \dots & x_n \end{pmatrix}).$$

Beweis. Für $k, l \in [1, n]$ mit $k \neq l$ gilt

$$\begin{aligned} &d(\begin{pmatrix} x_1 & \dots & x_{k-1} & x_k + cx_l & x_{k+1} & \dots & x_n \end{pmatrix}) \\ &= d(\begin{pmatrix} x_1 & \dots & x_{k-1} & x_k & x_{k+1} & \dots & x_n \end{pmatrix}) + ad(\begin{pmatrix} x_1 & \dots & x_{k-1} & x_l & x_{k+1} & \dots & x_n \end{pmatrix}) \\ &= d(\begin{pmatrix} x_1 & \dots & x_{k-1} & x_k & x_{k+1} & \dots & x_n \end{pmatrix}). \end{aligned}$$

□

(2.205) Proposition. Es seien $n \in \mathbb{N}$, ein Körper K, eine alternierende Multilinearform d auf $K^{n\times n}$ und ein n-Tupel $x = (x_j)_{j\in[1,n]}$ in $K^{n\times 1}$ gegeben. Für $\pi \in \mathrm{S}_n$ ist

$$d(\begin{pmatrix} x_{\pi(1)} & \dots & x_{\pi(n)} \end{pmatrix}) = (\operatorname{sgn}\pi)\, d(\begin{pmatrix} x_1 & \dots & x_n \end{pmatrix}).$$

Beweis. Es sei eine Transposition π gegeben, also $\pi = (k, l)$ für $k, l \in \mathbb{N}$ mit $k < l$. Dann gilt

$$\begin{aligned} 0 &= d(\begin{pmatrix} x_1 & \dots & x_{k-1} & x_k + x_l & x_{k+1} & \dots & x_{l-1} & x_k + x_l & x_{l+1} & \dots & x_n \end{pmatrix}) \\ &= d(\begin{pmatrix} x_1 & \dots & x_{k-1} & x_k & x_{k+1} & \dots & x_{l-1} & x_k & x_{l+1} & \dots & x_n \end{pmatrix}) \\ &\quad + d(\begin{pmatrix} x_1 & \dots & x_{k-1} & x_k & x_{k+1} & \dots & x_{l-1} & x_l & x_{l+1} & \dots & x_n \end{pmatrix}) \\ &\quad + d(\begin{pmatrix} x_1 & \dots & x_{k-1} & x_l & x_{k+1} & \dots & x_{l-1} & x_k & x_{l+1} & \dots & x_n \end{pmatrix}) \\ &\quad + d(\begin{pmatrix} x_1 & \dots & x_{k-1} & x_l & x_{k+1} & \dots & x_{l-1} & x_l & x_{l+1} & \dots & x_n \end{pmatrix}) \\ &= d(\begin{pmatrix} x_1 & \dots & x_n \end{pmatrix}) + d(\begin{pmatrix} x_{\pi(1)} & \dots & x_{\pi(n)} \end{pmatrix}), \end{aligned}$$

also

$$d(\begin{pmatrix} x_{\pi(1)} & \dots & x_{\pi(n)} \end{pmatrix}) = -d(\begin{pmatrix} x_1 & \dots & x_n \end{pmatrix}) = (\operatorname{sgn}\pi)\, d(\begin{pmatrix} x_1 & \dots & x_n \end{pmatrix})$$

nach Satz (1.97).
Nun zeigen wir durch Induktion nach $l \in \mathbb{N}_0$: Für $\pi \in \mathrm{S}_n$ so, dass π ein Kompositum von l Transpositionen ist, gilt

$$d(\begin{pmatrix} x_{\pi(1)} & \dots & x_{\pi(n)} \end{pmatrix}) = (\operatorname{sgn}\pi)\, d(\begin{pmatrix} x_1 & \dots & x_n \end{pmatrix}).$$

Für $l = 0$ gilt $\pi = \mathrm{id}_{[1,n]}$, also

$$d(\begin{pmatrix} x_{\pi(1)} & \dots & x_{\pi(n)} \end{pmatrix}) = d(\begin{pmatrix} x_1 & \dots & x_n \end{pmatrix}) = (\operatorname{sgn}\mathrm{id}_{[1,n]})\, d(\begin{pmatrix} x_1 & \dots & x_n \end{pmatrix}) = (\operatorname{sgn}\pi)\, d(\begin{pmatrix} x_1 & \dots & x_n \end{pmatrix}).$$

Es sei also $l \in \mathbb{N}$ gegeben und es sei angenommen, dass

$$d(\begin{pmatrix} x_{\pi'(1)} & \dots & x_{\pi'(n)} \end{pmatrix}) = (\operatorname{sgn}\pi')\, d(\begin{pmatrix} x_1 & \dots & x_n \end{pmatrix})$$

für $\pi' \in \mathrm{S}_n$ so, dass π' ein Kompositum von $l - 1$ Transpositionen ist. Ferner sei $\pi \in \mathrm{S}_n$ gegeben und es sei angenommen, dass π ein Kompositum von l Transpositionen ist. Dann ist $\pi = \pi' \circ \tau$ für ein $\pi' \in \mathrm{S}_n$, welches ein Kompositum von $l - 1$ Transpositionen ist, und eine Transposition $\tau \in \mathrm{S}_n$. Unter Ausnutzung des Spezialfalls und der Induktionsvoraussetzung erhalten wir

$$\begin{aligned} d(\begin{pmatrix} x_{\pi(1)} & \dots & x_{\pi(n)} \end{pmatrix}) &= d(\begin{pmatrix} x_{\pi'(\tau(1))} & \dots & x_{\pi'(\tau(n))} \end{pmatrix}) = (\operatorname{sgn}\pi')\, d(\begin{pmatrix} x_{\tau(1)} & \dots & x_{\tau(n)} \end{pmatrix}) \\ &= (\operatorname{sgn}\pi')(\operatorname{sgn}\tau)\, d(\begin{pmatrix} x_1 & \dots & x_n \end{pmatrix}) = \operatorname{sgn}(\pi' \circ \tau)\, d(\begin{pmatrix} x_1 & \dots & x_n \end{pmatrix}) \\ &= (\operatorname{sgn}\pi)\, d(\begin{pmatrix} x_1 & \dots & x_n \end{pmatrix}) \end{aligned}$$

Nach dem Induktionsprinzip und Proposition (1.87) folgt nun

$$d(\begin{pmatrix} x_{\pi(1)} & \dots & x_{\pi(n)} \end{pmatrix}) = (\operatorname{sgn}\pi)\, d(\begin{pmatrix} x_1 & \dots & x_n \end{pmatrix})$$

für alle $\pi \in \mathrm{S}_n$. □

Ist π in Proposition (2.205) eine Transposition, so gilt $\operatorname{sgn}\pi = -1$ nach Satz (1.97) und wir erhalten

$$d(\begin{pmatrix} x_{\pi(1)} & \dots & x_{\pi(n)} \end{pmatrix}) = -d(\begin{pmatrix} x_1 & \dots & x_n \end{pmatrix}).$$

Die Terminologie *alternierend* beruht auf dieser Eigenschaft: Jede Vertauschung von Spalten verändert das Vorzeichen von d.

(2.206) Proposition (Leibnizformel)**.** Es seien $n \in \mathbb{N}$, ein Körper K und eine alternierende Multilinearform d auf $K^{n\times n}$ gegeben. Für $A \in K^{n\times n}$ gilt

$$d(A) = d(\mathrm{E}_n) \sum_{\pi\in \mathrm{S}_n} (\operatorname{sgn}\pi) \prod_{j\in[1,n]} A_{\pi(j),j}.$$

Beweis. Zunächst haben wir

$$\begin{aligned} d(A) &= d\big(\big(\textstyle\sum_{i\in[1,n]} A_{i,1}\mathrm{e}_i \quad \dots \quad \sum_{i\in[1,n]} A_{i,n}\mathrm{e}_i\big)\big) = d\big(\big(\textstyle\sum_{i_1\in[1,n]} A_{i_1,1}\mathrm{e}_{i_1} \quad \dots \quad \sum_{i_n\in[1,n]} A_{i_n,n}\mathrm{e}_{i_n}\big)\big) \\ &= \sum_{i\in[1,n]^n} \big(\prod_{j\in[1,n]} A_{i_j,j}\big)\, d\big(\big(\mathrm{e}_{i_1} \quad \dots \quad \mathrm{e}_{i_n}\big)\big) \end{aligned}$$

Da d alternierend ist, gilt für $i = (i_j)_{j\in[1,n]} \in [1,n]^n$ jedoch genau dann $d\big(\big(\mathrm{e}_{i_1} \quad \dots \quad \mathrm{e}_{i_n}\big)\big) \neq 0$, wenn

$$\{i_j \mid j \in [1,n]\} = [1,n]$$

ist, also genau dann, wenn $[1,n] \to [1,n]$, $j \mapsto i_j$ eine Bijektion ist. Nach Proposition (2.205) folgt

$$\begin{aligned} d(A) &= \sum_{i\in[1,n]^n} \big(\prod_{j\in[1,n]} A_{i_j,j}\big)\, d\big(\big(\mathrm{e}_{i_1} \quad \dots \quad \mathrm{e}_{i_n}\big)\big) = \sum_{\pi\in\mathrm{S}_n} \big(\prod_{j\in[1,n]} A_{\pi(j),j}\big)\, d\big(\big(\mathrm{e}_{\pi(1)} \quad \dots \quad \mathrm{e}_{\pi(n)}\big)\big) \\ &= \sum_{\pi\in\mathrm{S}_n} \big(\prod_{j\in[1,n]} A_{\pi(j),j}\big)(\operatorname{sgn}\pi)\, d\big(\big(\mathrm{e}_1 \quad \dots \quad \mathrm{e}_n\big)\big) = d(\mathrm{E}_n) \sum_{\pi\in\mathrm{S}_n} (\operatorname{sgn}\pi) \prod_{j\in[1,n]} A_{\pi(j),j}. \end{aligned}$$

□

(2.207) Korollar. Es seien $n \in \mathbb{N}$, ein Körper K und alternierende Multilinearformen d und d' auf $K^{n\times n}$ gegeben. Dann gilt

$$d'(\mathrm{E}_n)d = d(\mathrm{E}_n)d'.$$

Beweis. Siehe Aufgabe 92. □

(2.208) Proposition. Es seien $n \in \mathbb{N}$, ein Körper K eine alternierende Multilinearform d auf $K^{n\times n}$ gegeben. Für $A, B \in K^{n\times n}$ gilt

$$d(AB)d(\mathrm{E}_n) = d(A)d(B).$$

Beweis. Siehe Aufgabe 93(b). □

(2.209) Satz. Es seien $n \in \mathbb{N}$ und ein Körper K gegeben. Für jedes $a \in K$ gibt es genau eine alternierende Multilinearform d auf $K^{n\times n}$ mit $d(\mathrm{E}_n) = a$, gegeben durch

$$d(A) = a \sum_{\pi\in\mathrm{S}_n} (\operatorname{sgn}\pi) \prod_{j\in[1,n]} A_{\pi(j),j}$$

für $A \in K^{n\times n}$.

Beweis. Es sei $a \in K$ gegeben. Die Eindeutigkeit folgt aus der Leibnizformel (2.206). Für die Existenz sei $d\colon K^{n\times n} \to K$ durch

$$d(A) = a \sum_{\pi\in\mathrm{S}_n} (\operatorname{sgn}\pi) \prod_{j\in[1,n]} A_{\pi(j),j}$$

für $A \in K^{n\times n}$ definiert. Wir zeigen, dass d eine alternierende Multilinearform auf $K^{n\times n}$ ist.
Für die Multilinearität sei ein $k \in [1,n]$ sowie eine Familie $x = (x_j)_{j\in[1,n]\setminus\{k\}}$ in $K^{n\times 1}$ gegeben. Dann gilt

$$\begin{aligned} &d\big(\big(x_1 \quad \dots \quad x_{k-1} \quad y+z \quad x_{k+1} \quad \dots \quad x_n\big)\big) \\ &= a \sum_{\pi\in\mathrm{S}_n} (\operatorname{sgn}\pi) \big(\prod_{j\in[1,k-1]} (x_j)_{\pi(j)}\big)(y+z)_{\pi(k)} \big(\prod_{j\in[k+1,n]} (x_j)_{\pi(j)}\big) \\ &= a \sum_{\pi\in\mathrm{S}_n} (\operatorname{sgn}\pi) \big(\prod_{j\in[1,k-1]} (x_j)_{\pi(j)}\big)(y_{\pi(k)} + z_{\pi(k)}) \big(\prod_{j\in[k+1,n]} (x_j)_{\pi(j)}\big) \end{aligned}$$

$$= a(\sum_{\pi\in \mathrm{S}_n}(\operatorname{sgn}\pi)(\prod_{j\in[1,k-1]}(x_j)_{\pi(j)})y_{\pi(k)}(\prod_{j\in[k+1,n]}(x_j)_{\pi(j)})$$
$$+\sum_{\pi\in \mathrm{S}_n}(\operatorname{sgn}\pi)(\prod_{j\in[1,k-1]}(x_j)_{\pi(j)})z_{\pi(k)}(\prod_{j\in[k+1,n]}(x_j)_{\pi(j)}))$$
$$= a\sum_{\pi\in \mathrm{S}_n}(\operatorname{sgn}\pi)(\prod_{j\in[1,k-1]}(x_j)_{\pi(j)})y_{\pi(k)}(\prod_{j\in[k+1,n]}(x_j)_{\pi(j)})$$
$$+a\sum_{\pi\in \mathrm{S}_n}(\operatorname{sgn}\pi)(\prod_{j\in[1,k-1]}(x_j)_{\pi(j)})z_{\pi(k)}(\prod_{j\in[k+1,n]}(x_j)_{\pi(j)})$$
$$= d(\begin{pmatrix}x_1 & \dots & x_{k-1} & y & x_{k+1} & \dots & x_n\end{pmatrix}) + d(\begin{pmatrix}x_1 & \dots & x_{k-1} & z & x_{k+1} & \dots & x_n\end{pmatrix})$$

für $y, z \in K^{n\times 1}$ sowie

$$d(\begin{pmatrix}x_1 & \dots & x_{k-1} & by & x_{k+1} & \dots & x_n\end{pmatrix}) = a\sum_{\pi\in \mathrm{S}_n}(\operatorname{sgn}\pi)(\prod_{j\in[1,k-1]}(x_j)_{\pi(j)})(by)_{\pi(k)}(\prod_{j\in[k+1,n]}(x_j)_{\pi(j)})$$
$$= a\sum_{\pi\in \mathrm{S}_n}(\operatorname{sgn}\pi)(\prod_{j\in[1,k-1]}(x_j)_{\pi(j)})(by_{\pi(k)})(\prod_{j\in[k+1,n]}(x_j)_{\pi(j)})$$
$$= ab\sum_{\pi\in \mathrm{S}_n}(\operatorname{sgn}\pi)(\prod_{j\in[1,k-1]}(x_j)_{\pi(j)})y_{\pi(k)}(\prod_{j\in[k+1,n]}(x_j)_{\pi(j)})$$
$$= ba\sum_{\pi\in \mathrm{S}_n}(\operatorname{sgn}\pi)(\prod_{j\in[1,k-1]}(x_j)_{\pi(j)})y_{\pi(k)}(\prod_{j\in[k+1,n]}(x_j)_{\pi(j)}) = b\,d(\begin{pmatrix}x_1 & \dots & x_{k-1} & y & x_{k+1} & \dots & x_n\end{pmatrix})$$

für $a \in K$, $y \in K^{n\times 1}$. Folglich ist

$$K^{n\times 1} \to K,\ y \mapsto d(\begin{pmatrix}x_1 & \dots & x_{k-1} & y & x_{k+1} & \dots & x_n\end{pmatrix})$$

ein K-Vektorraumhomomorphismus. Folglich ist d eine Multilinearform auf $K^{n\times n}$.
Es seien ein n-Tupel $x = (x_j)_{j\in[1,n]}$ in $K^{n\times 1}$ und $k, l \in [1, n]$ mit $k \neq l$ und $x_k = x_l$ gegeben. Wir definieren $\tau \in \mathrm{S}_n$ durch $\tau := (k, l)$. Dann ist

$$\prod_{j\in[1,n]}(x_j)_{\pi(\tau(j))} = (\prod_{j\in[1,n]\setminus\{k,l\}}(x_j)_{\pi(\tau(j))})(x_k)_{\pi(\tau(k))}(x_l)_{\pi(\tau(l))} = (\prod_{j\in[1,n]\setminus\{k,l\}}(x_j)_{\pi(j)})(x_k)_{\pi(l)}(x_l)_{\pi(k)}$$
$$= (\prod_{j\in[1,n]\setminus\{k,l\}}(x_j)_{\pi(j)})(x_l)_{\pi(l)}(x_k)_{\pi(k)} = \prod_{j\in[1,n]}(x_j)_{\pi(j)}.$$

Da sgn nach Proposition (1.95) ein Gruppenhomomorphismus ist und $\operatorname{sgn}\tau = -1$ nach Satz (1.97) gilt, ist

$$\{\pi \in \mathrm{S}_n \mid \operatorname{sgn}\pi = 1\} \to \{\sigma \in \mathrm{S}_n \mid \operatorname{sgn}\sigma = -1\},\ \pi \mapsto \pi\circ\tau$$

eine wohldefinierte Bijektion. Da K kommutativ ist, erhalten wir

$$\sum_{\pi\in \mathrm{S}_n}(\operatorname{sgn}\pi)\prod_{j\in[1,n]}(x_j)_{\pi(j)} = \sum_{\substack{\pi\in \mathrm{S}_n\\ \operatorname{sgn}\pi=1}}(\operatorname{sgn}\pi)\prod_{j\in[1,n]}(x_j)_{\pi(j)} + \sum_{\substack{\sigma\in \mathrm{S}_n\\ \operatorname{sgn}\sigma=-1}}(\operatorname{sgn}\sigma)\prod_{j\in[1,n]}(x_j)_{\sigma(j)}$$
$$= \sum_{\substack{\pi\in \mathrm{S}_n\\ \operatorname{sgn}\pi=1}}(\operatorname{sgn}\pi)\prod_{j\in[1,n]}(x_j)_{\pi(j)} + \sum_{\substack{\pi\in \mathrm{S}_n\\ \operatorname{sgn}\pi=1}}\operatorname{sgn}(\pi\circ\tau)\prod_{j\in[1,n]}(x_j)_{\pi(\tau(j))}$$
$$= \sum_{\substack{\pi\in \mathrm{S}_n\\ \operatorname{sgn}\pi=1}}\prod_{j\in[1,n]}(x_j)_{\pi(j)} + \sum_{\substack{\pi\in \mathrm{S}_n\\ \operatorname{sgn}\pi=1}}(-1)\prod_{j\in[1,n]}(x_j)_{\pi(\tau(j))}$$
$$= \sum_{\substack{\pi\in \mathrm{S}_n\\ \operatorname{sgn}\pi=1}}(\prod_{j\in[1,n]}(x_j)_{\pi(j)} - \prod_{j\in[1,n]}(x_j)_{\pi(\tau(j))}) = 0$$

und damit

$$d(\begin{pmatrix}x_1 & \dots & x_n\end{pmatrix}) = a\sum_{\pi\in \mathrm{S}_n}(\operatorname{sgn}\pi)\prod_{j\in[1,n]}(x_j)_{\pi(j)} = a\cdot 0 = 0.$$

Folglich ist d alternierend.
Schließlich gilt

$$\prod_{j\in[1,n]} (\mathrm{E}_n)_{\pi(j),j} = \prod_{j\in[1,n]} \delta_{\pi(j),j} = \left.\begin{cases} 1, & \text{falls } \pi(j) = j \text{ für alle } j \in [1,n], \\ 0, & \text{falls } \pi(j) \neq j \text{ für ein } j \in [1,n], \end{cases}\right\} = \begin{cases} 1, & \text{falls } \pi = \mathrm{id}_{[1,n]}, \\ 0, & \text{falls } \pi \neq \mathrm{id}_{[1,n]}, \end{cases}$$

und damit

$$d(\mathrm{E}_n) = a \sum_{\pi\in \mathrm{S}_n} (\operatorname{sgn}\pi) \prod_{j\in[1,n]} (\mathrm{E}_n)_{\pi(j),j} = a(\operatorname{sgn}\mathrm{id}_{[1,n]}) = a. \qquad \square$$

Definition der Determinante

Wir definieren die Determinante auf $K^{n\times n}$ für $n \in \mathbb{N}$ und einen Körper K als *normierte* alternierende Multilinearform auf $K^{n\times n}$.

(2.210) Definition (Determinante)**.** Es seien $n \in \mathbb{N}$ und ein Körper K gegeben. Die *Determinante* auf $K^{n\times n}$ ist die eindeutige alternierende Multilinearform det auf $K^{n\times n}$ mit

$$\det \mathrm{E}_n = 1.$$

(2.211) Bemerkung (Leibniz-Formel)**.** Es seien $n \in \mathbb{N}$ und ein Körper K gegeben. Für $A \in K^{n\times n}$ gilt

$$\det A = \sum_{\pi\in \mathrm{S}_n} (\operatorname{sgn}\pi) \prod_{j\in[1,n]} A_{\pi(j),j}$$

Beweis. Dies folgt aus Proposition (2.206). $\square$

(2.212) Korollar. Es seien $n \in \mathbb{N}$ und ein Körper K gegeben. Für $A \in K^{n\times n}$ gilt

$$\det A^{\mathrm{tr}} = \det A.$$

Beweis. Da $\mathrm{S}_n \to \mathrm{S}_n$, $\pi \mapsto \pi^{-1}$ eine Bijektion ist, gilt

$$\begin{aligned} \det A^{\mathrm{tr}} &= \sum_{\pi\in \mathrm{S}_n} (\operatorname{sgn}\pi) \prod_{j\in[1,n]} A^{\mathrm{tr}}_{\pi(j),j} = \sum_{\pi\in \mathrm{S}_n} (\operatorname{sgn}\pi) \prod_{j\in[1,n]} A^{\mathrm{tr}}_{j,\pi(j)} = \sum_{\pi\in \mathrm{S}_n} (\operatorname{sgn}\pi^{-1}) \prod_{j\in[1,n]} A^{\mathrm{tr}}_{\pi^{-1}(j),j} \\ &= \sum_{\pi\in \mathrm{S}_n} (\operatorname{sgn}\pi) \prod_{j\in[1,n]} A^{\mathrm{tr}}_{\pi(j),j} = \det A \end{aligned}$$

nach Korollar (1.96). $\square$

(2.213) Beispiel. Es sei ein Körper K gegeben.

(a) Die Determinante auf $K^{1\times 1}$ ist gegeben durch

$$\det\big(a\big) = a$$

für $a \in K$.

(b) Die Determinante auf $K^{2\times 2}$ ist gegeben durch

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$$

für $a, b, c, d \in K$.

Beweis.

(a) Es ist $\mathrm{S}_1 = \{\mathrm{id}_{\{1\}}\}$, also

$$\det\big(a\big) = (\operatorname{sgn}\mathrm{id}_{\{1\}})a = a$$

für $a \in K$.

(b) Es ist $\mathrm{S}_2 = \{\mathrm{id}_{\{1,2\}}, (1,2)\}$, also

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (\operatorname{sgn} \mathrm{id}_{\{1,2\}})ad + (\operatorname{sgn}(1,2))cb = ad - bc$$

für $a, b, c, d \in K$. □

(2.214) Bemerkung. Es seien $n \in \mathbb{N}$ und ein Körper K gegeben. Für jede alternernierende Multilinearform d auf $K^{n\times n}$ gilt

$$d = d(\mathrm{E}_n) \det.$$

Beweis. Nach Korollar (2.207) gilt

$$d = (\det \mathrm{E}_n)d = d(\mathrm{E}_n)\det.$$ □

(2.215) Korollar. Es seien $n \in \mathbb{N}$ und ein Körper K gegeben. Die Menge der alternierenden Multilinearformen auf $K^{n\times n}$ ist durch

$$K \det$$

gegeben. Insbesondere bildet sie einen 1-dimensionalen K-Untervektorraum von $\mathrm{Map}(K^{n\times n}, K)$.

Beweis. Es sei zunächst eine alternierende Multilinearform d auf $K^{n\times n}$ gegeben. Dann ist $d = d(\mathrm{E}_n) \det$, also insbesondere $d \in K \det$. Umgekehrt gibt es nach Satz (2.209) für jedes $a \in K$ genau eine alternierende Multilinearform d auf $K^{n\times n}$ mit $d(\mathrm{E}_n) = a$, so dass $d = d(\mathrm{E}_n) \det = a \det$ gilt. □

(2.216) Proposition. Es seien $n \in \mathbb{N}$ und ein Körper K gegeben. Dann ist

$$\det\colon K^{n\times n} \to K$$

ein surjektiver Monoidhomomorphismus.

Beweis. Siehe Aufgabe 93(c). □

Minoren und Laplace-Entwicklung

(2.217) Definition (Minor)**.** Es seien $n \in \mathbb{N}$, ein Körper K, ein $A \in K^{n\times n}$ sowie $k, l \in [1, n]$ gegeben. Der *Minor* von A an der Stelle (k, l) ist definiert als

$$\mathrm{M}_{k,l}(A) := \det \begin{pmatrix} A_{1,1} & \dots & A_{1,l-1} & A_{1,l+1} & \dots & A_{1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ A_{k-1,1} & \dots & A_{k-1,l-1} & A_{k-1,l+1} & \dots & A_{k-1,n} \\ A_{k+1,1} & \dots & A_{k+1,l-1} & A_{k+1,l+1} & \dots & A_{k+1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ A_{n,1} & \dots & A_{n,l-1} & A_{n,l+1} & \dots & A_{n,n} \end{pmatrix}$$

(2.218) Satz (Laplace-Entwicklung)**.** Es seien $n \in \mathbb{N}$, ein Körper K und ein $A \in K^{n\times n}$ gegeben.

(a) *Entwicklung nach der l-ten Spalte.* Für $l \in [1, n]$ gilt

$$\det A = \sum_{k\in[1,n]} (-1)^{k+l} A_{k,l} \mathrm{M}_{k,l}(A).$$

(b) *Entwicklung nach der k-ten Zeile.* Für $k \in [1, n]$ gilt

$$\det A = \sum_{l\in[1,n]} (-1)^{k+l} A_{k,l} \mathrm{M}_{k,l}(A).$$

Beweis.

(a) Es sei $l \in [1,n]$ gegeben.

Zunächst sei $A_{-,l} = \mathrm{e}_k$ für ein $k \in [1,n]$. Wir definieren $B \in K^{(n-1)\times(n-1)}$ durch

$$B := \begin{pmatrix} A_{1,1} & \dots & A_{1,l-1} & A_{1,l+1} & \dots & A_{1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ A_{k-1,1} & \dots & A_{k-1,l-1} & A_{k-1,l+1} & \dots & A_{k-1,n} \\ A_{k+1,1} & \dots & A_{k+1,l-1} & A_{k+1,l+1} & \dots & A_{k+1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ A_{n,1} & \dots & A_{n,l-1} & A_{n,l+1} & \dots & A_{n,n} \end{pmatrix},$$

so dass

$$B_{i,j} = \begin{cases} A_{i,j}, & \text{falls } i \in [1,k-1],\ j \in [1,l-1], \\ A_{i+1,j}, & \text{falls } i \in [k,n-1],\ j \in [1,l-1], \\ A_{i,j+1}, & \text{falls } i \in [1,k-1],\ j \in [l,n-1], \\ A_{i+1,j+1}, & \text{falls } i \in [k,n-1],\ j \in [l,n-1], \end{cases}$$

für $i,j \in [1,n]$ gilt. Für $\pi \in \mathrm{S}_n$ gilt $A_{\pi(l),l} = (\mathrm{e}_k)_{\pi(l)} = \delta_{\pi(l),k}$, so dass wir

$$\begin{aligned} \det A &= \sum_{\pi\in\mathrm{S}_n} (\operatorname{sgn}\pi) \prod_{j\in[1,n]} A_{\pi(j),j} = \sum_{\pi\in\mathrm{S}_n} (\operatorname{sgn}\pi)\Big(\prod_{j\in[1,l-1]} A_{\pi(j),j}\Big) A_{\pi(l),l} \Big(\prod_{j\in[l+1,n]} A_{\pi(j),j}\Big) \\ &= \sum_{\pi\in\mathrm{S}_n} (\operatorname{sgn}\pi)\Big(\prod_{j\in[1,l-1]} A_{\pi(j),j}\Big)\delta_{\pi(l),k}\Big(\prod_{j\in[l+1,n]} A_{\pi(j),j}\Big) \\ &= \sum_{\substack{\pi\in\mathrm{S}_n \\ \pi(l)=k}} (\operatorname{sgn}\pi)\Big(\prod_{j\in[1,l-1]} A_{\pi(j),j}\Big)\Big(\prod_{j\in[l+1,n]} A_{\pi(j),j}\Big) \end{aligned}$$

erhalten. Nun ist

$$f\colon \{\sigma \in \mathrm{S}_n \mid \sigma(n) = n\} \to \{\pi \in \mathrm{S}_n \mid \pi(l) = k\},\ \sigma \mapsto (k,\dots,n) \circ \sigma \circ (l,\dots,n)^{-1}$$

eine Bijektion. Für $\sigma \in \mathrm{S}_n$ mit $\sigma(n) = n$ gilt

$$\begin{aligned} \operatorname{sgn} f(\sigma) &= \operatorname{sgn}((k,\dots,n)\circ\sigma\circ(l,\dots,n)^{-1}) = (\operatorname{sgn}(k,\dots,n))(\operatorname{sgn}\sigma)(\operatorname{sgn}(l,\dots,n)) \\ &= (-1)^{n-k}(\operatorname{sgn}\sigma)(-1)^{n-l} = (-1)^{k+l}(\operatorname{sgn}\sigma) \end{aligned}$$

nach Proposition (1.95) und Korollar (1.96) sowie

$$(f(\sigma))(j) = \begin{cases} \sigma(j), & \text{falls } j \in [1,l-1],\ \sigma(j) \in [1,k-1], \\ \sigma(j)+1, & \text{falls } j \in [1,l-1],\ \sigma(j) \in [k,n-1], \\ k, & \text{falls } j = l, \\ \sigma(j-1), & \text{falls } j \in [l+1,n],\ \sigma(j-1) \in [1,k-1], \\ \sigma(j-1)+1, & \text{falls } j \in [l+1,n],\ \sigma(j-1) \in [k,n-1], \end{cases}$$

für $j \in [1,n]$. Es folgt

$$\begin{aligned} \det A &= \sum_{\substack{\pi\in\mathrm{S}_n \\ \pi(l)=k}} (\operatorname{sgn}\pi)\Big(\prod_{j\in[1,l-1]} A_{\pi(j),j}\Big)\Big(\prod_{j\in[l+1,n]} A_{\pi(j),j}\Big) \\ &= \sum_{\substack{\sigma\in\mathrm{S}_n \\ \sigma(n)=n}} (\operatorname{sgn} f(\sigma))\Big(\prod_{j\in[1,l-1]} A_{(f(\sigma))(j),j}\Big)\Big(\prod_{j\in[l+1,n]} A_{(f(\sigma))(j),j}\Big) \\ &= \sum_{\substack{\sigma\in\mathrm{S}_n \\ \sigma(n)=n}} (-1)^{k+l}(\operatorname{sgn}\sigma)\Big(\prod_{\substack{j\in[1,l-1] \\ \sigma(j)\in[1,k-1]}} A_{\sigma(j),j}\Big)\Big(\prod_{\substack{j\in[1,l-1] \\ \sigma(j)\in[k,n-1]}} A_{\sigma(j)+1,j}\Big)\Big(\prod_{\substack{j\in[l+1,n] \\ \sigma(j-1)\in[1,k-1]}} A_{\sigma(j-1),j}\Big) \end{aligned}$$

$$
\begin{aligned}
&\Big(\prod_{\substack{j\in[l+1,n]\\ \sigma(j-1)\in[k,n-1]}} A_{\sigma(j-1)+1,j}\Big)\\
&= (-1)^{k+l}\sum_{\substack{\sigma\in \mathrm{S}_n\\ \sigma(n)=n}} (\operatorname{sgn}\sigma)\Big(\prod_{\substack{j\in[1,l-1]\\ \sigma(j)\in[1,k-1]}} A_{\sigma(j),j}\Big)\Big(\prod_{\substack{j\in[1,l-1]\\ \sigma(j)\in[k,n-1]}} A_{\sigma(j)+1,j}\Big)\Big(\prod_{\substack{j\in[l,n-1]\\ \sigma(j)\in[1,k-1]}} A_{\sigma(j),j+1}\Big)\\
&\quad\Big(\prod_{\substack{j\in[l,n-1]\\ \sigma(j)\in[k,n-1]}} A_{\sigma(j)+1,j+1}\Big)\\
&= (-1)^{k+l}\sum_{\sigma\in \mathrm{S}_{n-1}} (\operatorname{sgn}\sigma)\Big(\prod_{\substack{j\in[1,l-1]\\ \sigma(j)\in[1,k-1]}} B_{\sigma(j),j}\Big)\Big(\prod_{\substack{j\in[1,l-1]\\ \sigma(j)\in[k,n-1]}} B_{\sigma(j),j}\Big)\Big(\prod_{\substack{j\in[l,n-1]\\ \sigma(j)\in[1,k-1]}} B_{\sigma(j),j}\Big)\\
&\quad\Big(\prod_{\substack{j\in[l,n-1]\\ \sigma(j)\in[k,n-1]}} B_{\sigma(j),j}\Big)\\
&= (-1)^{k+l}\sum_{\sigma\in \mathrm{S}_{n-1}} (\operatorname{sgn}\sigma)\Big(\prod_{j\in[1,l-1]} B_{\sigma(j),j}\Big) = (-1)^{k+l}\det B = (-1)^{k+l}\mathrm{M}_{k,l}(A).
\end{aligned}
$$

Nun sei $A \in K^{n\times n}$ beliebig. Dann folgt

$$
\begin{aligned}
\det A &= \det\begin{pmatrix} A_{-,1} & \dots & A_{-,l-1} & A_{-,l} & A_{-,l+1} & \dots & A_{-,n}\end{pmatrix}\\
&= \det\begin{pmatrix} A_{-,1} & \dots & A_{-,l-1} & \sum_{k\in[1,n]} A_{k,l}\mathrm{e}_k & A_{-,l+1} & \dots & A_{-,n}\end{pmatrix}\\
&= \sum_{k\in[1,n]} A_{k,l}\det\begin{pmatrix} A_{-,1} & \dots & A_{-,l-1} & \mathrm{e}_k & A_{-,l+1} & \dots & A_{-,n}\end{pmatrix}\\
&= \sum_{k\in[1,n]} A_{k,l}(-1)^{k+l}\mathrm{M}_{k,l}\Big(\begin{pmatrix} A_{-,1} & \dots & A_{-,l-1} & \mathrm{e}_k & A_{-,l+1} & \dots & A_{-,n}\end{pmatrix}\Big)\\
&= \sum_{k\in[1,n]} (-1)^{k+l}A_{k,l}\mathrm{M}_{k,l}(A).
\end{aligned}
$$

(b) Es sei $k \in [1,n]$ gegeben. Nach Korollar (2.212) und (a) gilt

$$\det A = \det A^{\mathrm{tr}} = \sum_{l\in[1,n]} (-1)^{l+k}A^{\mathrm{tr}}_{l,k}\mathrm{M}_{l,k}(A^{\mathrm{tr}}) = \sum_{l\in[1,n]} (-1)^{k+l}A_{k,l}\mathrm{M}_{k,l}(A). \qquad \square$$

(2.219) Beispiel. Es sei $A \in \mathbb{R}^{3\times 3}$ gegeben durch

$$A = \begin{pmatrix} 1 & -1 & 2\\ 4 & 3 & -1\\ 2 & -1 & 1\end{pmatrix}.$$

Dann ist

$$\det A = -12.$$

Beweis. Eine Laplace-Entwicklung (2.218)(a) nach der ersten Spalte liefert

$$
\begin{aligned}
\det A &= \det\begin{pmatrix} 1 & -1 & 2\\ 4 & 3 & -1\\ 2 & -1 & 1\end{pmatrix} = 1\det\begin{pmatrix} 3 & -1\\ -1 & 1\end{pmatrix} - 4\det\begin{pmatrix} -1 & 2\\ -1 & 1\end{pmatrix} + 2\det\begin{pmatrix} -1 & 2\\ 3 & -1\end{pmatrix}\\
&= 1(3\cdot 1 - (-1)(-1)) - 4((-1)\cdot 1 - 2(-1)) + 2((-1)(-1) - 2\cdot 3) = 1\cdot 2 - 4\cdot 1 + 2(-5) = -12. \qquad \square
\end{aligned}
$$

Etwas weniger chaotisch gestaltet sich die Rechnung, wenn wir die Matrix zunächst durch elementare Zeilenoperationen vereinfachen. Hierbei gilt zu beachten, dass Vertauschungs- und Multiplikationsoperatoren die Determinante verändern (gemäß der Multilinearität bzw. Proposition (2.205), unter Beachtung von Korollar (2.212)).

Alternativer Beweis zu Beispiel (2.219). Zunächst formen wir A mittels Additionsoperationen auf den Zeilen um:

$$\begin{pmatrix} 1 & -1 & 2 \\ 4 & 3 & -1 \\ 2 & -1 & 1 \end{pmatrix} \xmapsto{\mathrm{add}_{3,1,-2} \circ \mathrm{add}_{2,1,-4}} \begin{pmatrix} 1 & -1 & 2 \\ 0 & 7 & -9 \\ 0 & 1 & -3 \end{pmatrix} \xmapsto{\mathrm{add}_{2,3,-7}} \begin{pmatrix} 1 & -1 & 2 \\ 0 & 0 & 12 \\ 0 & 1 & -3 \end{pmatrix}$$

Nach Korollar (2.212) und Bemerkung (2.204) gilt

$$\det A = \det \begin{pmatrix} 1 & -1 & 2 \\ 4 & 3 & -1 \\ 2 & -1 & 1 \end{pmatrix} = \det \begin{pmatrix} 1 & -1 & 2 \\ 0 & 0 & 12 \\ 0 & 1 & -3 \end{pmatrix}.$$

Eine Laplace-Entwicklung (2.218)(a) liefert

$$\det A = \det \begin{pmatrix} 1 & -1 & 2 \\ 0 & 0 & 12 \\ 0 & 1 & -3 \end{pmatrix} = \det \begin{pmatrix} 0 & 12 \\ 1 & -3 \end{pmatrix} = -\det \begin{pmatrix} 12 \end{pmatrix} = -12. \qquad \square$$

De facto lässt sich die Determinante einer Matrix in Zeilenstufenform ablesen, siehe Korollar (2.226).

(2.220) Definition (Adjunkte)**.** Es seien $n \in \mathbb{N}$ und ein Körper K gegeben. Für $A \in K^{n \times n}$ heißt $\mathrm{Adj}(A) \in K^{n \times n}$ gegeben durch

$$\mathrm{Adj}(A)_{i,j} = (-1)^{i+j} \mathrm{M}_{j,i}(A)$$

für $i, j \in [1, n]$ die *Adjunkte* von A (oder die *komplementäre Matrix* zu A).

Die Laplace-Entwicklung lässt sich kompakt in folgender Formel zusammenfassen:

(2.221) Satz. Es seien $n \in \mathbb{N}$ und ein Körper K gegeben. Für $A \in K^{n \times n}$ gilt

$$\mathrm{Adj}(A)\, A = A\, \mathrm{Adj}(A) = (\det A)\mathrm{E}_n.$$

Beweis. Es sei $A \in K^{n \times n}$ gegeben. Für $i, k \in [1, n]$ liefert eine Laplace-Entwicklung (2.218)(a) nach der i-ten Spalte

$$\begin{aligned} (\mathrm{Adj}(A)\, A)_{i,k} &= \sum_{j \in [1,n]} \mathrm{Adj}(A)_{i,j} A_{j,k} = \sum_{j \in [1,n]} A_{j,k} (-1)^{i+j} \mathrm{M}_{j,i}(A) \\ &= \sum_{j \in [1,n]} A_{j,k} (-1)^{i+j} \mathrm{M}_{j,i}\big(\begin{pmatrix} A_{-,1} & \dots & A_{-,i-1} & A_{-,k} & A_{-,i+1} & \dots & A_{-,n} \end{pmatrix}\big) \\ &= \det \begin{pmatrix} A_{-,1} & \dots & A_{-,i-1} & A_{-,k} & A_{-,i+1} & \dots & A_{-,n} \end{pmatrix} = \delta_{i,k} (\det A) = ((\det A)\mathrm{E}_n)_{i,k}. \end{aligned}$$

Somit gilt $\mathrm{Adj}(A)\, A = (\det A)\mathrm{E}_n$.
Die Formel $A\, \mathrm{Adj}(A) = (\det A)\mathrm{E}_n$ lässt sich analog beweisen. $\square$

Die Adjunkte einer invertierbaren Matrix steht in engem Zusammenhang zur Inversen, wie wir im Folgenden sehen werden.

(2.222) Korollar. Es seien $n \in \mathbb{N}$ und ein Körper K gegeben. Dann ist

$$\mathrm{GL}_n(K) = \{A \in K^{n \times n} \mid \det A \neq 0\}.$$

Das Inverse von $A \in \mathrm{GL}_n(K)$ ist durch

$$A^{-1} = (\det A)^{-1} \mathrm{Adj}(A)$$

gegeben.

Beweis. Es sei $A \in K^{n\times n}$ gegeben.
Zunächst sei A invertierbar. Da $\det\colon K^{n\times n} \to K$ nach Proposition (2.216) ein Monoidhomomorphismus ist, folgt $\det A \in K^\times$ nach Bemerkung (1.66), d.h. $\det A \neq 0$.
Nun sei umgekehrt $\det A \neq 0$, also $\det A \in K^\times$. Dann ist nach Satz (2.221) auch A invertierbar mit

$$A^{-1} = (\det A)^{-1}\mathrm{Adj}(A). \qquad \square$$

Alternativer Beweis der ersten Aussage in Korollar (2.222). Zunächst sei A invertierbar. Da $\det\colon K^{n\times n} \to K$ nach Proposition (2.216) ein Monoidhomomorphismus ist, folgt $\det A \in K^\times$ nach Bemerkung (1.66), d.h. es ist $\det A \neq 0$.
Nun sei umgekehrt A nicht invertierbar. Nach Satz (2.199) ist A äquivalent zu $\mathrm{Q}_{\mathrm{rk}\,A}$, d.h. es gibt $P, Q \in \mathrm{GL}_n(K)$ mit $Q^{-1}AP = \mathrm{Q}_{\mathrm{rk}\,A}$. Nach Bemerkung (2.196) ist aber $\mathrm{rk}\,A < n$, so dass nach Proposition (2.216) und Bemerkung (1.66) nun

$$(\det Q)^{-1}(\det A)(\det P) = \det(Q^{-1}AP) = \det \mathrm{Q}_{\mathrm{rk}\,A} = \det\begin{pmatrix} \mathrm{e}_1 & \dots & \mathrm{e}_{\mathrm{rk}\,A} & 0 & \dots & 0\end{pmatrix} = 0$$

und damit $\det A = 0$ folgt. $\square$

Für $n \in \mathbb{N}$, $A \in \mathbb{Z}^{n\times n}$ ist $\mathrm{Adj}(A) \in \mathbb{Z}^{n\times n}$, wie man an der Leibniz-Formel (2.211) erkennen kann. Ist zudem $A \in \mathrm{GL}_n(\mathbb{Q})$, d.h. invertierbar aufgefasst als Matrix mit Einträgen in $\mathbb{Q}$, so ist im Allgemeinen $A^{-1} \notin \mathbb{Z}^{n\times n}$, sondern nur noch $A^{-1} \in \mathbb{Q}^{n\times n}$. In diesem Fall kann also die Adjunkte als „diskretes Analogon“ der Inversen angesehen werden.

(2.223) Korollar. Es seien $n \in \mathbb{N}$ und ein Körper K gegeben. Der Monoidhomomorphismus $\det\colon K^{n\times n} \to K$ schränkt ein zu einem surjektiven Gruppenhomomorphismus

$$\det\colon \mathrm{GL}_n(K) \to K^\times.$$

Der Kästchensatz

(2.224) Proposition (Kästchensatz für Determinanten)**.** Es seien $m, n \in \mathbb{N}$ und ein Körper K gegeben. Für $A \in K^{m\times m}$, $B \in K^{m\times n}$, $C \in K^{n\times n}$ gilt

$$\det\begin{pmatrix} A & B \\ 0 & C\end{pmatrix} = (\det A)(\det C).$$

Beweis. Eine Laplace-Entwicklung (2.218)(a) nach der ersten Spalte und Induktion nach m liefert

$$\begin{aligned}\det\begin{pmatrix} A & B \\ 0 & C\end{pmatrix} &= \sum_{k\in[1,m+n]} (-1)^{k+1}\begin{pmatrix} A & B \\ 0 & C\end{pmatrix}_{k,1} \mathrm{M}_{k,1}(\begin{pmatrix} A & B \\ 0 & C\end{pmatrix}) = \sum_{k\in[1,m]} (-1)^{k+1}A_{k,1}\mathrm{M}_{k,1}(A)(\det C)\\ &= (\sum_{k\in[1,m]} (-1)^{k+1}A_{k,1}\mathrm{M}_{k,1}(A))(\det C) = (\det A)(\det C). \qquad \square\end{aligned}$$

(2.225) Definition (obere Dreiecksmatrix)**.** Es seien $n \in \mathbb{N}_0$ und ein Körper K gegeben. Ein $A \in K^{n\times n}$ heißt *obere Dreiecksmatrix*, falls $A_{i,j} = 0$ für $i, j \in [1, n]$ mit $i > j$.

(2.226) Korollar. Es seien $n \in \mathbb{N}$ und ein Körper K gegeben. Für jede obere Dreiecksmatrix $A \in K^{n\times n}$ gilt

$$\det A = \prod_{j\in[1,n]} A_{j,j}.$$

Beweis. Dies folgt aus dem Kästchensatz für Determinanten (2.224) und Induktion. $\square$

Nach Korollar (2.226) lassen sich also insbesondere Determinanten von Matrizen in Zeilenstufenform ablesen.

Alternativer Beweis zu Beispiel (2.219). Zunächst formen wir A mittels Additionsoperationen auf den Zeilen um:

$$\begin{pmatrix} 1 & -1 & 2 \\ 4 & 3 & -1 \\ 2 & -1 & 1\end{pmatrix} \xmapsto{\mathrm{add}_{3,1,-2}\circ\mathrm{add}_{2,1,-4}} \begin{pmatrix} 1 & -1 & 2 \\ 0 & 7 & -9 \\ 0 & 1 & -3\end{pmatrix} \xmapsto{\mathrm{add}_{2,3,-7}} \begin{pmatrix} 1 & -1 & 2 \\ 0 & 0 & 12 \\ 0 & 1 & -3\end{pmatrix}$$

Nach Korollar (2.212), Proposition (2.205) und Korollar (2.226) gilt

$$\det A = \det \begin{pmatrix} 1 & -1 & 2 \\ 4 & 3 & -1 \\ 2 & -1 & 1 \end{pmatrix} = \det \begin{pmatrix} 1 & -1 & 2 \\ 0 & 0 & 12 \\ 0 & 1 & -3 \end{pmatrix} = -\det \begin{pmatrix} 1 & -1 & 2 \\ 0 & 1 & -3 \\ 0 & 0 & 12 \end{pmatrix} = -(1 \cdot 1 \cdot 12) = -12. \qquad \square$$

Ähnlichkeit

(2.227) Definition (Ähnlichkeit von Matrizen)**.** Es seien $n \in \mathbb{N}_0$ und ein Körper K gegeben. Für $A, B \in K^{n\times n}$ sagen wir, dass A *ähnlich* (oder *konjugiert*) zu B ist, wenn es ein $P \in \mathrm{GL}_n(K)$ mit

$$P^{-1}AP = B$$

gibt.

(2.228) Bemerkung. Es seien $n \in \mathbb{N}_0$ und ein Körper K gegeben. Ähnlichkeit von Matrizen ist eine Äquivalenzrelation auf $K^{n\times n}$.

Beweis. Es seien $A, B, C \in K^{n\times n}$ so gegeben, dass A ähnlich zu B und B ähnlich zu C ist. Dann gibt es $P, Q \in \mathrm{GL}_n(K)$ mit $P^{-1}AP = B$ und $Q^{-1}BQ = C$. Es folgt

$$(PQ)^{-1}A(PQ) = Q^{-1}P^{-1}APQ = Q^{-1}BQ = C,$$

also A ähnlich zu C. Folglich ist Ähnlichkeit von Matrizen transitiv.
Für $A \in K^{n\times n}$ gilt $\mathrm{E}_n^{-1}A\mathrm{E}_n = A$, also A ähnlich zu A. Folglich ist Ähnlichkeit von Matrizen reflexiv.
Es seien $A, B \in K^{n\times n}$ so gegeben, dass A ähnlich zu B ist. Dann gibt es ein $P \in \mathrm{GL}_n(K)$ mit $Q^{-1}AP = B$. Es folgt $(P^{-1})^{-1}BP^{-1} = A$, also B ähnlich zu A. Folglich ist Ähnlichkeit von Matrizen symmetrisch.
Insgesamt ist Ähnlichkeit von Matrizen eine Äquivalenzrelation auf $K^{n\times n}$. $\square$

Die Determinante eines Endomorphismus

(2.229) Bemerkung. Es seien $n \in \mathbb{N}$, ein Körper K und $A, B \in K^{n\times n}$ gegeben. Wenn A ähnlich zu B ist, dann gilt

$$\det A = \det B.$$

Beweis. Es sei A ähnlich zu B, so dass es ein $P \in \mathrm{GL}_n(K)$ mit $P^{-1}AP = B$ gibt. Nach Proposition (2.216) folgt

$$\det B = \det(P^{-1}AP) = (\det P)^{-1}(\det A)(\det P) = \det A. \qquad \square$$

(2.230) Korollar. Es seien ein Körper K, ein endlichdimensionaler K-Vektorraum V und ein K-Vektorraumendomorphismus $\varphi\colon V \to V$ gegeben. Für parametrisierte Basen $s = (s_j)_{j\in[1,\dim V]}$ und $s' = (s'_j)_{j\in[1,\dim V]}$ von V gilt

$$\det \mathrm{M}_s^s(\varphi) = \det \mathrm{M}_{s'}^{s'}(\varphi).$$

Beweis. Nach Bemerkung (2.185) ist $\mathrm{M}_s^s(\varphi)$ ähnlich zu $\mathrm{M}_{s'}^{s'}(\varphi)$, so dass Bemerkung (2.229) bereits

$$\det \mathrm{M}_s^s(\varphi) = \det \mathrm{M}_{s'}^{s'}(\varphi)$$

impliziert. $\square$

(2.231) Definition (Determinante)**.** Es seien ein Körper K und ein endlichdimensionaler K-Vektorraum V gegeben. Für einen K-Vektorraumendomorphismus $\varphi\colon V \to V$ definieren wir

$$\det \varphi = \det \mathrm{M}_s^s(\varphi),$$

wobei $s = (s_j)_{j\in[1,\dim V]}$ eine beliebige parametrisierte Basis von V bezeichne.

(2.232) Bemerkung. Es seien $n \in \mathbb{N}$, ein Körper K und ein $A \in K^{n\times n}$ gegeben. Dann ist

$$\det A = \det \varphi_A.$$

Beweis. Es ist

$$\det A = \det \mathrm{M}_{\mathrm{e}}^{\mathrm{e}}(\varphi_A) = \det \varphi_A. \qquad \square$$

Aufgaben

Aufgabe 92 (Eindeutigkeit alternierender Multilinearformen)**.** Es seien $n \in \mathbb{N}$, ein Körper K und alternierende Multilinearformen d und d' auf $K^{n\times n}$ gegeben. Zeigen Sie: Für $A \in K^{n\times n}$ gilt

$$d'(\mathrm{E}_n)d(A) = d(\mathrm{E}_n)d'(A).$$

Aufgabe 93 (Multiplikativität der Determinante)**.** Es seien $n \in \mathbb{N}$ und ein Körper K gegeben.

(a) Es sei eine alternierende Multilinearform d auf $K^{n\times n}$ und ein $B \in K^{n\times n}$ gegeben. Zeigen Sie: Dann ist auch

$$d' \colon K^{n\times n} \to K,\ A \mapsto d(BA)$$

eine alternierende Multilinearform auf $K^{n\times n}$ mit $d'(\mathrm{E}_n) = d(B)$.

(b) Es sei eine alternierende Multilinearform d auf $K^{n\times n}$ gegeben. Zeigen Sie: Für $A, B \in K^{n\times n}$ gilt

$$d(BA)d(\mathrm{E}_n) = d(B)d(A).$$

(c) Zeigen Sie, dass $\det \colon K^{n\times n} \to K$ ein surjektiver Monoidhomomorphismus ist.

Aufgabe 94 (Berechnung von Determinanten)**.**

(a) Es sei ein Körper K gegeben. Berechnen Sie die Determinanten von $A \in K^{3\times 3}$, $B \in \mathbb{F}_7^{5\times 5}$, $C \in \mathbb{R}^{5\times 5}$ gegeben durch

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 3 & 2 \\ 0 & 2 & 2 \end{pmatrix},\ B = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 2^2 & 2 & 0 & 0 & 0 \\ 3^3 & 3^2 & 3 & 0 & 0 \\ 4^4 & 4^3 & 4^2 & 4 & 0 \\ 5^5 & 5^4 & 5^3 & 5^2 & 5 \end{pmatrix},\ C = \begin{pmatrix} e^2 & 0 & e & \pi & \pi^2 \\ 1 & e^{-2} & \sqrt{2} & \sqrt{\pi} & 0 \\ 1 & e^{-2} & \sqrt{3} & \sqrt[3]{e\pi} & 1 \\ 0 & 0 & e^{\frac{\pi}{4}} & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

(b) Es seien $A, B \in \mathbb{Q}^{4\times 4}$ gegeben durch

$$A = \begin{pmatrix} 1 & 1 & -2 & 3 \\ -1 & -2 & 4 & -1 \\ -2 & -4 & 6 & -5 \\ -2 & -1 & 6 & 1 \end{pmatrix},\ B = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 3 & 1 & -1 \\ 0 & 4 & 1 & -7 \\ 3 & -3 & 1 & 16 \end{pmatrix}.$$

Berechnen Sie die Determinanten von A, B und $A^{-2}BA^3B^{-2}$.

Aufgabe 95 (Invertierbarkeitskriterium)**.** Es sei ein Körper K gegeben. Für $c \in K$ sei ferner $A_c \in K^{3\times 3}$ gegeben durch

$$A_c = \begin{pmatrix} 5c & 6-c & 3c+7 \\ -2c & c-3 & -3-2c \\ 4c & -c+5 & 6+3c \end{pmatrix}.$$

Für welche $c \in K$ ist $A_c \in \mathrm{GL}_3(K)$?

9 Algebren und Polynome

Wir wollen Polynome definieren. Ein Polynom in X soll hierbei ein Ausdruck der Form $\sum_{i\in[0,n]} a_i X^i$ für ein beliebiges $n \in \mathbb{N}_0$ sein, also eine Linearkombination von $(X^i)_{i\in[1,n]}$. Dabei ist X^i eine Potenz von X, also ein iteriertes Produkt mit sich selbst. Auch weil wir Polynome miteinander multiplizieren wollen, brauchen wir daher eine Struktur, in der wir multiplizieren können, also ein Monoid. Andererseits haben wir es auch mit einer Linearkombination zu tun, d.h. wir brauchen auch eine Struktur, in welcher wir addieren und mit Skalaren multiplizieren können, also einen Vektorraum. Dies führt uns auf den Begriff einer Algebra.

Assoziative Algebren

(2.233) Definition (assoziative Algebra)**.** Es sei ein Körper K gegeben.

(a) Eine *Algebra über K* (oder *K-Algebra* oder *Algebra*, genauer *unitäre assoziative Algebra* oder *assoziative Algebra mit Einselement* oder *assoziative Algebra mit Eins*) besteht aus einem K-Vektorraum A zusammen mit einer Verknüpfung m auf A so, dass die unterliegende Menge von A ein Monoid mit Multiplikation m wird und so, dass folgende Axiome gelten.

- *Distributivität von Addition und Multiplikation.* Für $x, y, z \in A$ ist

$$m(x+y,z) = m(x,z) + m(y,z),$$
$$m(x,y+z) = m(x,y) + m(x,z).$$

- *Distributivität von Skalarmultiplikation und Multiplikation.* Für $a \in K$, $x, y \in A$ ist

$$m(ax,y) = am(x,y),$$
$$m(x,ay) = am(x,y).$$

Die Verknüpfung m wird *Multiplikation* von A genannt.

(b) Es seien K-Algebren A und B gegeben. Ein *Algebrenhomomorphismus über K* (oder *K-Algebrenhomomorphismus* oder *Homomorphismus von K-Algebren* oder *Homomorphismus*) von A nach B ist ein K-Vektorraumhomomorphismus $\varphi\colon A \to B$ so, dass φ ein Ringhomomorphismus (bzgl. der Multiplikation in A und B) ist.

(2.234) Definition (kommutative Algebra)**.** Es sei ein Körper K gegeben. Eine K-Algebra A heißt *kommutativ*, falls die Multiplikation von A kommutativ ist.

Wir betonen, dass wir die in Definition (1.37) eingeführte Notation für die Multiplikation und das Einselement eines Magmas (und also insbesondere eines Monoids) auch für Algebren weiterhin verwenden. Die Axiome einer Algebra A über einem Körper K lesen sich damit wie folgt:

- *Assoziativität der Addition.* Für $x, y, z \in A$ ist $x + (y + z) = (x + y) + z$.
- *Existenz der Null.* Es existiert ein $n \in A$ mit $n + x = x + n = x$ für alle $x \in A$. Dieses n ist nach Korollar (1.28) eindeutig bestimmt und wird mit $0 = 0^A$ bezeichnet. Wir haben also $0 + x = x + 0 = x$ für alle $x \in A$.
- *Existenz der Negativen.* Für jedes $x \in A$ existiert ein $y \in A$ mit $y + x = x + y = 0$. Dieses y ist nach Korollar (1.33) eindeutig bestimmt und wird mit $-x = (-x)^A$ bezeichnet. Wir haben also $(-x) + x = x + (-x) = 0$.
- *Kommutativität der Addition.* Für $x, y \in A$ ist $x + y = y + x$.
- *Assoziativität der Skalarmultiplikation.* Für $a, b \in K$, $x \in A$ ist $(ab)x = a(bx)$.
- *Einselement der Skalarmultiplikation.* Für $x \in A$ ist $1^K x = x$.
- *Distributivität von Addition und Skalarmultiplikation.* Für $a, b \in K$, $x \in A$ ist $(a + b)x = ax + bx$. Für $a \in K$, $x, y \in A$ ist $a(x + y) = ax + ay$.
- *Assoziativität der Multiplikation.* Für $x, y, z \in A$ ist $x(yz) = (xy)z$.
- *Existenz der Eins.* Es existiert ein $e \in A$ mit $ex = xe = x$ für alle $x \in A$. Dieses e ist nach Korollar (1.28) eindeutig bestimmt und wird mit $1 = 1^A$ bezeichnet. Wir haben also $1^A x = x1^A = x$ für alle $x \in A$.
- *Distributivität von Addition und Multiplikation.* Für $x, y, z \in A$ ist $(x + y)z = (xz) + (yz)$ und $x(y + z) = (xy) + (xz)$.
- *Distributivität von Skalarmultiplikation und Multiplikation.* Für $a \in K$, $x, y \in A$ ist $(ax)y = a(xy)$ und $x(ay) = a(xy)$.

Ist A kommutativ, so gilt zusätzlich noch:

- *Kommutativität der Multiplikation.* Für $x, y \in A$ ist $xy = yx$.

Die Axiome eines Algebrenhomomorphismus $\varphi\colon A \to B$ über einem Körper K in Standardnotation lesen sich wie folgt:

- *Verträglichkeit mit den Additionen.* Für $x, x' \in A$ ist $\varphi(x + x') = \varphi(x) + \varphi(x')$.
- *Verträglichkeit der Nullen.* Es ist $\varphi(0) = 0$.
- *Verträglichkeit der Negativen.* Für $x \in A$ ist $\varphi(-x) = -\varphi(x)$.
- *Verträglichkeit mit den Skalarmultiplikationen.* Für $a \in K$, $x \in A$ ist $\varphi(ax) = a\,\varphi(x)$.
- *Verträglichkeit mit den Multiplikationen.* Für $x, x' \in A$ ist $\varphi(xx') = \varphi(x)\varphi(x')$.
- *Verträglichkeit der Einsen.* Es ist $\varphi(1) = 1$.

Nach Bemerkung (2.36) wissen wir, dass das zweite und dritte Axiom (Verträglichkeit der Nullen und der Negativen) eines Algebrenhomomorphismus redundant sind.
Insbesondere ist jede Algebra bzgl. Addition und Multiplikation ein Ring und jeder Algebrenhomomorphismus ein Ringhomomorphismus.
Analog zu Bemerkung (2.41) lassen sich die Distributivgesetze der Multiplikation einer Algebra auch wie folgt lesen:

(2.235) Bemerkung. Es seien ein Körper K und eine K-Algebra A gegeben.

(a) Für $y \in A$ ist

$$\rho_y\colon A \to A,\ x \mapsto xy$$

ein K-Vektorraumhomomorphismus.

(b) Für $x \in A$ ist

$$\lambda_x\colon A \to A,\ y \mapsto xy$$

ein K-Vektorraumhomomorphismus.

Beweis.

(a) Es sei $y \in A$ gegeben. Da für $x, x' \in A$ stets

$$\rho_y(x + x') = (x + x')y = xy + x'y = \rho_y(x) + \rho_y(x')$$

und für $a \in K$, $x \in A$ stets

$$\rho_y(ax) = (ax)y = a(xy) = \rho_y(x)$$

gilt, ist ρ_y nach Bemerkung (2.36) ein Vektorraumhomomorphismus.

(b) Es sei $x \in A$ gegeben. Da für $y, y' \in A$ stets

$$\lambda_x(y + y') = x(y + y') = xy + xy' = \lambda_x(y) + \lambda_x(y')$$

und für $a \in K$, $y \in A$ stets

$$\lambda_x(ay) = x(ay) = a(xy) = a\lambda_x(y)$$

gilt, ist λ_x nach Bemerkung (2.36) ein Vektorraumhomomorphismus. □

(2.236) Beispiel. Es sei ein Körper K gegeben.

(a) Es wird K, aufgefasst als K-Vektorraum wie in Beispiel (2.33)(a)(i), eine K-Algebra mit Multiplikation gegeben durch Multiplikation des Körpers K.

(b) Für jeden K-Vektorraum V wird $\mathrm{Hom}_K(V,V) = \mathrm{End}_K(V)$ eine K-Algebra mit Multiplikation gegeben durch Komposition.

(c) Für $n \in \mathbb{N}_0$ wird $K^{n\times n}$ eine K-Algebra mit Multiplikation gegeben durch Matrixmultiplikation.

Beweis.

(b) Dies folgt aus Proposition (2.146).

(c) Dies folgt aus Proposition (2.161). □

(2.237) Definition (Algebrenisomorphismus)**.** Es seien ein Körper K und K-Algebren A und B gegeben.

(a) Ein *Algebrenisomorphismus über* K (oder K*-Algebrenisomorphismus* oder *Isomorphismus von* K*-Algebren* oder *Isomorphismus*) von A nach B ist ein K-Algebrenhomomorphismus $\varphi\colon A \to B$ so, dass φ eine invertierbare Abbildung und $\varphi^{-1}\colon B \to A$ ein K-Algebrenhomomorphismus ist.

(b) Wir sagen, dass A *isomorph* zu B (*als* K*-Algebren*) ist, geschrieben $A \cong B$, falls ein K-Algebrenisomorphismus von A nach B existiert.

Polynomalgebra

(2.238) Definition (Polynomalgebra)**.** Es sei ein Körper K gegeben. Eine *Polynomalgebra* über K (oder K*-Polynomalgebra* oder *Polynomalgebra* oder *Polynomring*) besteht aus einer K-Algebra P zusammen mit einem Element $X \in P$ so, dass $(X^i)_{i\in\mathbb{N}_0}$ eine Basis von P ist. Das Element X wird *Unbestimmte* von P genannt.
Für eine K-Polynomalgebra P mit Unbestimmter X sagen wir, dass P eine *Polynomalgebra in* (*der Unbestimmten*) X ist. Die Elemente von P werden *Polynome* in X genannt. Das Nullelement von P wird auch *Nullpolynom* genannt.

Es seien ein Körper K und eine K-Polynomalgebra P in der Unbestimmten X gegeben. Da $(X^i)_{i\in\mathbb{N}_0}$ ein Erzeugendensystem von P ist, gibt es für jedes Element $f \in P$ ein $a \in K^{(\mathbb{N}_0)}$ mit $f = \sum_{i\in\mathbb{N}_0} a_i X^i$. Für jedes $a \in K^{(\mathbb{N}_0)}$ ist jedoch $a_i = 0$ für fast alle $i \in \mathbb{N}_0$, d.h. es existiert ein $n \in \mathbb{N}_0$ mit $\sum_{i\in\mathbb{N}_0} a_i X^i = \sum_{i\in[0,n]} a_i X^i$. Andererseits ist $(X^i)_{i\in\mathbb{N}_0}$ auch linear unabhängig, d.h. aus $\sum_{i\in\mathbb{N}_0} a_i X^i = \sum_{i\in\mathbb{N}_0} b_i X^i$ für $a, b \in K^{(\mathbb{N}_0)}$ folgt bereits $a_i = b_i$ für alle $i \in \mathbb{N}_0$. Polynome in X sind also durch ihre Koeffizienten eindeutig festgelegt.

(2.239) Bemerkung. Es seien ein Körper K und eine K-Polynomalgebra P in X gegeben. Ferner sei $s := (X^i)_{i\in\mathbb{N}_0}$. Dann ist

$$\lambda_s\colon K^{(\mathbb{N}_0)} \to P,\ a \mapsto \sum_{i\in\mathbb{N}_0} a_i X^i$$

ein K-Vektorraumisomorphismus.

Beweis. Da s eine Basis von P ist, folgt dies nach Bemerkung (2.108). □

(2.240) Bemerkung. Es seien ein Körper K und eine K-Polynomalgebra P in X gegeben. Für $a, b \in K^{(\mathbb{N}_0)}$ gilt

$$(\sum_{i\in\mathbb{N}_0} a_i X^i)(\sum_{j\in\mathbb{N}_0} b_j X^j) = \sum_{k\in\mathbb{N}_0} (\sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}} a_i b_j) X^k$$

in P.

Beweis. Für $a, b \in K^{(\mathbb{N}_0)}$ gilt

$$(\sum_{i\in\mathbb{N}_0} a_i X^i)(\sum_{j\in\mathbb{N}_0} b_j X^j) = \sum_{i\in\mathbb{N}_0}\sum_{j\in\mathbb{N}_0} a_i b_j X^{i+j} = \sum_{k\in\mathbb{N}_0} (\sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}} a_i b_j) X^k$$

in P. □

(2.241) Korollar. Es seien ein Körper K und eine K-Polynomalgebra P in X gegeben. Dann ist P ein kommutative K-Algebra.

(2.242) Proposition. Es sei ein Körper K gegeben. Wir definieren $X \in K^{(\mathbb{N}_0)}$ durch

$$X := \mathrm{e}_1.$$

Dann wird der K-Vektorraum $K^{(\mathbb{N}_0)}$ eine K-Polynomalgebra in X mit Multiplikation gegeben durch

$$ab = (\sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}} a_i b_j)_{k\in\mathbb{N}_0}$$

für $a, b \in K^{(\mathbb{N}_0)}$. Die Eins von $K^{(\mathbb{N}_0)}$ ist gegeben durch

$$1 = \mathrm{e}_0.$$

Beweis. Wir definieren

$$m\colon K^{(\mathbb{N}_0)} \times K^{(\mathbb{N}_0)} \to K^{(\mathbb{N}_0)},\ (a,b) \mapsto (\sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}} a_i b_j)_{k\in\mathbb{N}_0}.$$

Zunächst wollen wir zeigen, dass der K-Vektorraum $K^{(\mathbb{N}_0)}$ eine K-Algebra mit Multiplikation m wird.
Für $a, b, c \in K^{(\mathbb{N}_0)}$ gilt

$$\begin{aligned} m(a, m(b,c)) &= m(a, (\sum_{\substack{j,k\in\mathbb{N}_0\\ j+k=r}} b_j c_k)_{r\in\mathbb{N}_0}) = (\sum_{\substack{i,r\in\mathbb{N}_0\\ i+r=l}} a_i \sum_{\substack{j,k\in\mathbb{N}_0\\ j+k=r}} b_j c_k)_{l\in\mathbb{N}_0} = (\sum_{\substack{i,r\in\mathbb{N}_0\\ i+r=l}} \sum_{\substack{j,k\in\mathbb{N}_0\\ j+k=r}} a_i(b_j c_k))_{l\in\mathbb{N}_0} \\ &= (\sum_{\substack{i,j,k\in\mathbb{N}_0\\ i+j+k=l}} a_i b_j c_k)_{l\in\mathbb{N}_0} = (\sum_{\substack{r,k\in\mathbb{N}_0\\ r+k=l}} \sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=r}} (a_i b_j) c_k)_{l\in\mathbb{N}_0} = (\sum_{\substack{r,k\in\mathbb{N}_0\\ r+k=l}} (\sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=r}} a_i b_j) c_k)_{l\in\mathbb{N}_0} \\ &= m((\sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=r}} a_i b_j)_{r\in\mathbb{N}_0}, c) = m(m(a,b), c). \end{aligned}$$

Folglich ist m assoziativ.
Für $a \in K^{(\mathbb{N}_0)}$ gilt

$$m(\mathrm{e}_0, a) = (\sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}} (\mathrm{e}_0)_i a_j)_{k\in\mathbb{N}_0} = (\sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}} \delta_{i,0} a_j)_{k\in\mathbb{N}_0} = (a_k)_{k\in\mathbb{N}_0} = a.$$

Folglich ist e_0 ein neutrales Element bzgl. m.
Für $a, b, c \in K^{(\mathbb{N}_0)}$ gilt

$$\begin{aligned} m(a+b, c) &= m((a_i + b_i)_{i\in\mathbb{N}_0}, c) = (\sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}} (a_i + b_i) c_j)_{k\in\mathbb{N}_0} = (\sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}} a_i c_j + \sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}} b_i c_j)_{k\in\mathbb{N}_0} \\ &= (\sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}} a_i c_j)_{k\in\mathbb{N}_0} + (\sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}} b_i c_j)_{k\in\mathbb{N}_0} = m(a,c) + m(b,c), \\ m(a, b+c) &= m(a, (b_j + c_j)_{j\in\mathbb{N}_0}) = (\sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}} a_i (b_j + c_j))_{k\in\mathbb{N}_0} = (\sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}} a_i b_j + \sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}} a_i c_j)_{k\in\mathbb{N}_0} \\ &= (\sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}} a_i b_j)_{k\in\mathbb{N}_0} + (\sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}} a_i c_j)_{k\in\mathbb{N}_0} = m(a,b) + m(a,c). \end{aligned}$$

Für $c \in K$, $a, b \in K^{(\mathbb{N}_0)}$ gilt

$$m(ca, b) = m((ca_i)_{i\in\mathbb{N}_0}, b) = (\sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}} (ca_i) b_j)_{k\in\mathbb{N}_0} = (c \sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}} a_i b_j)_{k\in\mathbb{N}_0} = c(\sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}} a_i b_j)_{k\in\mathbb{N}_0} = cm(a,b),$$

$$m(a,cb) = m(a,(cb_j)_{j\in\mathbb{N}_0}) = (\sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}} a_i(cb_j))_{k\in\mathbb{N}_0} = (c\sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}} a_ib_j)_{k\in\mathbb{N}_0} = c(\sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}} a_ib_j)_{k\in\mathbb{N}_0} = cm(a,b).$$

Folglich ist m kompatibel mit Addition und Skalarmultiplikation auf $K^{(\mathbb{N}_0)}$.
Insgesamt wird $K^{(\mathbb{N}_0)}$ eine K-Algebra mit Multiplikation m, d.h. mit

$$ab = m(a,b) = (\sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}} a_ib_j)_{k\in\mathbb{N}_0}$$

für $a,b \in K^{(\mathbb{N}_0)}$. Um zu zeigen, dass $K^{(\mathbb{N}_0)}$ eine Polynomalgebra in $X = \mathrm{e}_1$ wird, verbleibt es zu zeigen, dass $(X^l)_{l\in\mathbb{N}_0}$ eine Basis von $K^{(\mathbb{N}_0)}$ ist. Hierzu zeigen wir per Induktion nach $l \in \mathbb{N}_0$, dass $X^l = \mathrm{e}_l$ ist. Für $l = 0$ gilt $X^0 = 1 = \mathrm{e}_0$. Es sei also ein $l \in \mathbb{N}$ gegeben und es gelte $X^{l-1} = \mathrm{e}_{l-1}$. Dann folgt

$$X^l = X^{l-1}X = \mathrm{e}_{l-1}\mathrm{e}_l = (\sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}} (\mathrm{e}_{l-1})_i(\mathrm{e}_1)_j)_{k\in\mathbb{N}_0} = (\sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}} \delta_{i,l-1}\delta_{j,1})_{k\in\mathbb{N}_0} = (\delta_{k,l})_{k\in\mathbb{N}_0} = \mathrm{e}_l.$$

Folglich ist $(X^l)_{l\in\mathbb{N}_0} = (\mathrm{e}_l)_{l\in\mathbb{N}_0} = \mathrm{e}$ die Standardbasis von $K^{(\mathbb{N}_0)}$ und damit $K^{(\mathbb{N}_0)}$ eine Polynomalgebra in X. □

Der Einsetzungshomomorphismus

(2.243) Proposition. Es seien ein Körper K und eine K-Polynomalgebra P in X gegeben. Für jede K-Algebra A und alle $x \in A$ gibt es genau einen K-Algebrenhomomorphismus $\mathrm{ev}_x\colon P \to A$ mit $\mathrm{ev}_x(X) = x$, gegeben durch

$$\mathrm{ev}_x(\sum_{i\in\mathbb{N}_0} a_iX^i) = \sum_{i\in\mathbb{N}_0} a_ix^i$$

für $a \in K^{(\mathbb{N}_0)}$.

Beweis. Nach Proposition (2.111)(a) gibt es einen eindeutigen K-Vektorraumhomomorphismus $\mathrm{ev}_x\colon P \to A$ mit $\mathrm{ev}_x(X^i) = x^i$ für $i \in \mathbb{N}_0$, gegeben durch

$$\mathrm{ev}_x(\sum_{i\in\mathbb{N}_0} a_iX^i) = \sum_{i\in\mathbb{N}_0} a_ix^i$$

für $a \in K^{(\mathbb{N}_0)}$. Insbesondere gilt also $\mathrm{ev}_x(X) = x$. Für $a,b \in K^{(\mathbb{N}_0)}$ gilt ferner

$$\begin{aligned}\mathrm{ev}_x((\sum_{i\in\mathbb{N}_0} a_iX^i)(\sum_{j\in\mathbb{N}_0} b_jX^j)) &= \mathrm{ev}_x(\sum_{k\in\mathbb{N}_0}(\sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}} a_ib_j)X^k) = \sum_{k\in\mathbb{N}_0}(\sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}} a_ib_j)x^k = (\sum_{i\in\mathbb{N}_0} a_ix^i)(\sum_{j\in\mathbb{N}_0} b_jx^j)\\ &= \mathrm{ev}_x(\sum_{i\in\mathbb{N}_0} a_iX^i)\,\mathrm{ev}_x(\sum_{j\in\mathbb{N}_0} b_jX^j).\end{aligned}$$

Folglich ist ev_x ein K-Algebrenhomomorphismus.
Nun sei umgekehrt ein beliebiger K-Algebrenhomomorphismus $\varphi\colon P \to A$ mit $\varphi(X) = x$ gegeben. Für $i \in \mathbb{N}_0$ gilt dann auch

$$\varphi(X^i) = \varphi(X)^i = x^i = \mathrm{ev}_x(X^i).$$

Da aber $(X^i)_{i\in\mathbb{N}_0}$ eine Basis von P und φ insbesondere ein K-Vektorraumhomomorphismus ist, impliziert dies bereits $\varphi = \mathrm{ev}_x$ nach Proposition (2.111)(a). □

(2.244) Definition (Einsetzungshomomorphismus)**.** Es seien ein Körper K, eine K-Polynomalgebra P in X und eine K-Algebra A gegeben. Für $x \in A$ heißt der eindeutige K-Algebrenhomomorphismus

$$\mathrm{ev}_x = \mathrm{ev}_x^P\colon P \to A$$

mit $\mathrm{ev}_x(X) = x$ der *Einsetzungshomomorphismus*. Wir schreiben

$$f(x) := \mathrm{ev}_x(f)$$

für $f \in P$.

(2.245) Bemerkung. Es seien ein Körper K, eine K-Polynomalgebra P in X und eine K-Polynomalgebra Q in Y gegeben. Dann sind $\mathrm{ev}_Y^P\colon P \to Q$ und $\mathrm{ev}_X^Q\colon Q \to P$ sich gegenseitig invertierende K-Algebrenisomorphismen.

Beweis. Es gilt $\mathrm{ev}_X^Q(\mathrm{ev}_Y^P(X)) = \mathrm{ev}_X^Q(Y) = X$ und $\mathrm{ev}_Y^P(\mathrm{ev}_X^Q(Y)) = \mathrm{ev}_Y^P(X) = Y$. Andererseits haben wir aber auch $\mathrm{id}_P(X) = X$ und $\mathrm{id}_Q(Y) = Y$. Nach Proposition (2.243) folgt $\mathrm{ev}_X^Q \circ \mathrm{ev}_Y^P = \mathrm{id}_P$ und $\mathrm{ev}_Y^P \circ \mathrm{ev}_X^Q = \mathrm{id}_P$, d.h. ev_Y^P und ev_X^Q sind sich gegenseitig invertierende K-Algebrenisomorphismen. □

(2.246) Konvention. Es sei ein Körper K gegeben. Nach Proposition (2.242) und Bemerkung (2.245) gibt es bis auf Isomorphie von K-Algebren genau eine K-Polynomalgebra. Wenn wir im Folgenden von $K[X]$ sprechen und X nicht anderweitig definiert ist, so meinen wir damit stets eine K-Polynomalgebra in der Unbestimmten X. Ein Polynom f in $K[X]$ ist dann also von der Form

$$f = \sum_{i\in\mathbb{N}_0} a_i X^i$$

für ein $a \in K^{(\mathbb{N}_0)}$.

Wir veranschaulichen das Einsetzen von Algebrenelementen in Polynome noch einmal an einigen Beispielen:

(2.247) Beispiel. Es seien ein Körper K sowie $f \in K[X]$, $a \in K^{(\mathbb{N}_0)}$ mit $f = \sum_{i\in\mathbb{N}_0} a_i X^i$ gegeben.

(a) Für $b \in K$ ist $f(b) \in K$ gegeben durch

$$f(b) = \sum_{i\in\mathbb{N}_0} a_i b^i.$$

(b) Es sei ein K-Vektorraum V gegeben. Für $\varphi \in \mathrm{End}_K(V)$ ist

$$f(\varphi) = \sum_{i\in\mathbb{N}_0} a_i \varphi^i.$$

(c) Es sei $n \in \mathbb{N}_0$ gegeben. Für $A \in K^{n\times n}$ ist

$$f(A) = \sum_{i\in\mathbb{N}_0} a_i A^i.$$

(d) Es ist

$$f(X) = \sum_{i\in\mathbb{N}_0} a_i X^i = f.$$

(2.248) Proposition. Es sei ein Körper K gegeben. Die Abbildung

$$\iota\colon K \to K[X],\ a \mapsto a \cdot 1^{K[X]}$$

ist ein injektiver Ringhomomorphismus.

Beweis. Für $a, b \in K$ gilt

$$\iota(a+b) = (a+b)\cdot 1^{K[X]} = a\cdot 1^{K[X]} + b\cdot 1^{K[X]} = \iota(a) + \iota(b),$$
$$\iota(ab) = (ab)\cdot 1^{K[X]} = (a\cdot 1^{K[X]})(b\cdot 1^{K[X]}) = \iota(a)\,\iota(b).$$

Da ferner auch

$$\iota(1) = 1^K \cdot 1^{K[X]} = 1^{K[X]}$$

gilt, ist ι nach Bemerkung (1.103) ein Ringhomomorphismus. Für $a, b \in K$ mit $\iota(a) = \iota(b)$ in $K[X]$ gilt $a\cdot 1^{K[X]} = b\cdot 1^{K[X]}$, also $a = b$ in K wegen der linearen Unabhängigkeit von $(1^{K[X]})$. Folglich ist ι injektiv. □

(2.249) Konvention. Es sei ein Körper K gegeben. Von jetzt an identifizieren wir K mit dem Bild der injektiven Abbildung $\iota\colon K \to K[X]$, $a \mapsto a\cdot 1^{K[X]}$ aus Proposition (2.248). Das heißt, unter Missbrauch der Notationen schreiben wir K anstatt $\mathrm{Im}\,\iota$, und, für $a \in K$, notieren wir das Bild $\iota(a)$ von a auch durch a.

Grad eines Polynoms

Es seien ein Körper K und ein $f \in K[X] \setminus \{0\}$ gegeben. Da $(X^i)_{i\in\mathbb{N}_0}$ eine Basis von $K[X]$ ist, gibt es genau ein $a \in K^{(\mathbb{N}_0)}$ mit

$$f = \sum_{i\in\mathbb{N}_0} a_i X^i.$$

Wegen $a_i = 0$ für fast alle $i \in \mathbb{N}_0$, d.h. es gibt ein $n \in \mathbb{N}_0$ mit $a_n \neq 0$ und $a_i = 0$ für $i > n$. Somit ist

$$f = \sum_{i\in[0,n]} a_i X^i.$$

Wir wollen nun etwas Terminologie für diese endliche Darstellung eines Polynoms festlegen.

(2.250) Definition (Grad, Koeffizienten)**.** Es seien ein Körper K, ein $f \in K[X] \setminus \{0\}$ und $a \in K^{(\mathbb{N}_0)}$ mit $f = \sum_{i\in\mathbb{N}_0} a_i X^i$ gegeben.

(a) Der *Grad* von f ist definiert als

$$\deg f := \max\{i \in \mathbb{N}_0 \mid a_i \neq 0\}.$$

(b) Die Einträge a_i von a für $i \in [0, \deg f]$ werden *Koeffizienten* von f genannt. Der Eintrag $a_{\deg f}$ heißt *Leitkoeffizient* von f. Der Eintrag a_0 heißt *konstanter Koeffizient* von f.

(c) Wir sagen, dass f ein *normiertes* Polynom ist, falls der Leitkoeffizient von f gleich 1 ist.

Für jedes $f \in K[X] \setminus \{0\}$ für einen Körper K gibt es also $a_i \in K$ für $i \in [0, \deg f]$ mit

$$f = \sum_{i\in[0,\deg f]} a_i X^i.$$

Der Leitkoeffizient $a_{\deg f}$ ist nach Definition (2.250)(a) stets ungleich 0.
Wir betonen, dass das Nullpolynom keinen Grad hat.

(2.251) Bemerkung. Es seien ein Körper K und ein $f \in K[X]$ gegeben. Dann ist $f(0^K)$ der konstante Koeffizient von f.

(2.252) Bemerkung. Es sei ein Körper K gegeben. Dann ist

$$K = \{f \in K[X] \mid f = 0 \text{ oder } \deg f = 0\}.$$

(2.253) Bemerkung. Es seien ein Körper K und $f, g \in K[X] \setminus \{0\}$ gegeben.

(a) Wenn $f + g \neq 0$ ist, gilt

$$\deg(f + g) \leq \max(\deg f, \deg g).$$

Wenn $\deg f \neq \deg g$ ist, gilt

$$\deg(f + g) = \max(\deg f, \deg g).$$

(b) Für $f, g \in K[X] \setminus \{0\}$ gilt $fg \neq 0$ und

$$\deg(fg) = \deg f + \deg g.$$

Beweis. Es seien $a, b \in K^{(\mathbb{N}_0)}$ mit $f = \sum_{i\in\mathbb{N}_0} a_i X^i$ und $g = \sum_{i\in\mathbb{N}_0} b_i X^i$ gegeben.

(a) Es ist $f+g=\sum_{i\in\mathbb{N}_0}(a_i+b_i)X^i$. Für $i\in\mathbb{N}_0$ mit $a_i+b_i\neq 0$ gilt auch $a_i\neq 0$. Folglich ist

$$\deg(f+g)=\max\{i\in\mathbb{N}_0\mid a_i+b_i\neq 0\}\leq\max\{i\in\mathbb{N}_0\mid a_i\neq 0\}=\deg f.$$

Analog lässt sich $\deg(f+g)\leq\deg g$ zeigen.

Nun gelte $\deg f\neq\deg g$. Wir nehmen o.B.d.A. an, dass $\deg f<\deg g$ ist. Für $i\in\mathbb{N}_0$ mit $i\geq\deg g$ gilt dann $a_i=0$ und damit

$$a_i+b_i=\begin{cases}b_{\deg g}, & \text{falls } i=\deg g,\\ 0, & \text{falls } i>\deg g.\end{cases}$$

Folglich ist $\deg(f+g)=\deg g=\max(\deg f,\deg g)$.

(b) Nach Bemerkung (2.240) ist $fg=\sum_{k\in\mathbb{N}_0}(\sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}}a_ib_j)X^k$. Für $k\in\mathbb{N}_0$ mit $k\geq\deg f+\deg g$ gilt dann

$$\sum_{\substack{i,j\in\mathbb{N}_0\\ i+j=k}}a_ib_j=\begin{cases}a_{\deg f}b_{\deg g}, & \text{falls } k=\deg f+\deg g,\\ 0, & \text{falls } i>\deg f+\deg g.\end{cases}$$

Folglich ist $fg\neq 0$ und $\deg(fg)=\deg f+\deg g$. □

(2.254) Korollar. Es seien ein Körper K und $f,g,h\in K[X]$ gegeben. Genau dann gilt $fg=fh$, wenn $g=h$ ist.

Beweis. Dies folgt aus Aufgabe 37 und Bemerkung (2.253)(b). □

(2.255) Korollar. Es sei ein Körper K gegeben. Dann ist

$$K[X]^\times=K^\times=K\setminus\{0\}.$$

Beweis. Für $f\in K[X]^\times$ gilt

$$\deg f+\deg f^{-1}=\deg(ff^{-1})=\deg 1=0,$$

also $\deg f=\deg f^{-1}=0$ und damit $f,f^{-1}\in K^\times=K\setminus\{0\}$. □

Teilbarkeitslehre in Polynomringen

Wir leiten für Polynome über einem Körper eine Division mit Rest her, ganz ähnlich zu der, welche wir von den ganzen Zahlen her kennen, vgl. Erinnerung (1.116).

(2.256) Satz (Division mit Rest)**.** Es sei ein Körper K gegeben. Für alle $f\in K[X]$, $g\in K[X]\setminus\{0\}$ gibt es eindeutige $q,r\in K[X]$ mit

$$f=qg+r$$

und $\deg r<\deg g$ oder $r=0$.

Beweis. Ist $\deg f<\deg g$ oder $f=0$, so gilt $f=qg+r$ mit $q=0$ und $r=f$. Im Folgenden sei angenommen, dass $\deg f\geq\deg g$ ist. Wir zeigen durch Induktion nach $\deg f$, dass es $q,r\in K[X]$ mit $f=qg+r$ und $\deg r<\deg g$ oder $r=0$ gibt.
Ist $\deg f=0$, so ist wegen $\deg f\geq\deg g$ auch $\deg g=0$, also $g\in K[X]^\times$ und damit $f=qg+r$ mit $q=fg^{-1}$ und $r=0$.
Es sei also $\deg f>0$ und für $f'\in K[X]$ mit $\deg f'<\deg f$ gebe es $q',r\in K[X]$ mit $f'=q'g+r'$ und $\deg r'<\deg g$ oder $r'=0$. Ferner seien $a,b\in K^{(\mathbb{N}_0)}$ mit $f=\sum_{i\in\mathbb{N}_0}a_iX^i$ und $g=\sum_{i\in\mathbb{N}_0}b_iX^i$ gegeben. Wir setzen $f':=f-a_{\deg f}b_{\deg g}^{-1}X^{\deg f-\deg g}g$. Dann ist

$$f'=f-a_{\deg f}b_{\deg g}^{-1}X^{\deg f-\deg g}g=\sum_{i\in\mathbb{N}_0}a_iX^i-a_{\deg f}b_{\deg g}^{-1}X^{\deg f-\deg g}\sum_{i\in\mathbb{N}_0}b_iX^i$$

$$
\begin{aligned}
&= \sum_{i\in\mathbb{N}_0} a_i X^i - \sum_{i\in\mathbb{N}_0} a_{\deg f} b_{\deg g}^{-1} b_i X^{i+\deg f-\deg g} \\
&= \sum_{i\in[0,\deg f-\deg g-1]} a_i X^i + \sum_{\substack{i\in\mathbb{N}_0 \\ i\geq \deg f-\deg g}} a_i X^i - \sum_{\substack{i\in\mathbb{N}_0 \\ i\geq \deg f-\deg g}} a_{\deg f} b_{\deg g}^{-1} b_{i-(\deg f-\deg g)} X^i \\
&= \sum_{i\in[0,\deg f-\deg g-1]} a_i X^i + \sum_{\substack{i\in\mathbb{N}_0 \\ i\geq \deg f-\deg g}} (a_i - a_{\deg f} b_{\deg g}^{-1} b_{i-(\deg f-\deg g)}) X^i,
\end{aligned}
$$

also $\deg(f') < \deg f$ oder $f' = 0$. Nach Induktionsvoraussetzung und unserer Vorbemerkung gibt es $q', r \in K[X]$ mit $f' = q'g + r$ und $\deg r < \deg g$ oder $r = 0$. Wir setzen $q := q' + a_{\deg f} b_{\deg g}^{-1} X^{\deg f-\deg f}$ und erhalten

$$
\begin{aligned}
f &= f' + a_{\deg f} b_{\deg g}^{-1} X^{\deg f-\deg f} g = q'g + r + a_{\deg f} b_{\deg g}^{-1} X^{\deg f-\deg f} g \\
&= (q' + a_{\deg f} b_{\deg g}^{-1} X^{\deg f-\deg f})g + r = qg + r.
\end{aligned}
$$

Für die Eindeutigkeit seien $q, q', r, r' \in K[X]$ mit $f = qg + r = q'g + r'$, mit $\deg r < \deg g$ oder $r = 0$, und mit $\deg r' < \deg g$ oder $r' = 0$ gegeben. Dann gilt

$$(q - q')g = qg - q'g = r' - r.$$

Wäre $q - q' \neq 0$, so wäre nach Bemerkung (2.253) auch $r' - r \neq 0$ und

$$\deg(q - q') + \deg g = \deg((q - q')g) = \deg(r' - r) < \deg g.$$

Da dies ein Widerspruch ist, folgt $q - q' = 0$ und damit auch $r' - r = 0$ nach Bemerkung (2.253). Somit ist $q = q'$ und $r = r'$. □

(2.257) Definition (Teilbarkeit)**.** Es seien ein Körper K und $f, g \in K[X]$ gegeben. Wir sagen f *teilt* g (oder dass f ein *Teiler* von g ist oder dass g ein *Vielfaches* von f ist), geschrieben $f \mid g$, falls es ein $q \in K[X]$ mit $g = qf$ gibt. Wenn f kein Teiler von g ist, so schreiben wir $f \nmid g$.

Nullstellen

(2.258) Definition (Nullstelle)**.** Es seien ein Körper K und ein $f \in K[X]$ gegeben. Eine *Nullstelle* von f ist ein $a \in K$ mit

$$f(a) = 0.$$

(2.259) Bemerkung. Es seien ein Körper K, ein $f \in K[X]$ und ein $a \in K$ gegeben. Genau dann ist a eine Nullstelle von f, wenn

$$(X - a) \mid f$$

gilt.

Beweis. Nach dem Satz über die Division mit Rest (2.256) gibt es $q, r \in K[X]$ mit

$$f = q \cdot (X - a) + r$$

und $\deg(r) < \deg(X - a)$ oder $r = 0$. Wegen $\deg(X - a) = 1$ ist $r = 0$ oder $\deg r = 0$, also $r \in K$. Nun ist aber

$$0 = f(a) = q(a)(a - a) + r(a) = r(a),$$

d.h. der konstante Koeffizient von r ist 0. Folglich ist $r = 0$ und damit $f = q \cdot (X - a)$, d.h. $(X - a) \mid f$.
Gilt umgekehrt $(X - a) \mid f$, d.h. gibt es ein $q \in K[X]$ mit $f = q \cdot (X - a)$, so folgt

$$f(a) = q(a)(a - a) = 0,$$

d.h. a ist eine Nullstelle von f. □

(2.260) Korollar. Es sei ein Körper K gegeben. Jedes $f \in K[X] \setminus \{0\}$ hat höchstens $\deg f$ Nullstellen.

Beweis. Wir führen Induktion nach $\deg f$. Ist $\deg f = 0$, so hat f wegen $f \neq 0$ keine Nullstellen. Es sei also $\deg f > 0$ und es sei angenommen, dass alle $f' \in K[X] \setminus \{0\}$ mit $\deg f' < \deg f$ höchstens $\deg f'$ Nullstellen haben. Wenn f keine Nullstellen hat, so hat f insbesondere höchstens $\deg f$ Nullstellen. Wir nehmen daher im Folgenden an, dass f eine Nullstelle a hat. Nach Bemerkung (2.259) gilt $(X-a) \mid f$, d.h. es gibt ein $q \in K[X]$ mit $f = q \cdot (X-a)$. Wegen $f \neq 0$ ist $q \neq 0$ und

$$\deg f = \deg(q \cdot (X-a)) = \deg q + \deg(X-a) = \deg q + 1$$

nach Bemerkung (2.253)(b). Für jede von a verschiedene Nullstelle b von f gilt außerdem $0 = f(b) = q(b)(b-a)$ und damit $q(b) = 0$, d.h. b ist eine Nullstelle von q. Wegen $\deg q = \deg f - 1 < \deg f$ hat q nach Induktionsvoraussetzung höchstens $\deg q$ Nullstellen. Folglich hat f höchstens $\deg q = \deg f - 1$ von a verschiedene Nullstellen und damit höchstens $\deg f$ Nullstellen. □

(2.261) Definition (Zerfällung in Linearfaktorung)**.** Es seien ein Körper K und ein $f \in K[X] \setminus \{0\}$ gegeben. Wir sagen, dass f in *Linearfaktoren zerfällt*, falls es $b \in K$ und $a_i \in K$ für $i \in [1, \deg f]$ mit

$$f = b \prod_{i \in [1, \deg f]} (X - a_i)$$

gibt.

Wir betonen, dass die a_i in Definition (2.261) nicht notwendigerweise verschieden sein müssen.

(2.262) Proposition. Es seien ein Körper K und ein $f \in K[X] \setminus \{0\}$ gegeben. Für jedes $a \in K$ gibt es eindeutige $m \in \mathbb{N}_0$, $g \in K[X]$ mit

$$f = (X-a)^m g$$

und $g(a) \neq 0$.

Beweis. Es sei $a \in K$ gegeben. Wir zeigen durch Induktion nach $\deg f$, dass es $m \in \mathbb{N}_0$, $g \in K[X]$ mit $f = (X-a)^m g$ und $g(a) \neq 0$ gibt.
Ist $\deg f = 0$, so ist a keine Nullstelle von f und es gilt $f = (X-a)^m g$ mit $m = 0$ und $g = f$.
Es sei also $\deg f > 0$ und für $f' \in K[X]$ mit $\deg f' < \deg f$ gebe es $m' \in \mathbb{N}_0$, $g' \in K[X]$ mit $f = (X-a)^m g$ und $g(a) \neq 0$. Wenn a keine Nullstelle von f ist, dann gilt $f = (X-a)^m g$ mit $m = 0$ und $g = f$. Es sei also im Folgenden a eine Nullstelle von f. Nach Bemerkung (2.259) ist $X - a$ ein Teiler von f, d.h. es gibt ein $q \in K[X]$ mit $f = (X-a)q$. Dann ist

$$\deg f = \deg((X-a)q) = \deg(X-a) + \deg q = 1 + \deg q,$$

also $\deg q < \deg f$. Nach Induktionsvoraussetzung gibt es $m' \in \mathbb{N}_0$, $g \in K[X]$ mit $q = (X-a)^{m'} g$ und $g(a) \neq 0$. Wir setzen $m := 1 + m'$ und erhalten

$$f = (X-a)q = (X-a)(X-a)^{m'} g = (X-a)^{1+m'} g = (X-a)^m g.$$

Für die Eindeutigkeit seien $m, m' \in \mathbb{N}_0$, $g, g' \in K[X]$ mit $f = (X-a)^m g = (X-a)^{m'} g'$ und $g(a) \neq 0$ und $g'(a) \neq 0$ gegeben. O.B.d.A. gelte $m \leq m'$. Nach Korollar (2.254) folgt $g = (X-a)^{m'-m} g'$, also

$$g(a) = (a-a)^{m'-m} g'(a) = 0^{m'-m} g'(a).$$

Wegen $g(a) \neq 0$ ist somit auch $0^{m'-m} \neq 0$, also $m' = m$. Folglich haben $(X-a)^m g = (X-a)^m g'$ und damit auch $g = g'$ nach Korollar (2.254). □

(2.263) Definition (Vielfachheit)**.** Es seien ein Körper K und ein $f \in K[X] \setminus \{0\}$ gegeben. Für $a \in K$ heißt das eindeutige $m \in \mathbb{N}_0$ mit $(X-a)^m \mid f$ und $(X-a)^{m+1} \nmid f$ die *Vielfachheit* (oder *Multiplizität*) von a als Nullstelle von f.

(2.264) Definition (algebraisch abgeschlossen)**.** Ein Körper K heißt *algebraisch abgeschlossen*, falls jedes $f \in K[X] \setminus K$ eine Nullstelle hat.

(2.265) Bemerkung. Es sei ein algebraisch abgeschlossener Körper K gegeben. Jedes $f \in K[X] \setminus K$ zerfällt in Linearfaktoren.

Beweis. Es sei $f \in K[X]$ gegeben. Wir führen Induktion nach $\deg f$.
Es sei zunächst $\deg f = 1$, so dass es $b \in K \setminus \{0\}$, $c \in K$ mit $f = bX + c$ gibt. Mit $a_1 := -b^{-1}c$ folgt

$$f = bX + c = b(X + b^{-1}c) = b(X - a).$$

Somit zerfällt f in Linearfaktoren.
Nun sei $\deg > 1$ und es sei angenommen, dass alle $f' \in K[X] \setminus K$ mit $\deg f' < \deg f$ in Linearfaktoren zerfallen. Da K algebraisch abgeschlossen ist, hat f eine Nullstelle $a_{\deg f}$. Nach Bemerkung (2.259) gilt $(X - a_{\deg f}) \mid f$, d.h. es gibt ein $q \in K[X]$ mit $f = q \cdot (X - a)$. Wegen $f \neq 0$ ist $q \neq 0$ und

$$\deg f = \deg(q \cdot (X - a)) = \deg q + \deg(X - a) = \deg q + 1$$

nach Bemerkung (2.253)(b), also $\deg q = \deg f - 1 < \deg q$. Nach Induktionsvoraussetzung zerfällt q in Linearfaktoren, d.h. es gibt $b \in K$ und $a_i \in K$ für $i \in [1, \deg q]$ mit $q = b \prod_{i \in [1, \deg q]} (X - a_i)$. Es folgt

$$\begin{aligned} f = q \cdot (X - a_{\deg f}) &= b \prod_{i \in [1, \deg q]} (X - a_i) \cdot (X - a_{\deg f}) = b \prod_{i \in [1, \deg f - 1]} (X - a_i) \cdot (X - a_{\deg f}) \\ &= b \prod_{i \in [1, \deg f]} (X - a_i). \end{aligned}$$

Somit zerfällt f ebenfalls in Linearfaktoren. □

(2.266) Satz (Fundamentalsatz der Algebra)**.** Der Körper der komplexen Zahlen $\mathbb{C}$ ist algebraisch abgeschlossen.

Ohne Beweis. □

Quotientenkörper der Polynomalgebra

In diesem Abschnitt werden wir sehen, dass wir die Polynomalgebra $K[X]$ über einem Körper K in einen Körper $K(X)$ *einbetten* können, d.h. dass wir einen Körper $K(X)$ und einen injektiven Ringhomomorphismus $K[X] \to K(X)$ konstruieren können. Um zu sehen, wie sich diese Konstruktion durchführen lässt, machen wir zunächst eine Analyse.
Es seien ein kommutatives Monoid Q und ein injektiver Monoidhomomorphismus $\iota\colon K[X] \to Q$ mit $\iota(f)$ invertierbar in Q für alle $f \in K[X] \setminus \{0\}$ gegeben. Wenn wir $K[X]$ mit $\operatorname{Im} \iota$ identifizieren, so können wir also Q als „Erweiterung“ von $K[X]$ auffassen, in welcher Inverse für alle Elemente ungleich der Null existieren und in welcher sich die üblichen Rechenregeln bzgl. der Multiplikation, wie Assoziativität und Kommutativität, fortsetzen.
Wir erhalten die Abbildung

$$F\colon K[X] \times (K[X] \setminus \{0\}) \to Q,\ (f, d) \mapsto \iota(f)\, \iota(d)^{-1}.$$

Wir wollen nun der Frage nachgehen, welche Elemente aus $K[X] \times (K[X] \setminus \{0\})$ via F auf dasselbe Element in Q abgebildet werden Es seien $(f, d), (g, e) \in K[X] \times (K[X] \setminus \{0\})$ gegeben. Nach Definition von F gilt genau dann $F(f, d) = F(g, e)$, wenn $\iota(f)\, \iota(d)^{-1} = \iota(g)\, \iota(e)^{-1}$ ist. Dies ist äquivalent zu $\iota(f)\iota(e) = \iota(g)\iota(d)$. Da ι als Homomorphismus verträglich mit den Multiplikationen ist, gilt dies wiederum genau dann, wenn $\iota(fe) = \iota(gd)$ ist, und dies ist auf Grund der Injektivität von ι äquivalent zu $fe = gd$.
Diese Analyse motiviert nun folgende Definition.

(2.267) Definition (Bruchgleichheit)**.** Es sei ein Körper K gegeben. Die Relation $\equiv$ auf $K[X] \times (K[X] \setminus \{0\})$ sei wie folgt definiert: Für $(f, d), (g, e) \in K[X] \times (K[X] \setminus \{0\})$ gelte genau dann $(f, d) \equiv (g, e)$, wenn

$$fe = gd$$

ist.
Haben wir $(f, d), (g, e) \in K[X] \times (K[X] \setminus \{0\})$ mit $(f, d) \equiv (g, e)$ gegeben, so sagen wir, dass (f, d) und (g, e) *bruchgleich* sind.

(2.268) Bemerkung. Es sei ein Körper K gegeben. Dann ist $\equiv$ eine Äquivalenzrelation auf $K[X] \times (K[X] \setminus \{0\})$.

Beweis. Es seien $(f,c),(g,d),(h,e) \in K[X] \times (K[X] \setminus \{0\})$ mit $(f,c) \equiv (g,d)$ und $(g,d) \equiv (h,e)$ gegeben. Dann gilt $fd = gc$ und $ge = hd$, also

$$fed = fde = gce = gec = hdc = hcd.$$

Nach Korollar (2.254) folgt $fe = hc$, d.h. $(f,c) \equiv (h,e)$. Folglich ist $\equiv$ transitiv.
Für $(f,d) \in K[X] \times (K[X] \setminus \{0\})$ gilt $fd = fd$, also $(f,d) \equiv (f,d)$. Folglich ist $\equiv$ reflexiv.
Für $(f,d),(g,e) \in K[X] \times (K[X] \setminus \{0\})$ mit $(f,d) \equiv (g,e)$ gilt $fe = gd$, also auch $gd = fe$ und damit $(g,e) \equiv (f,d)$. Folglich ist $\equiv$ symmetrisch.
Insgesamt ist $\equiv$ eine Äquivalenzrelation auf $K[X] \times (K[X] \setminus \{0\})$. □

(2.269) Definition (Menge der Brüche)**.** Es sei ein Körper K gegeben. Die *Menge der Brüche in* $K[X]$ ist definiert als

$$K(X) := (K[X] \times (K[X] \setminus \{0\}))/\equiv.$$

Die Äquivalenzklasse eines $(f,d) \in K[X] \times (K[X] \setminus \{0\})$ wird *Bruch* von (f,d) genannt und als

$$\frac{f}{d} := [(f,d)]_\equiv$$

notiert.

(2.270) Bemerkung. Es sei ein Körper K gegeben. Für $(f,d) \in K[X] \times (K[X] \setminus \{0\})$, $c \in \mathbb{Z} \setminus \{0\}$ gilt

$$\frac{fc}{dc} = \frac{f}{c}$$

in $K(X)$.

Beweis. Für $(f,d) \in K[X] \times (K[X] \setminus \{0\})$, $c \in \mathbb{Z} \setminus \{0\}$ gilt $fcd = fdc$, also $(fc,fc) \equiv (f,d)$ und damit $\frac{fc}{dc} = \frac{f}{d}$ in $K(X)$ nach Proposition (1.9)(b). □

Als nächstes kommen wir zu ersten Aussagen hinsichtlich der algebraischen Struktur von $K(X)$ für einen Körper K. Wir haben $K(X)$ aus der Not heraus, nicht durch beliebige Polynome ungleich 0 dividieren zu können, konstruiert. Daher sollte sich nun eine Multiplikation auf $K(X)$ ergeben, bei welcher jedes Element ungleich 0 ein Inverses besitzt.

(2.271) Satz. Es sei ein Körper K gegeben. Die Menge $K(X)$ wird ein Körper mit Addition und Multiplikation gegeben durch

$$\frac{f}{d} +^{K(X)} \frac{g}{e} = \frac{f \cdot^{K[X]} e +^{K[X]} d \cdot^{K[X]} g}{d \cdot^{K[X]} e},$$
$$\frac{f}{d} \cdot^{K(X)} \frac{g}{e} = \frac{f \cdot^{K[X]} g}{d \cdot^{K[X]} e},$$

für $(f,d),(g,e) \in K[X] \times (K[X] \setminus \{0\})$. Die Null und die Eins von $K(X)$ sind gegeben durch

$$0^{K(X)} = \frac{0^{K[X]}}{1^{K[X]}},$$
$$1^{K(X)} = \frac{1^{K[X]}}{1^{K[X]}}.$$

Für $(f,d) \in K[X] \times (K[X] \setminus \{0\})$ ist das Negative von $\frac{f}{d}$ in $K(X)$ gegeben durch

$$(-\frac{f}{d})^{K(X)} = \frac{(-f)^{K[X]}}{d}.$$

Für $(f,d) \in K[X] \times (K[X] \setminus \{0\})$ mit $\frac{f}{d} \neq 0$ in $K(X)$ ist das Inverse von $\frac{f}{d}$ gegeben durch

$$((\frac{f}{d})^{-1})^{K(X)} = \frac{d}{f}.$$

Beweis. Nach Bemerkung (2.253)(b) folgt aus $d \neq 0$ und $e \neq 0$ auch $de \neq 0$. Somit ist für $(f,d),(g,e) \in K[X] \times (K[X] \setminus \{0\})$ auch $(fg,de) \in K[X] \times (K[X] \setminus \{0\})$. Um zu zeigen, dass die beschriebene Multiplikation wohldefiniert ist, seien $(f,d),(\tilde{f},\tilde{d}),(g,e),(\tilde{g},\tilde{e}) \in K[X] \times (K[X] \setminus \{0\})$ mit $(f,d) \equiv (\tilde{f},\tilde{d})$ und $(g,e) \equiv (\tilde{g},\tilde{e})$ gegeben. Dann gilt $f\tilde{d} = \tilde{f}d$ und $g\tilde{e} = \tilde{g}e$, also auch

$$fg\tilde{d}\tilde{e} = f\tilde{d}g\tilde{e} = \tilde{f}d\tilde{g}e = \tilde{f}\tilde{g}de,$$

d.h. $(fg,de) \equiv (\tilde{f}\tilde{g},\tilde{d}\tilde{e})$.
Somit erhalten wir eine wohldefinierte Verknüpfung

$$m\colon K(X) \times K(X) \to K(X),\ (\frac{f}{d},\frac{g}{e}) \mapsto \frac{fg}{de}.$$

Wir wollen zeigen, dass $K(X)$ ein kommutatives Monoid mit Multiplikation m wird.
Für $(f,c),(g,d),(h,e) \in K[X] \times (K[X] \setminus \{0\})$ gilt

$$m(\frac{f}{c},m(\frac{g}{d},\frac{h}{e})) = m(\frac{f}{c},\frac{gh}{de}) = \frac{f(gh)}{c(de)} = \frac{(fg)h}{(cd)e} = m(\frac{fg}{cd},\frac{h}{e}) = m(m(\frac{f}{c},\frac{g}{d}),\frac{h}{e}).$$

Folglich ist m assoziativ.
Für $(f,d),(g,e) \in K[X] \times (K[X] \setminus \{0\})$ gilt

$$m(\frac{f}{d},\frac{g}{e}) = \frac{fg}{de} = \frac{gf}{ed} = m(\frac{g}{e},\frac{f}{d}).$$

Folglich ist m kommutativ.
Für $(f,d) \in K[X] \times (K[X] \setminus \{0\})$ gilt

$$m(\frac{f}{d},\frac{1}{1}) = \frac{f \cdot 1}{d \cdot 1} = \frac{f}{d}.$$

Folglich ist $\frac{1}{1}$ ein neutrales Element bzgl. m.
Insgesamt wird $K(X)$ ein kommutatives Monoid mit Multiplikation gegeben durch $\frac{f}{d} \cdot \frac{g}{e} = m(\frac{f}{d},\frac{g}{e}) = \frac{fg}{de}$ für$(f,d),(g,e) \in K[X] \times (K[X] \setminus \{0\})$ und Eins $1 = \frac{1}{1}$.
Um zu zeigen, dass die beschriebene Addition wohldefiniert ist, seien $(f,d),(\tilde{f},\tilde{d}),(y,e),(\tilde{f},\tilde{e}) \in K[X] \times (K[X] \setminus \{0\})$ mit $(f,d) \equiv (\tilde{f},\tilde{d})$ und $(g,e) \equiv (\tilde{g},\tilde{e})$ gegeben. Dann gilt $f\tilde{d} = \tilde{f}d$ und $g\tilde{e} = \tilde{g}e$, also auch

$$(fe+dg)\tilde{d}\tilde{e} = fe\tilde{d}\tilde{e} + dg\tilde{d}\tilde{e} = f\tilde{d}e\tilde{e} + d\tilde{d}g\tilde{e} = \tilde{f}de\tilde{e} + d\tilde{d}\tilde{g}e = \tilde{f}\tilde{e}de + \tilde{d}\tilde{g}de = (\tilde{f}\tilde{e}+\tilde{d}\tilde{g})de.$$

Dies impliziert aber $(fe+dg,de) \equiv (\tilde{f}\tilde{e}+\tilde{d}\tilde{g},\tilde{d}\tilde{e})$.
Somit erhalten wir eine wohldefinierte Verknüpfung

$$n\colon K(X) \times K(X) \to K(X),\ (\frac{f}{d},\frac{g}{e}) \mapsto \frac{fe+dg}{de}.$$

Wir wollen zunächst zeigen, dass $K(X)$ ein Körper mit Addition n wird.
Für $(f,c),(g,d),(h,e) \in K[X] \times (K[X] \setminus \{0\})$ gilt

$$\begin{aligned} n(\frac{f}{c},n(\frac{g}{d},\frac{h}{e})) &= n(\frac{f}{c},\frac{ge+dh}{de}) = \frac{fde+c(ge+dh)}{c(de)} = \frac{fde+cge+cdh}{cde} = \frac{(fd+cg)e+cdh}{(cd)e} \\ &= n(\frac{fd+cg}{cd},\frac{h}{e}) = n(n(\frac{f}{c},\frac{g}{d}),\frac{h}{e}). \end{aligned}$$

Folglich ist n assoziativ.
Für $(f,d),(g,e) \in K[X] \times (K[X] \setminus \{0\})$ gilt

$$n(\frac{f}{d},\frac{g}{e}) = \frac{fe+dg}{de} = \frac{gd+ef}{ed} = n(\frac{g}{e},\frac{f}{d}).$$

Folglich ist n kommutativ.

Für $(f,d) \in K[X] \times (K[X] \setminus \{0\})$ gilt

$$n(\frac{f}{d}, \frac{0}{1}) = \frac{f \cdot 1 + d \cdot 0}{d \cdot 1} = \frac{f}{d}.$$

Folglich ist $\frac{0}{1}$ ein neutrales Element bzgl. n.
Für $(f,d) \in K[X] \times (K[X] \setminus \{0\})$ gilt

$$n(\frac{f}{d}, \frac{-f}{d}) = \frac{fd + d(-f)}{dd} = \frac{0}{d^2} = \frac{0 \cdot d^2}{1 \cdot d^2} = \frac{0}{1}$$

nach Bemerkung (2.270). Folglich ist $\frac{-f}{d}$ ein inverses Element zu $\frac{f}{d}$ bzgl. n.
Für $(f,c),(g,d),(h,e) \in K[X] \times (K[X] \setminus \{0\})$ gilt

$$\begin{aligned}\frac{f}{c} \cdot n(\frac{g}{d}, \frac{h}{e}) &= \frac{f}{c} \cdot \frac{ge + dh}{de} = \frac{f(ge+dh)}{c(de)} = \frac{fge + fdh}{cde} = \frac{fge + dfh}{cde} = \frac{(fge+dfh)c}{(cde)c} = \frac{fgec + dfgc}{cdec} \\ &= \frac{fgce + cdfh}{cdce} = n(\frac{fg}{cd}, \frac{fh}{ce}) = n(\frac{f}{c} \cdot \frac{g}{d}, \frac{f}{c} \cdot \frac{h}{e}).\end{aligned}$$

Folglich gelten die Distributivgesetze.
Insgesamt wird $K(X)$ ein kommutativer Ring mit Addition gegeben durch $\frac{f}{d} + \frac{g}{e} = n(\frac{f}{d}, \frac{g}{e}) = \frac{fe+dg}{de}$ für $(f,d),(g,e) \in K[X] \times (K[X] \setminus \{0\})$, Null $0 = \frac{0}{1}$ und Negativen $-\frac{f}{d} = \frac{-f}{d}$ für $(f,d) \in K[X] \times (K[X] \setminus \{0\})$. Um zu zeigen, dass $K(X)$ ein Körper ist, bleibt es zu zeigen, dass jedes Element in $K(X) \setminus \{0\}$ invertierbar ist. Hierzu sei $(f,d) \in K[X] \times (K[X] \setminus \{0\})$ mit $\frac{f}{d} \neq 0 = \frac{0}{1}$ gegeben. Dann ist $f \cdot 1 \neq 0 \cdot d = 0$, also $f \neq 0$ und damit $f \in K[X] \setminus \{0\}$. Wir erhalten

$$\frac{f}{d} \cdot \frac{d}{f} = \frac{fd}{df} = \frac{1}{1} = 1,$$

d.h. $\frac{d}{f}$ ist ein zu $\frac{f}{d}$ inverses Element in $K(X)$. Folglich ist $K(X)$ ein Körper. □

(2.272) Konvention. Es sei ein Körper K gegeben. Ab jetzt betrachten wir $K(X)$ als Körper mit Addition und Multiplikation gegeben wie in Satz (2.271).

Nun können wir den Polynomring in der Menge der Brüche wiederfinden:

(2.273) Proposition. Es sei ein Körper K gegeben. Die Abbildung

$$\iota\colon K[X] \to K(X),\ f \mapsto \frac{f}{1}$$

ist ein injektiver Homomorphismus kommutativer Monoide.

Beweis. Für $f,g \in K[X]$ gilt

$$\begin{aligned}\iota(f+g) &= \frac{f+g}{1} = \frac{f \cdot 1 + 1 \cdot g}{1 \cdot 1} = \frac{f}{1} + \frac{g}{1} = \iota(f) + \iota(g), \\ \iota(fg) &= \frac{fg}{1} = \frac{fg}{1 \cdot 1} = \frac{f}{1} \cdot \frac{g}{1} = \iota(f)\,\iota(g).\end{aligned}$$

Ferner ist

$$\iota(1) = \frac{1}{1} = 1.$$

Insgesamt ist ι somit ein Ringhomomorphismus. Für $f,g \in K[X]$ mit $\iota(f) = \iota(g)$ in $K(X)$ gilt ferner $\frac{f}{1} = \frac{g}{1}$, also $f = f \cdot 1 = g \cdot 1 = g$ in $K[X]$. Folglich ist ι injektiv. □

(2.274) Konvention. Es sei ein Körper K gegeben. Von jetzt an identifizieren wir $K[X]$ mit dem Bild der injektiven Abbildung $\iota\colon K[X] \to K(X)$ aus Proposition (2.273). Das heißt, unter Missbrauch der Notationen schreiben wir $K[X]$ anstatt $\operatorname{Im}\iota$, und, für $f \in K[X]$, notieren wir das Bild $\iota(f) = \frac{f}{1}$ von f auch durch f.

Durch diese Konvention können wir nun eine neue Darstellung der Elemente in $K(X)$ herleiten:

(2.275) Bemerkung. Es sei ein Körper K gegeben. Für $(f,d) \in K[X] \times (K[X] \setminus \{0\})$ ist

$$\frac{f}{d} = fd^{-1}.$$

Beweis. Für $(f,d) \in K[X] \times (K[X] \setminus \{0\})$ ist

$$\frac{f}{d} = \frac{f}{1} \cdot \frac{1}{d} = \frac{f}{1} \cdot (\frac{d}{1})^{-1} = fd^{-1}.$$ □

(2.276) Bemerkung. Es sei ein Körper K gegeben.

(a) Es ist

$$K(X) = \{fg^{-1} \mid f \in K[X],\, g \in K[X] \setminus \{0\}\}.$$

(b) Für $f,g \in K[X]$, $d,e \in K[X] \setminus \{0\}$ gilt genau dann

$$fd^{-1} = ge^{-1}$$

in $K(X)$, wenn

$$fe = gd$$

in $K[X]$ gilt.

Beweis.

(a) Nach Bemerkung (2.275) gilt

$$\begin{aligned} K(X) &= (K[X] \times (K[X] \setminus \{0\}))/\equiv = \{\frac{f}{d} \mid (f,d) \in K[X] \times (K[X] \setminus \{0\})\} \\ &= \{fd^{-1} \mid (f,d) \in K[X] \times (K[X] \setminus \{0\})\}. \end{aligned}$$ □

Da die Darstellung der Elemente von $K(X)$ für einen Körper K als Brüche, d.h. als Äquivalenzklassen von Elementen aus $K[X] \times (K[X] \setminus \{0\})$ durchaus üblich ist, werden wir, trotz Bemerkung (2.275) und Bemerkung (2.276), im Folgenden dieser kürzeren Darstellung meist den Vorzug geben.

Kapitel III

Eigenwerttheorie

Die Darstellungsmatrix eines Endomorphismus $\varphi\colon V \to V$ eines endlichdimensionalen Vektorraums V ist abhängig von einer gewählten Basis $s = (s_j)_{j\in[1,n]}$ von V. Dabei sind einige Basen zum Rechnen besser geeignet als andere:
Es sei etwa $A \in \mathbb{R}^{3\times 3}$ gegeben durch

$$A = \begin{pmatrix} -1 & -5 & -3 \\ 0 & 1 & 0 \\ 0 & 1 & 2 \end{pmatrix}.$$

Dann ist die Darstellungsmatrix der Standardinterpretation $\varphi_A\colon \mathbb{R}^{3\times 1} \to \mathbb{R}^{3\times 1}$, $x \mapsto Ax$ bzgl. der Standardbasis $\mathrm{e} = (\mathrm{e}_1, \mathrm{e}_2, \mathrm{e}_3)$ von $\mathbb{R}^{3\times 1}$ gegeben durch

$$\mathrm{M}^{\mathrm{e}}_{\mathrm{e}}(\varphi_A) = A = \begin{pmatrix} -1 & -5 & -3 \\ 0 & 1 & 0 \\ 0 & 1 & 2 \end{pmatrix}.$$

Für die Matrix $s = (s_1, s_2, s_3)$ von $\mathbb{R}^{3\times 1}$ gegeben durch

$$s = (\begin{pmatrix} -1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ -1 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix})$$

gilt hingegen

$$\mathrm{M}^s_s(\varphi_A) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

Für einige Zwecke sind die Darstellungsmatrix $\mathrm{M}^s_s(\varphi_A)$ und die Basis s besser geeignet als die Ausgangsmatrix A und die Standardbasis e. So können wir etwa mit Hilfe der Basis s leicht Potenzen von (der Darstellungsmatrix von) φ_A berechnen:

$$\mathrm{M}^s_s(\varphi^3_A) = (\mathrm{M}^s_s(\varphi_A))^3 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}^3 = \begin{pmatrix} (-1)^3 & 0 & 0 \\ 0 & 1^3 & 0 \\ 0 & 0 & 2^3 \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 8 \end{pmatrix}.$$

Wenn wir mit Hilfe der Standardbasis e arbeiten wollen, so haben wir hingegen die Rechnung

$$\begin{aligned} \mathrm{M}^{\mathrm{e}}_{\mathrm{e}}(\varphi^3_A) = (\mathrm{M}^{\mathrm{e}}_{\mathrm{e}}(\varphi_A))^3 &= \begin{pmatrix} -1 & -5 & -3 \\ 0 & 1 & 0 \\ 0 & 1 & 2 \end{pmatrix}^3 = \begin{pmatrix} -1 & -5 & -3 \\ 0 & 1 & 0 \\ 0 & 1 & 2 \end{pmatrix} \begin{pmatrix} -1 & -5 & -3 \\ 0 & 1 & 0 \\ 0 & 1 & 2 \end{pmatrix} \begin{pmatrix} -1 & -5 & -3 \\ 0 & 1 & 0 \\ 0 & 1 & 2 \end{pmatrix} \\ &= \begin{pmatrix} -1 & -5 & -3 \\ 0 & 1 & 0 \\ 0 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & -3 & -3 \\ 0 & 1 & 0 \\ 0 & 3 & 4 \end{pmatrix} = \begin{pmatrix} -1 & -11 & -9 \\ 0 & 1 & 0 \\ 0 & 7 & 8 \end{pmatrix} \end{aligned}$$

durchzuführen.
Unser Bestreben ist es, nach Basen zu suchen, bzgl. derer die Darstellungsmatrix eines Endomorphismus eine besonders „schöne“, d.h. für das Rechnen praktische, Gestalt hat. Die „schönste“ vorstellbare Form ist dabei eine Diagonalmatrix wie in unserem Beispiel gerade. Leider gibt es nicht immer eine Basis so, dass wir diese Gestalt erreichen können. Wir werden Kriterien für die Existenz einer solchen Basis herleiten, siehe Korollar (3.39) und Satz (3.40).

1 Eigenwerte und Eigenvektoren

Es seien $n \in \mathbb{N}$, ein Körper K, ein n-dimensionaler K-Vektorraum V und ein K-Vektorraumendomorphismus $\varphi\colon V \to V$ gegeben. Wenn es eine Basis $s = (s_j)_{j\in[1,n]}$ von V so gibt, dass

$$\mathrm{M}_s^s(\varphi) = \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix}$$

für gewisse $a_j \in K$ für $j \in [1,n]$ ist, so bedeutet dies gerade, dass

$$\varphi(s_j) = a_j s_j$$

für $j \in [1,n]$ gelten muss. Dies führt auf die Begriffe Eigenwert und Eigenvektor, welche wir in diesem Abschnitt einführen wollen.

Definition und Beispiele

(3.1) Definition (Eigenwert, Eigenvektor)**.** Es sei ein Körper K gegeben.

(a) Es seien ein K-Vektorraum V und ein K-Vektorraumendomorphismus $\varphi\colon V \to V$ gegeben. Ein *Eigenwert* von φ ist ein $a \in K$ derart, dass es ein $v \in V$ mit $v \neq 0$ und

$$\varphi(v) = av$$

gibt. Ein solches $v \in V$ heißt dann auch *Eigenvektor* von φ zum Eigenwert a.

(b) Es seien $n \in \mathbb{N}_0$ und $A \in K^{n\times n}$ gegeben. Ein *Eigenwert* von A ist ein *Eigenwert* von φ_A. Ein *Eigenvektor* von A ist ein Eigenvektor von φ_A.

Wir betonen, dass per Definition der Nullvektor kein Eigenvektor eines Vektorraumendomorphismus $\varphi\colon V \to V$ ist. Für alle $a \in K$ gilt dennoch $\varphi(0) = a0$.

(3.2) Bemerkung. Es seien $n \in \mathbb{N}_0$, ein Körper K, ein $A \in K^{n\times n}$ und ein $a \in K$ gegeben. Genau dann ist a ein Eigenwert von A, wenn es ein $x \in K^{n\times 1}$ mit $x \neq 0$ und $Ax = ax$ gibt.

(3.3) Beispiel. Es seien $A \in \mathbb{Q}^{2\times 2}$, $x, y \in \mathbb{Q}^{2\times 1}$ gegeben durch

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix},\ x = \begin{pmatrix} 1 \\ -1 \end{pmatrix},\ y = \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Dann ist x ein Eigenvektor von A zum Eigenwert 1 und y ein Eigenvektor von A zum Eigenwert 3.

Beweis. Wir haben

$$Ax = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \end{pmatrix} = x,$$
$$Ay = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ 3 \end{pmatrix} = 3\begin{pmatrix} 1 \\ 1 \end{pmatrix} = 3y.$$

□

Eigenräume

(3.4) Notation. Es seien ein Körper K und $a \in K$ gegeben.

(a) Es seien ein K-Vektorraum V und ein K-Vektorraumendomorphismus $\varphi\colon V \to V$ gegeben. Wir setzen

$$\mathrm{Eig}_\varphi(a) := \{v \in V \mid \varphi(v) = av\}.$$

(b) Es seien $n \in \mathbb{N}_0$ und ein $A \in K^{n\times n}$ gegeben. Wir setzen

$$\mathrm{Eig}_A(a) := \mathrm{Eig}_{\varphi_A}(a).$$

(3.5) Bemerkung. Es seien $n \in \mathbb{N}_0$, ein Körper K und ein $A \in K^{n\times n}$ gegeben. Für $a \in K$ ist

$$\mathrm{Eig}_A(a) = \{x \in K^{n\times 1} \mid Ax = ax\}.$$

Beweis. Für $a \in K$ ist

$$\mathrm{Eig}_A(a) = \mathrm{Eig}_{\varphi_A}(a) = \{x \in K^{n\times 1} \mid \varphi_A(x) = ax\} = \{x \in K^{n\times 1} \mid Ax = ax\}. \qquad \square$$

(3.6) Bemerkung. Es seien ein Körper K, ein K-Vektorraum V und ein K-Vektorraumendomorphismus $\varphi\colon V \to V$ gegeben. Für $a \in K$ ist

$$\mathrm{Eig}_\varphi(a) = \mathrm{Ker}(\varphi - a\,\mathrm{id}_V).$$

Insbesondere ist $\mathrm{Eig}_\varphi(a)$ ein K-Untervektorraum von V.

Beweis. Für $a \in K$ ist

$$\begin{aligned}\mathrm{Eig}_\varphi(a) &= \{v \in V \mid \varphi(v) = av\} = \{v \in V \mid \varphi(v) - av = 0\} = \{v \in V \mid \varphi(v) - a\,\mathrm{id}_V(v) = 0\}\\ &= \{v \in V \mid (\varphi - a\,\mathrm{id}_V)(v) = 0\} = \mathrm{Ker}(\varphi - a\,\mathrm{id}_V).\end{aligned}$$ $\square$

(3.7) Definition (Eigenraum)**.** Es sei ein Körper K gegeben.

(a) Es seien ein K-Vektorraum V, ein K-Vektorraumendomorphismus $\varphi\colon V \to V$ und ein Eigenwert a von φ gegeben. Der K-Untervektorraum $\mathrm{Eig}_\varphi(a)$ von V aus Bemerkung (3.6) heißt *Eigenraum* von φ zum Eigenwert a.

(b) Es seien $n \in \mathbb{N}_0$, $A \in K^{n\times n}$ und ein Eigenwert a von A gegeben. Der K-Untervektorraum $\mathrm{Eig}_A(a)$ von $K^{n\times 1}$ heißt *Eigenraum* von A zum Eigenwert a.

(3.8) Bemerkung. Es seien ein Körper K, ein K-Vektorraum V, ein K-Vektorraumendomorphismus $\varphi\colon V \to V$ und ein $a \in K$ gegeben. Genau dann ist a ein Eigenwert von φ, wenn

$$\mathrm{Eig}_\varphi(a) \neq \{0\}$$

ist. In diesem Fall ist $\mathrm{Eig}_\varphi(a) \setminus \{0\}$ gerade die Menge aller Eigenvektoren von φ zum Eigenwert a.

(3.9) Proposition. Es seien ein Körper K, ein endlichdimensionaler K-Vektorraum V, eine parametrisierte Basis $s = (s_j)_{j\in[1,n]}$ von V, ein K-Vektorraumendomorphismus $\varphi\colon V \to V$ und ein $a \in K$ gegeben. Dann ist

$$\kappa_s(\mathrm{Eig}_\varphi(a)) = \mathrm{Eig}_{\mathrm{M}_s^s(\varphi)}(a).$$

Insbesondere ist a genau dann ein Eigenwert von φ, wenn a ein Eigenwert von $\mathrm{M}_s^s(\varphi)$ ist, und ein $v \in V$ ist genau dann ein Eigenvektor von φ zum Eigenwert a, wenn $\kappa_s(v)$ ein Eigenvektor von $\mathrm{M}_s^s(\varphi)$ zum Eigenwert a ist.

Beweis. Es ist

$$\begin{aligned}\kappa_s(\mathrm{Eig}_\varphi(a)) &= \{\kappa_s(v) \mid v \in \mathrm{Eig}_\varphi(a)\} = \{\kappa_s(v) \mid v \in V \text{ mit } \varphi(v) = av\}\\ &= \{\kappa_s(v) \mid v \in V \text{ mit } \kappa_s(\varphi(v)) = \kappa_s(av)\} = \{\kappa_s(v) \mid v \in V \text{ mit } \mathrm{M}_s^s(\varphi)\,\kappa_s(v) = a\kappa_s(v)\}\\ &= \{x \in K^{n\times 1} \mid \mathrm{M}_s^s(\varphi)x = ax\} = \mathrm{Eig}_{\mathrm{M}_s^s(\varphi)}(a).\end{aligned}$$ $\square$

Berechnung von Eigenwerten und Eigenräumen

(3.10) Proposition. Es seien ein Körper K, ein endlichdimensionaler K-Vektorraum V, ein K-Vektorraumendomorphismus $\varphi\colon V \to V$ und ein $a \in K$ gegeben. Die folgenden Bedingungen sind äquivalent:

(a) Es ist a ein Eigenwert von φ.

(b) Es ist $\operatorname{Ker}(\varphi - a\operatorname{id}_V) \neq \{0\}$.

(c) Es ist $\dim \operatorname{Im}(\varphi - a\operatorname{id}_V) < n$.

(d) Es ist $\det(\varphi - a\operatorname{id}_V) = 0$.

Gelten die äquivalenten Bedingungen, so ist $\operatorname{Ker}(\varphi - a\operatorname{id}_V) \setminus \{0\}$ die Menge aller Eigenvektoren von φ zum Eigenwert a.

Beweis. Nach Bemerkung (3.8) und Bemerkung (3.6) ist a genau dann ein Eigenwert von φ, wenn

$$\operatorname{Ker}(\varphi - a\operatorname{id}_V) = \operatorname{Eig}_\varphi(a) \neq \{0\}$$

ist. Folglich sind Bedingung (a) und Bedingung (b) äquivalent.
Die Äquivalenz von Bedingung (b) und Bedingung (c) gilt wegen

$$n = \dim V = \dim \operatorname{Ker}(\varphi - a\operatorname{id}_V) + \dim \operatorname{Im}(\varphi - a\operatorname{id}_V).$$

Die Äquivalenz von Bedingung (c) und Bedingung (d) gilt nach Bemerkung (2.196) und Korollar (2.222), da für jede parametrisierte Basis $s = (s_j)_{j\in[1,\dim V]}$ von V stets

$$\mathrm{M}_s^s(\varphi - a\operatorname{id}_V) = \mathrm{M}_s^s(\varphi) - a\mathrm{M}_s^s(\operatorname{id}_V) = \mathrm{M}_s^s(\varphi) - a\mathrm{E}_n$$

ist und damit $\dim \operatorname{Im}(\varphi - a\operatorname{id}_V) = \operatorname{rk}(\mathrm{M}_s^s(\varphi) - a\mathrm{E}_n)$ sowie $\det(\varphi - a\operatorname{id}_V) = \det(\mathrm{M}_s^s(\varphi) - a\mathrm{E}_n)$ gilt. □

Die Äquivalenz der ersten und der letzten Aussage aus Proposition (3.10) übersetzt sich für Matrizen wie folgt: Es seien $n \in \mathbb{N}$, ein Körper K, ein $A \in K^{n\times n}$ und ein $a \in K$ gegeben. Genau dann ist a ein Eigenwert von A, wenn $\det(A - a\mathrm{E}_n) = 0$ ist. Der Eigenraum von A zum Eigenwert a ist dann durch $\operatorname{Ker}(\varphi_A - a\operatorname{id}_{K^{n\times 1}}) = \operatorname{Sol}_0(A - a\mathrm{E}_n)$ gegeben, die Menge aller Eigenvektoren von A zum Eigenwert a durch $\operatorname{Sol}_0(A - a\mathrm{E}_n) \setminus \{0\}$.

(3.11) Beispiel. Es sei $A \in \mathbb{Q}^{2\times 2}$ gegeben durch

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

Dann sind die Eigenwerte von A gerade 1 und 3 und es gilt

$$\operatorname{Eig}_A(1) = \langle \begin{pmatrix} 1 \\ -1 \end{pmatrix} \rangle \text{ und } \operatorname{Eig}_A(3) = \langle \begin{pmatrix} 1 \\ 1 \end{pmatrix} \rangle.$$

Beweis. Nach Proposition (3.10) ist $a \in K$ genau dann ein Eigenwert von A, wenn

$$0 = \det(A - a\mathrm{E}_2) = \det(\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} - a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}) = \det\begin{pmatrix} 2-a & 1 \\ 1 & 2-a \end{pmatrix} = (2-a)^2 - 1^2 = a^2 - 4a + 3$$
$$= (a-1)(a-3)$$

ist. Folglich sind die Eigenwerte von A gerade 1 und 3. Weiter gilt

$$\operatorname{Eig}_A(1) = \operatorname{Ker}\varphi_{A-\mathrm{E}_2} = \operatorname{Sol}_0(A - \mathrm{E}_2) = \operatorname{Sol}_0(\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}) = \operatorname{Sol}_0(\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}) = \langle \begin{pmatrix} 1 \\ -1 \end{pmatrix} \rangle,$$
$$\operatorname{Eig}_A(3) = \operatorname{Ker}\varphi_{A-3\mathrm{E}_2} = \operatorname{Sol}_0(A - 3\,\mathrm{E}_2) = \operatorname{Sol}_0(\begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix}) = \operatorname{Sol}_0(\begin{pmatrix} 1 & -1 \\ 0 & 0 \end{pmatrix}) = \langle \begin{pmatrix} 1 \\ 1 \end{pmatrix} \rangle.$$ □

Eigenschaften von Eigenvektoren

(3.12) Proposition. Es seien $m \in \mathbb{N}_0$, ein Körper K, ein endlichdimensionaler K-Vektorraum V, ein K-Vektorraumendomorphismus $\varphi\colon V \to V$, verschiedene Eigenwerte a_j von φ für $j \in [1,m]$ und ein m-Tupel $s = (s_j)_{j\in[1,m]}$ in V so gegeben, dass s_j für $j \in [1,m]$ ein Eigenvektor von φ zum Eigenwert a_j ist. Dann ist s linear unabhängig.

Beweis. Wir führen Induktion nach m, wobei für $m = 0$ nichts zu zeigen ist. Es sei also $m \in \mathbb{N}$ gegeben und es sei $(s_j)_{j\in[1,m-1]}$ linear unabhängig. Um zu zeigen, dass s linear unabhängig ist, seien $b_j \in K$ für $j \in [1,m]$ mit $\sum_{j\in[1,m]} b_j s_j = 0$ gegeben. Dann gilt

$$\begin{aligned}0 &= (\varphi - a_m\mathrm{id}_V)(0) = (\varphi - a_m\mathrm{id}_V)(\sum_{j\in[1,m]} b_j s_j) = \sum_{j\in[1,m]} b_j(\varphi - a_m\mathrm{id}_V)(s_j)\\ &= \sum_{j\in[1,m]} b_j(\varphi(s_j) - a_m\mathrm{id}_V(s_j)) = \sum_{j\in[1,m]} b_j(a_j s_j - a_m s_j) = \sum_{j\in[1,m]} b_j(a_j - a_m)s_j\\ &= \sum_{j\in[1,m-1]} b_j(a_j - a_m)s_j.\end{aligned}$$

Nach Induktionsvoraussetzung ist $(s_j)_{j\in[1,m-1]}$ linear unabhängig, also $b_j(a_j - a_m) = 0$ für $j \in [1, m-1]$. Da $a_j \neq a_m$ für $j \in [1, m-1]$ gilt, folgt $b_j = 0$ für $j \in [1, m-1]$. Dann ist aber $b_m s_m = 0$, wegen $s_m \neq 0$ also auch $b_m = 0$. Folglich ist s linear unabhängig. □

Geometrische Vielfachheit

(3.13) Definition (geometrische Vielfachheit)**.** Es seien ein Körper K und ein $a \in K$ gegeben.

(a) Es seien ein endlichdimensionaler K-Vektorraum V und ein K-Vektorraumendomorphismus $\varphi\colon V \to V$ gegeben. Die *geometrische Vielfachheit* (oder *geometrische Multiplizität*) von a als Eigenwert von φ ist definiert als

$$\dim_K \mathrm{Eig}_\varphi(a).$$

(b) Es seien $n \in \mathbb{N}_0$ und $A \in K^{n\times n}$ gegeben. Die *geometrische Vielfachheit* (oder *geometrische Multiplizität*) von a als Eigenwert von A ist definiert als die geometrische Vielfachheit von a bzgl. φ_A.

(3.14) Beispiel. Es sei $A \in \mathbb{Q}^{2\times 2}$ gegeben durch

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

Die geometrische Vielfachheit von 1 und 3 ist 1.

Beweis. Dies folgt aus Beispiel (3.11). □

(3.15) Bemerkung. Es seien $n \in \mathbb{N}_0$, ein Körper K, ein $A \in K^{n\times n}$ und ein $a \in K$ gegeben. Die geometrische Vielfachheit von a als Eigenwert von A ist durch $\dim_K \mathrm{Eig}_A(a)$ gegeben.

Beweis. Es ist $\dim \mathrm{Eig}_{\varphi_A}(a) = \dim \mathrm{Eig}_A(a)$. □

(3.16) Bemerkung. Es seien ein Körper K, ein endlichdimensionaler K-Vektorraum V, eine parametrisierte Basis $s = (s_j)_{j\in[1,n]}$ von V, ein K-Vektorraumendomorphismus $\varphi\colon V \to V$ und ein $a \in K$ gegeben. Die geometrische Vielfachheit von a als Eigenwert von φ ist die geometrische Vielfachheit von a als Eigenwert von $\mathrm{M}_s^s(\varphi)$.

Beweis. Nach Proposition (3.9) ist

$$\kappa_s(\mathrm{Eig}_\varphi(a)) = \mathrm{Eig}_{\mathrm{M}_s^s(\varphi)}(a).$$

Da $\kappa_s\colon V \to K^{n\times 1}$ und damit auch

$$\kappa_s|^{\mathrm{Eig}_{\mathrm{M}_s^s(\varphi)}(a)}_{\mathrm{Eig}_\varphi(a)}\colon \mathrm{Eig}_\varphi(a) \to \mathrm{Eig}_{\mathrm{M}_s^s(\varphi)}(a)$$

ein Isomorphismus ist, gilt nach Satz (2.137) insbesondere

$$\dim \mathrm{Eig}_\varphi(a) = \dim \mathrm{Eig}_{\mathrm{M}_s^s(\varphi)}(a).$$ □

Aufgaben

Aufgabe 96 (Eigenwerte und Polynome)**.** Es seien ein Körper K, ein endlichdimensionaler K-Vektorraum V, ein K-Vektorraumendomorphismus $\varphi\colon V \to V$, ein Eigenwert a von φ und ein $f \in K[X]$ gegeben. Zeigen Sie, dass $f(a)$ ein Eigenwert von $f(\varphi)$ ist.

Aufgabe 97 (Eigenwerte und Invertierbarkeit)**.** Es seien $n \in \mathbb{N}$, ein Körper K und ein $A \in K^{n\times n}$ gegeben.

(a) Zeigen Sie, dass A genau dann invertierbar ist, wenn 0 kein Eigenwert von A ist.

(b) Es sei A invertierbar und es sei ein Eigenwert a von A gegeben. Zeigen Sie, dass a^{-1} ein Eigenwert von A^{-1} ist.

(c) Es seien $x \in K^{n\times 1}$ und $a \in K$ gegeben und es sei a kein Eigenwert von A. Zeigen Sie, dass x genau dann ein Eigenvektor von A ist, wenn x ein Eigenvektor von $(A - a\mathrm{E}_n)^{-1}$ ist.

Aufgabe 98 (Eigenräume)**.** Es sei $A \in \mathbb{F}_7^{4\times 4}$ gegeben durch

$$A = \begin{pmatrix} 2 & 3 & 2 & 2 \\ 3 & 2 & 3 & 3 \\ 0 & -3 & -3 & 1 \\ 3 & 0 & -2 & 1 \end{pmatrix}.$$

Bestimmen Sie die Eigenwerte und Eigenräume von A.

2 Charakteristisches Polynom

Definition des charakteristischen Polynoms

Es seien $n \in \mathbb{N}$, ein Körper K, ein $A \in K^{n\times n}$ und ein $a \in K$ gegeben. Nach Proposition (3.10) ist a genau dann ein Eigenwert von A, wenn $\det(A - a\mathrm{E}_n) = 0$ ist. Da dies genau dann gilt, wenn $\det(a\mathrm{E}_n - A) = 0$ ist, motiviert dies folgende Definition:

(3.17) Definition (charakteristische Matrix, charakteristisches Polynom)**.** Es seien ein $n \in \mathbb{N}$, ein Körper K und ein $A \in K^{n\times n}$ gegeben.

(a) Die Matrix $X\mathrm{E}_n - A$ mit Einträgen in $K[X]$ heißt *charakteristische Matrix* von A.

(b) Das *charakteristische Polynom* von A ist definiert als

$$\chi_A := \det(X\mathrm{E}_n - A).$$

Da wir Determinanten nur über Körpern definiert haben, haben wir an dieser Stelle benutzt, dass sich der Polynomring $K[X]$ über einem Körper K in einen Körper $K(X)$ einbetten lässt. Aus der Leibniz-Formel (2.211) folgt, dass das charakteristische Polynom χ_A ein Element von $K[X]$, d.h. ein Polynom über K, ist.

(3.18) Beispiel. Es sei $A \in \mathbb{Q}^{2\times 2}$ gegeben durch

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

Das charakteristische Polynom von A ist

$$\chi_A = X^2 - 4X + 3 = (X - 1)(X - 3).$$

Beweis. Es ist

$$\begin{aligned}\chi_A &= \det(X\mathrm{E}_2 - A) = \det(X\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}) = \det\begin{pmatrix} X-2 & -1 \\ -1 & X-2 \end{pmatrix} = (X-2)^2 - (-1)^2 \\ &= X^2 - 4X + 3 = (X-1)(X-3).\end{aligned}$$

□

(3.19) Proposition. Es seien $n \in \mathbb{N}$, ein Körper K und ein $A \in K^{n\times n}$ gegeben. Das charakteristische Polynom χ_A ist normiert und vom Grad n.

Beweis. Nach der Leibniz-Formel (2.211) ist

$$\begin{aligned}\chi_A = \det(X\mathrm{E}_n - A) &= \sum_{\pi\in \mathrm{S}_n} (\operatorname{sgn}\pi) \prod_{j\in[1,n]} (X\mathrm{E}_n - A)_{\pi(j),j} = \sum_{\pi\in \mathrm{S}_n} (\operatorname{sgn}\pi) \prod_{j\in[1,n]} (\delta_{\pi(j),j}X - A_{\pi(j),j}) \\ &= \prod_{j\in[1,n]} (X - A_{j,j}) + \sum_{\substack{\pi\in \mathrm{S}_n \\ \pi\neq \mathrm{id}_{[1,n]}}} (\operatorname{sgn}\pi) \prod_{j\in[1,n]} (\delta_{\pi(j),j}X - A_{\pi(j),j}).\end{aligned}$$

Für $\pi \in \mathrm{S}_n$ mit $\pi \neq \mathrm{id}_{[1,n]}$ gibt es jedoch $i, j \in [1, n]$ mit $\pi(i) \neq i$ und $\pi(j) \neq j$. Folglich ist entweder $\sum_{\substack{\pi\in \mathrm{S}_n \\ \pi\neq \mathrm{id}_{[1,n]}}} (\operatorname{sgn}\pi) \prod_{j\in[1,n]}(\delta_{\pi(j),j}X - A_{\pi(j),j}) = 0$ oder $\deg(\sum_{\substack{\pi\in \mathrm{S}_n \\ \pi\neq \mathrm{id}_{[1,n]}}} (\operatorname{sgn}\pi) \prod_{j\in[1,n]}(\delta_{\pi(j),j}X - A_{\pi(j),j})) \leq n-2$. Da jedoch $\prod_{j\in[1,n]}(X - A_{j,j})$ ein normiertes Polynom vom Grad n ist, gilt dies somit auch für χ_A. □

Das charakteristische Polynom eines Endomorphismus

(3.20) Bemerkung. Es seien $n \in \mathbb{N}$, ein Körper K und $A, B \in K^{n\times n}$ gegeben. Wenn A ähnlich zu B ist, dann gilt

$$\chi_A = \chi_B.$$

Beweis. Es sei A ähnlich zu B, so dass es ein $P \in \mathrm{GL}_n(K)$ mit $P^{-1}AP = B$ gibt. Nach Bemerkung (2.229) gilt

$$\chi_B = \det(X\mathrm{E}_n - B) = \det(P^{-1}X\mathrm{E}_nP - P^{-1}AP) = \det(P^{-1}(X\mathrm{E}_n - A)P) = \det(X\mathrm{E}_n - A) = \chi_A. \qquad \square$$

(3.21) Korollar. Es seien ein Körper K, ein endlichdimensionaler K-Vektorraum $V \neq \{0\}$ und ein K-Vektorraumendomorphismus $\varphi\colon V \to V$ gegeben. Für parametrisierte Basen $s = (s_j)_{j\in[1,\dim V]}$ und $s' = (s'_j)_{j\in[1,\dim V]}$ von V gilt

$$\chi_{\mathrm{M}_s^s(\varphi)} = \chi_{\mathrm{M}_{s'}^{s'}(\varphi)}.$$

(3.22) Definition (charakteristisches Polynom)**.** Es seien ein Körper K, ein endlichdimensionaler K-Vektorraum $V \neq \{0\}$ und ein K-Vektorraumendomorphismus $\varphi\colon V \to V$ gegeben. Das *charakteristische Polynom* von φ ist definiert als

$$\chi_\varphi := \chi_{\mathrm{M}_s^s(\varphi)}$$

für eine beliebige Basis s von V.

(3.23) Bemerkung. Es seien $n \in \mathbb{N}$, ein Körper K und ein $A \in K^{n\times n}$ gegeben. Dann ist

$$\chi_A = \chi_{\varphi_A}.$$

Beweis. Es ist

$$\chi_A = \chi_{\mathrm{M}_\mathrm{e}^\mathrm{e}(\varphi_A)} = \chi_{\varphi_A}. \qquad \square$$

Berechnung von Eigenwerten

(3.24) Bemerkung. Es seien $n \in \mathbb{N}$, ein Körper K und ein $A \in K^{n\times n}$ gegeben. Für $a \in K$ ist

$$\chi_A(a) = \det(a\mathrm{E}_n - A).$$

Beweis. Es ist

$$\begin{aligned}\chi_A(a) = \operatorname{ev}_a(\chi_A) = \operatorname{ev}_a(\chi_A) = \operatorname{ev}_a(\det(X\mathrm{E}_n - A)) &= \operatorname{ev}_a\Big(\sum_{\pi\in \mathrm{S}_n} (\operatorname{sgn}\pi) \prod_{j\in[1,n]} (X\mathrm{E}_n - A)_{\pi(j),j}\Big) \\ = \operatorname{ev}_a\Big(\sum_{\pi\in \mathrm{S}_n} (\operatorname{sgn}\pi) \prod_{j\in[1,n]} (\delta_{\pi(j),j}X - A_{\pi(j),j})\Big) &= \sum_{\pi\in \mathrm{S}_n} (\operatorname{sgn}\pi) \prod_{j\in[1,n]} (\delta_{\pi(j),j}a - A_{\pi(j),j}) \\ = \sum_{\pi\in \mathrm{S}_n} (\operatorname{sgn}\pi) \prod_{j\in[1,n]} (a\mathrm{E}_n - A)_{\pi(j),j} &= \det(a\mathrm{E}_n - A). \qquad \square\end{aligned}$$

(3.25) Korollar. Es seien ein Körper K, ein endlichdimensionaler K-Vektorraum $V \neq \{0\}$ und ein K-Vektorraumendomorphismus $\varphi\colon V \to V$ gegeben. Die Eigenwerte von φ sind genau die Nullstellen von χ_φ.

Beweis. Es sei $a \in K$ gegeben. Ferner sei $s = (s_j)_{[1,\dim V]}$ eine beliebige Basis von V. Nach Bemerkung (3.24) gilt dann

$$\begin{aligned}\chi_\varphi(a) &= \chi_{\mathrm{M}_s^s(\varphi)}(a) = \det(a\mathrm{E}_n - \mathrm{M}_s^s(\varphi)) = \det(a\mathrm{M}_s^s(\mathrm{id}_V) - \mathrm{M}_s^s(\varphi)) = \det(\mathrm{M}_s^s(a\,\mathrm{id}_V - \varphi))\\ &= \det(a\,\mathrm{id}_V - \varphi) = (-1)^{\dim V}\det(\varphi - a\,\mathrm{id}_V).\end{aligned}$$

Nun ist a nach Proposition (3.10) genau dann ein Eigenwert von φ, wenn $\det(\varphi - a\,\mathrm{id}_V) = 0$ ist, was wegen $\chi_\varphi(a) = (-1)^{\dim V}\det(\varphi - a\,\mathrm{id}_V)$ aber dazu äquivalent ist, dass a eine Nullstelle von χ_φ ist. □

Algebraische Vielfachheit

(3.26) Definition (algebraische Vielfachheit)**.** Es seien ein Körper K und ein $a \in K$ gegeben.

(a) Es seien ein endlichdimensionaler K-Vektorraum $V \neq \{0\}$ und ein K-Vektorraumendomorphismus $\varphi\colon V \to V$ gegeben. Die *algebraische Vielfachheit* (oder *algebraische Multiplizität*) von a als Eigenwert von φ ist definiert als die Vielfachheit von a als Nullstelle von χ_φ.

(b) Es seien $n \in \mathbb{N}$ und $A \in K^{n\times n}$ gegeben. Die *algebraische Vielfachheit* (oder *algebraische Multiplizität*) von a als Eigenwert von A ist definiert als die algebraische Vielfachheit von a bzgl. φ_A.

(3.27) Beispiel. Es sei $A \in \mathbb{Q}^{2\times 2}$ gegeben durch

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

Die algebraische Vielfachheit von 1 und 3 ist 1.

Beweis. Dies folgt aus Beispiel (3.18). □

(3.28) Bemerkung. Es seien $n \in \mathbb{N}$, ein Körper K, ein $A \in K^{n\times n}$ und ein $a \in K$ gegeben. Die algebraische Vielfachheit von a als Eigenwert von A ist die Vielfachheit von a als Nullstelle von χ_A.

(3.29) Bemerkung. Es seien ein Körper K, ein endlichdimensionaler K-Vektorraum $V \neq \{0\}$, eine parametrisierte Basis $s = (s_j)_{j\in[1,n]}$ von V, ein K-Vektorraumendomorphismus $\varphi\colon V \to V$ und ein $a \in K$ gegeben. Die algebraische Vielfachheit von a als Eigenwert von φ ist die algebraische Vielfachheit von a als Eigenwert von $\mathrm{M}_s^s(\varphi)$.

Beweis. Es ist $\chi_\varphi = \chi_{\mathrm{M}_s^s(\varphi)}$. □

(3.30) Bemerkung. Es seien ein Körper K, ein endlichdimensionaler K-Vektorraum $V \neq \{0\}$ und ein K-Vektorraumendomorphismus $\varphi\colon V \to V$ gegeben. Die Summe der algebraischen Vielfachheiten der Elemente aus K ist kleiner oder gleich $\dim V$.

Beweis. Nach Proposition (3.19) ist $\deg\chi_\varphi = \dim V$ und nach Korollar (2.260) hat χ_φ inklusive Multiplizitäten höchstens $\deg\chi = \dim V$ Nullstellen. Die Nullstellen von χ_φ sind nach Korollar (3.25) aber gerade die Eigenwerte von φ und die Multiplizitäten die algebraischen Vielfachheiten, so dass die Summe der algebraischen Vielfachheiten durch $\dim V$ beschränkt ist. □

(3.31) Proposition. Es seien ein Körper K, ein endlichdimensionaler K-Vektorraum $V \neq \{0\}$ und ein K-Vektorraumendomorphismus $\varphi\colon V \to V$ gegeben. Für alle $a \in K$ ist die geometrische Vielfachheit von a als Eigenwert von φ immer kleiner oder gleich der algebraischen Vielfachheit von a als Eigenwert von φ.

Beweis. Es sei a in K gegeben. Ferner bezeichne γ die geometrische Vielfachheit von a als Eigenwert von φ, so dass $\dim\mathrm{Eig}_\varphi(a) = \gamma$ gilt. Nach Proposition (2.139) und Korollar (2.124) gibt es eine Basis $s = (s_j)_{j\in[1,\dim V]}$ derart, dass $(s_j)_{j\in[1,\gamma]}$ eine Basis von $\mathrm{Eig}_\varphi(a)$ ist. Folglich ist

$$\mathrm{M}_s^s(\varphi) = \begin{pmatrix} a\mathrm{E}_\gamma & B \\ 0 & C \end{pmatrix}$$

für gewisse $B \in K^{\gamma\times(\dim V-\gamma)}$, $C \in K^{(\dim V-\gamma)\times(\dim V-\gamma)}$. Nach Proposition (2.224) erhalten wir

$$\begin{aligned}\chi_\varphi = \chi_{\mathrm{M}_s^s(\varphi)} &= \det(X\mathrm{E}_{\dim V} - \mathrm{M}_s^s(\varphi)) = \det(X\begin{pmatrix}\mathrm{E}_\gamma & 0\\ 0 & \mathrm{E}_{\dim V-\gamma}\end{pmatrix} - \begin{pmatrix}a\mathrm{E}_\gamma & B\\ 0 & C\end{pmatrix})\\ &= \det(\begin{pmatrix}(X-a)\mathrm{E}_\gamma & -B\\ 0 & X\mathrm{E}_{\dim V-\gamma} - C\end{pmatrix}) = \det((X-a)\mathrm{E}_\gamma)\det(X\mathrm{E}_{\dim V-\gamma} - C) = (X-a)^\gamma\,\chi_C.\end{aligned}$$

Folglich ist die Vielfachheit von a als Nullstelle von χ_φ, d.h. die algebraische Vielfachheit von a als Eigenwert von φ, größer oder gleich γ. □

3 Diagonalisierbarkeit

Diagonalmatrizen

(3.32) Definition (Diagonalmatrix)**.** Es seien $n \in \mathbb{N}_0$ und ein Körper K gegeben. Eine *Diagonalmatrix* über K ist eine Matrix $D \in K^{n\times n}$ mit $D_{i,j} = 0$ für $i, j \in [1, n]$ mit $i \neq j$.
Für eine Diagonalmatrix $D \in K^{n\times n}$ schreiben wir

$$\mathrm{Diag}(D_{1,1}, \ldots, D_{n,n}) := D.$$

Diagonalisierbarkeit

(3.33) Definition (diagonalisierbar)**.** Es sei ein Körper K gegeben.

(a) Es sei ein endlichdimensionaler K-Vektorraum V gegeben. Ein K-Vektorraumendomorphismus $\varphi\colon V \to V$ heißt *diagonalisierbar*, falls eine parametrisierte Basis $s = (s_j)_{j\in[1,\dim_K V]}$ von V so existiert, dass $\mathrm{M}_s^s(\varphi)$ eine Diagonalmatrix ist.

(b) Es sei $n \in \mathbb{N}_0$ gegeben. Ein $A \in K^{n\times n}$ heißt *diagonalisierbar*, falls φ_A diagonalisierbar ist.

(3.34) Bemerkung. Es seien $n \in \mathbb{N}_0$, ein Körper K und ein $A \in K^{n\times n}$ gegeben. Genau dann ist A diagonalisierbar, wenn A ähnlich zu einer Diagonalmatrix ist.

Beweis. Zunächst sei A diagonalisierbar, d.h. es sei φ_A diagonalisierbar. Dann gibt es eine parametrisierte Basis s von $K^{n\times 1}$ derart, dass $\mathrm{M}_s^s(\varphi_A)$ eine Diagonalmatrix ist. Nach Korollar (2.178) gilt aber

$$\mathrm{M}_s^s(\varphi_A) = (\mathrm{M}_{\mathrm{e}}^s(\mathrm{id}_{K^{n\times 1}}))^{-1}\,\mathrm{M}_{\mathrm{e}}^{\mathrm{e}}(\varphi_A)\,\mathrm{M}_{\mathrm{e}}^s(\mathrm{id}_{K^{n\times 1}}) = (\mathrm{M}_{\mathrm{e}}^s(\mathrm{id}_{K^{n\times 1}}))^{-1}\,A\,\mathrm{M}_{\mathrm{e}}^s(\mathrm{id}_{K^{n\times 1}}),$$

es ist also A ähnlich zur Diagonalmatrix $\mathrm{M}_s^s(\varphi_A)$.
Umgekehrt sei nun A ähnlich zu einer Diagonalmatrix D, d.h. es gebe ein $P \in \mathrm{GL}_n(K)$ mit $P^{-1}AP = D$. Wir setzen $s := (P_{-,j})_{j\in[1,n]}$. Wegen der Invertierbarkeit von P ist s nach Bemerkung (2.196) eine Basis von $K^{n\times 1}$ und es gilt $\mathrm{M}_{\mathrm{e}}^s(\mathrm{id}_{K^{n\times 1}}) = P$. Nach Korollar (2.178) folgt

$$\mathrm{M}_s^s(\varphi_A) = (\mathrm{M}_{\mathrm{e}}^s(\mathrm{id}_{K^{n\times 1}}))^{-1}\,\mathrm{M}_{\mathrm{e}}^{\mathrm{e}}(\varphi_A)\,\mathrm{M}_{\mathrm{e}}^s(\mathrm{id}_{K^{n\times 1}}) = P^{-1}\,A\,P = D.$$

Folglich ist φ_A und damit A diagonalisierbar. □

(3.35) Beispiel. Es sei $A \in \mathbb{Q}^{2\times 2}$ gegeben durch

$$A = \begin{pmatrix}2 & 1\\ 1 & 2\end{pmatrix}.$$

Dann ist A diagonalisierbar.

Beweis. Es gilt

$$\begin{pmatrix}1 & 1\\ -1 & 1\end{pmatrix}^{-1}\begin{pmatrix}2 & 1\\ 1 & 2\end{pmatrix}\begin{pmatrix}1 & 1\\ -1 & 1\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 3\end{pmatrix}.$$

□

Eigenbasen

(3.36) Definition (Eigenbasis)**.** Es sei ein Körper K gegeben.

(a) Es seien ein endlichdimensionaler K-Vektorraum V und ein K-Vektorraumendomorphismus $\varphi\colon V \to V$ gegeben. Eine (*parametrisierte*) *Eigenbasis* von V bzgl. φ ist eine parametrisierte Basis $s = (s_j)_{j\in[1,\dim_K V]}$ von V derart, dass s_j für jedes $j \in [1, \dim_K V]$ ein Eigenvektor von φ ist.

(b) Es seien $n \in \mathbb{N}_0$ und $A \in K^{n\times n}$ gegeben. Eine (*parametrisierte*) *Eigenbasis* von $K^{n\times 1}$ bzgl. A ist eine parametrisierte Eigenbasis von $K^{n\times 1}$ bzgl. φ_A.

(3.37) Bemerkung. Es seien ein Körper K, ein endlichdimensionaler K-Vektorraum V, eine parametrisierte Basis $s = (s_j)_{j\in[1,n]}$ von V und ein K-Vektorraumendomorphismus $\varphi\colon V \to V$ gegeben. Genau dann ist s eine Eigenbasis von V bzgl. φ, wenn $\mathrm{M}_s^s(\varphi)$ eine Diagonalmatrix ist.

Beweis. Genau dann ist s eine Eigenbasis von V bzgl. φ, wenn für jedes $j \in [1, n]$ ein $a_j \in K$ mit $\varphi(s_j) = a_j s_j$ existiert. Nach Bemerkung (2.154) ist dies aber äquivalent dazu, dass es für jedes $j \in [1, n]$ ein $a_j \in K$ mit $(\mathrm{M}_s^s(\varphi))_{-,j} = a_j \mathrm{e}_j$ gibt, d.h. dazu, dass $\mathrm{M}_s^s(\varphi)$ eine Diagonalmatrix ist. □

(3.38) Korollar. Es seien ein Körper K, ein endlichdimensionaler K-Vektorraum V und ein K-Vektorraumendomorphismus $\varphi\colon V \to V$ gegeben. Genau dann ist φ diagonalisierbar, wenn es eine Eigenbasis von V bzgl. φ gibt.

(3.39) Korollar. Es seien ein Körper K, ein endlichdimensionaler K-Vektorraum V und ein K-Vektorraumendomorphismus $\varphi\colon V \to V$ gegeben. Wenn es $\dim_K V$ verschiedene Eigenwerte von φ gibt, dann ist φ diagonalisierbar.

Beweis. Es seien verschiedene Eigenwerte a_j von φ und für $j \in [1, \dim V]$ gegeben. Ferner sei für $j \in [1, \dim V]$ ein Eigenvektor s_j von φ zum Eigenwert a_j gegeben. Nach Proposition (3.12) ist $(s_j)_{j\in[1,\dim V]}$ linear unabhängig und damit eine Basis nach Korollar (2.136). Dies bedeutet aber, dass $(s_j)_{j\in[1,\dim V]}$ eine Eigenbasis von V bzgl. φ ist. Die Diagonalisierbarkeit von φ folgt aus Korollar (3.38). □

Alternativer Beweis zu Beispiel (3.35). Nach Beispiel (3.3) und Proposition (3.12) ist

$$\left(\begin{pmatrix}1\\-1\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}\right)$$

eine Eigenbasis von A. Insbesondere ist A diagonalisierbar nach Korollar (3.38) diagonalisierbar. □

(3.40) Satz. Es seien ein Körper K, ein endlichdimensionaler K-Vektorraum V und ein K-Vektorraumendomorphismus $\varphi\colon V \to V$ gegeben. Genau dann ist φ diagonalisierbar, wenn χ_φ in Linearfaktoren zerfällt und wenn für jedes $a \in K$ die geometrische Vielfachheit von a als Eigenwert von φ gleich der algebraischen Vielfachheit von a als Eigenwert von φ ist.

Beweis. Zunächst sei φ diagonalisierbar, so dass es eine parametrisierte Basis $s = (s_j)_{j\in[1,\dim V]}$ von V derart gibt, dass $\mathrm{M}_s^s(\varphi) = \mathrm{Diag}(a_1, \ldots, a_{\dim V})$ für gewisse $a_j \in K$ für $j \in [1, \dim V]$, ist. Nach Korollar (2.226) erhalten wir

$$\begin{aligned}\chi_\varphi &= \chi_{\mathrm{M}_s^s(\varphi)} = \det(X\mathrm{E}_n - \mathrm{M}_s^s(\varphi)) = \det(X\mathrm{E}_n - \mathrm{Diag}(a_1, \ldots, a_{\dim V}))\\ &= \det \mathrm{Diag}(X - a_1, \ldots, X - a_{\dim V}) = \prod_{j\in[1,\dim V]} (X - a_j),\end{aligned}$$

das charakteristische Polynom χ_φ zerfällt also in Linearfaktoren. Die Summe der algebraischen Vielfachheiten von Skalaren als Eigenwerte von φ ist also gleich $\dim V$. Ferner ist s eine Eigenbasis von V bzgl. φ. Folglich ist die Summe aller geometrischen Vielfachheiten von Skalaren als Eigenwerte von φ mindestens gleich $\dim V$, der Summe aller algebraischen Vielfachheiten. Nach Proposition (3.31) ist aber jede geometrische Vielfachheit stets kleiner oder gleich der entsprechenden algebraischen Vielfachheit. Dies impliziert bereits, dass jede geometrische Vielfachheit gleich der entsprechenden algebraischen Vielfachheit ist.
Nun sei umgekehrt vorausgesetzt, dass χ_φ in Linearfaktoren zerfällt und dass für jedes $a \in K$ die geometrische Vielfachheit von a als Eigenwert von φ gleich der algebraischen Vielfachheit von a als Eigenwert von φ ist. Aus Proposition (3.12) folgt, dass sich Basen der Eigenräume von φ zu einer Basis von V und damit einer Eigenbasis von V bzgl. φ zusammensetzen lassen. Nach Korollar (3.38) ist φ diagonalisierbar. □

Aufgaben

Aufgabe 99 (Eigenwerte des Transponierens)**.** Es sei ein Körper K gegeben und es sei

$$\varphi\colon K^{2\times 2} \to K^{2\times 2},\ A \mapsto A^{\mathrm{tr}}.$$

(a) Bestimmen Sie die Eigenwerte und Eigenräume von φ.

(b) Ist φ diagonalisierbar?

Kapitel IV

Euklidische und unitäre Vektorräume

1 Sesquilinearformen

Definition

(4.1) Definition (Sesquilinearform)**.** Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$ und ein K-Vektorraum V gegeben. Eine *Sesquilinearform* auf V ist eine Abbildung $\beta\colon V \times V \to K$ derart, dass folgendes gilt:

- *Linearität in der zweiten Komponente.* Für $v \in V$ ist $\beta(v, -)\colon V \to K$ ein K-Vektorraumhomomorphismus.
- *Semilinearität in der ersten Komponente.* Für $w \in V$ ist $\beta(-, w)\colon V \to K$ ein Homomorphismus abelscher Gruppen und es gilt

  $$\beta(av, w) = \overline{a}\beta(v, w)$$

  für $a \in K$, $v \in V$.

Ist $K = \mathbb{R}$, so wird eine Sesquilinearform auf V auch *Bilinearform* auf V genannt.

Ausgeschrieben lesen sich die Axiome einer Sesquilinearform β auf einem Vektorraum V über $K \in \{\mathbb{R}, \mathbb{C}\}$ wie folgt:

- *Verträglichkeit mit den Additionen.* Für $v, w, w' \in V$ ist $\beta(v, w+w') = \beta(v, w) + \beta(v, w')$. Für $v, v', w \in V$ ist $\beta(v + v', w) = \beta(v, w) + \beta(v', w)$.
- *Verträglichkeit der Nullelemente.* Für $v \in V$ ist $\beta(v, 0) = \beta(0, v) = 0$.
- *Verträglichkeit der negativen Elemente.* Für $v, w \in V$ ist $\beta(v, -w) = \beta(-v, w) = -\beta(v, w)$.
- *Verträglichkeit mit den Skalarmultiplikationen.* Für $a \in K$, $v, w \in V$ ist $\beta(v, aw) = a\,\beta(v, w)$. Für $a \in K$, $v, w \in V$ ist $\beta(av, w) = \overline{a}\beta(v, w)$. (Falls $K = \mathbb{R}$ ist, so bedeutet dies, dass für $a \in K$, $v, w \in V$ stets $\beta(av, w) = a\,\beta(v, w)$ ist.)

Nach Lemma (1.67) wissen wir, dass diese Axiome redundant sind.

Gram-Matrix

Im Folgenden werden wir $K^{1\times 1}$ mit K identifizieren.

(4.2) Bemerkung. Es seien $n \in \mathbb{N}_0$, $K \in \{\mathbb{R}, \mathbb{C}\}$ und $A \in K^{n\times n}$ gegeben. Die Abbildung

$$\beta_A\colon K^{n\times 1} \times K^{n\times 1} \to K,\ (x, y) \mapsto \overline{x}^{\mathrm{tr}} A y$$

ist eine Sesquilinearform auf $K^{n\times 1}$.

Beweis. Für $x \in K^{n\times 1}$ ist $\beta_A(x,-) = \varphi_{\overline{x}^{\mathrm{tr}}A}\colon K^{n\times 1} \to K$ ein K-Vektorraumhomomorphismus. Es sei $y \in K^{n\times 1}$ gegeben. Dann gilt

$$\beta_A(x+x',y) = \overline{x+x'}^{\mathrm{tr}}Ay = \overline{x}^{\mathrm{tr}}Ay + \overline{x'}^{\mathrm{tr}}Ay = \beta_A(x,y) + \beta_A(x',y)$$

für $x, x' \in K^{n\times 1}$, d.h. $\beta_A(-,y)$ ist ein Homomorphismus abelscher Gruppen nach Lemma (1.67), sowie

$$\beta_A(ax,y) = \overline{ax}^{\mathrm{tr}}Ay = \overline{a}\,\overline{x}^{\mathrm{tr}}Ay = \overline{a}\beta_A(x,y)$$

für $a \in K$, $x \in K^{n\times 1}$. Insgesamt ist β_A eine Sesquilinearform auf $K^{n\times 1}$. □

(4.3) Definition (Gram-Matrix)**.** Es seien $K \in \{\mathbb{R},\mathbb{C}\}$, ein endlichdimensionaler K-Vektorraum V, eine parametrisierte Basis $s = (s_j)_{j\in[1,n]}$ von V und eine Sesquilinearform β auf V gegeben. Die Matrix

$$\mathrm{G}_s(\beta) := (\beta(s_i,s_j))_{i,j\in[1,n]}$$

heißt *Gram-Matrix* (oder *Darstellungsmatrix*) von β bzgl. s.

(4.4) Bemerkung. Es seien $n \in \mathbb{N}_0$, $K \in \{\mathbb{R},\mathbb{C}\}$ und $A \in K^{n\times n}$ gegeben. Dann ist

$$\mathrm{G}_{\mathrm{e}}(\beta_A) = A.$$

Beweis. Für $i,j \in [1,n]$ ist

$$\mathrm{G}_{\mathrm{e}}(\beta_A)_{i,j} = \beta_A(\mathrm{e}_i,\mathrm{e}_j) = \mathrm{e}_i^{\mathrm{tr}}A\mathrm{e}_j = \mathrm{e}_i^{\mathrm{tr}}A_{-,j} = A_{i,j}.$$

Somit gilt $\mathrm{G}_{\mathrm{e}}(\beta_A) = A$. □

(4.5) Proposition. Es seien $K \in \{\mathbb{R},\mathbb{C}\}$, ein endlichdimensionaler K-Vektorraum V, eine parametrisierte Basis $s = (s_j)_{j\in[1,n]}$ von V und eine Sesquilinearform β auf V gegeben. Für $v,w \in V$ gilt

$$\beta(v,w) = \overline{\kappa_s(v)}^{\mathrm{tr}}\,\mathrm{G}_s(\beta)\kappa_s(w) = \beta_{\mathrm{G}_s(\beta)}(\kappa_s(v),\kappa_s(w)).$$

Beweis. Für $v,w \in V$ gilt

$$\begin{aligned}\beta(v,w) &= \beta\Big(\sum_{i\in[1,n]}(\kappa_s(v))_i s_i, \sum_{j\in[1,n]}(\kappa_s(w))_j s_j\Big) = \sum_{i\in[1,n]}\sum_{j\in[1,n]}\overline{(\kappa_s(v))_i}\beta(s_i,s_j)(\kappa_s(w))_j \\ &= \sum_{i\in[1,n]}\sum_{j\in[1,n]}(\overline{\kappa_s(v)}^{\mathrm{tr}})_i(\mathrm{G}_s(\beta))_{i,j}(\kappa_s(w))_j = \overline{\kappa_s(v)}^{\mathrm{tr}}\mathrm{G}_s(\beta)\kappa_s(w).\end{aligned}$$

□

(4.6) Korollar. Es seien $K \in \{\mathbb{R},\mathbb{C}\}$, ein endlichdimensionaler K-Vektorraum V, parametrisierte Basen $s = (s_j)_{j\in[1,n]}$ und $s' = (s'_j)_{j\in[1,n]}$ von V und eine Sesquilinearform β auf V gegeben. Dann ist

$$\mathrm{G}_{s'}(\beta) = \overline{\mathrm{M}_s^{s'}(\mathrm{id}_V)}^{\mathrm{tr}}\,\mathrm{G}_s(\beta)\,\mathrm{M}_s^{s'}(\mathrm{id}_V).$$

Beweis. Für $k,l \in [1,n]$ gilt

$$\begin{aligned}\beta(s'_k,s'_l) &= \overline{\kappa_s(s'_k)}^{\mathrm{tr}}\mathrm{G}_s(\beta)\kappa_s(s'_l) = \overline{(\mathrm{M}_s^{s'}(\mathrm{id}_V))_{-,k}}^{\mathrm{tr}}\,\mathrm{G}_s(\beta)(\mathrm{M}_s^{s'}(\mathrm{id}_V))_{-,l} \\ &= (\overline{\mathrm{M}_s^{s'}(\mathrm{id}_V)}^{\mathrm{tr}})_{k,-}\,(\mathrm{G}_s(\beta)\,\mathrm{M}_s^{s'}(\mathrm{id}_V))_{-,l} = (\overline{\mathrm{M}_s^{s'}(\mathrm{id}_V)}^{\mathrm{tr}}\,\mathrm{G}_s(\beta)\,\mathrm{M}_s^{s'}(\mathrm{id}_V))_{k,l}\end{aligned}$$

und damit

$$\mathrm{G}_{s'}(\beta) = \overline{\mathrm{M}_s^{s'}(\mathrm{id}_V)}^{\mathrm{tr}}\,\mathrm{G}_s(\beta)\,\mathrm{M}_s^{s'}(\mathrm{id}_V).$$

□

Hermitizität

(4.7) Definition (hermitesch)**.** Es sei $K \in \{\mathbb{R}, \mathbb{C}\}$ gegeben.

(a) Es sei ein K-Vektorraum V gegeben. Eine Sesquilinearform β auf V heißt *hermitesch*, falls für $v, w \in V$ stets

$$\beta(w, v) = \overline{\beta(v, w)}$$

ist.

Ist $K = \mathbb{R}$, so wird eine hermitesche Sesquilinearform auf V auch *symmetrische Bilinearform* auf V genannt.

(b) Es sei $n \in \mathbb{N}_0$ gegeben. Ein $A \in K^{n\times n}$ heißt *hermitesch*, falls β_A hermitesch ist.

Ist $K = \mathbb{R}$, so wird eine hermitesche Matrix auch *symmetrische Matrix* genannt.

(4.8) Bemerkung. Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$, ein endlichdimensionaler K-Vektorraum V, eine parametrisierte Basis $s = (s_j)_{j\in[1,n]}$ von V und eine Sesquilinearform β auf V gegeben. Genau dann ist β hermitesch, wenn $\mathrm{G}_s(\beta)$ hermitesch ist.

Beweis. Nach Proposition (4.5) gilt $\beta(v, w) = \beta_{\mathrm{G}_s(\beta)}(\kappa_s(v), \kappa_s(w))$ für $v, w \in V$. Es ist aber $\kappa_s \colon V \to K^{n\times 1}$ ein Isomorphismus und damit insbesondere eine Bijektion. Folglich ist β genau dann hermitesch, wenn $\beta_{\mathrm{G}_s(\beta)}$ hermitesch ist, d.h. wenn $\mathrm{G}_s(\beta)$ hermitesch ist. □

(4.9) Bemerkung. Es seien $n \in \mathbb{N}_0$, $K \in \{\mathbb{R}, \mathbb{C}\}$ und ein $A \in K^{n\times n}$ gegeben. Genau dann ist A hermitesch, wenn

$$\overline{A}^{\mathrm{tr}} = A$$

ist.

Beweis. Es sei zunächst A hermitesch, d.h. es sei β_A hermitesch. Für $i, j \in [1, n]$ gilt dann

$$(\overline{A}^{\mathrm{tr}})_{i,j} = \overline{A_{j,i}} = \overline{\mathrm{e}_j^{\mathrm{tr}} A \mathrm{e}_i} = \overline{\beta_A(\mathrm{e}_j, \mathrm{e}_i)} = \beta_A(\mathrm{e}_i, \mathrm{e}_j) = \mathrm{e}_i^{\mathrm{tr}} A \mathrm{e}_j = A_{i,j},$$

d.h. es ist $\overline{A}^{\mathrm{tr}} = A$.
Nun gelte umgekehrt $\overline{A}^{\mathrm{tr}} = A$. Für $x, y \in K^{n\times 1}$ ergibt sich dann

$$\overline{\beta_A(y, x)} = \overline{\beta_A(y, x)}^{\mathrm{tr}} = \overline{\overline{y}^{\mathrm{tr}} A x}^{\mathrm{tr}} = \overline{x}^{\mathrm{tr}} \overline{A}^{\mathrm{tr}} y = \overline{x}^{\mathrm{tr}} A y = \beta_A(x, y),$$

d.h. β_A ist hermitesch. Dies bedeutet aber, dass A hermitesch ist. □

Die nachfolgende Bemerkung zeigt, dass die Axiome einer hermiteschen Sesquilinearform redundant sind.

(4.10) Bemerkung. Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$, ein K-Vektorraum V und eine Abbildung $\beta \colon V \times V \to K$ gegeben. Genau dann ist β eine hermitesche Sesquilinearform, wenn folgende Eigenschaften gelten.

- *Linearität in der zweiten Komponente.* Für $v \in V$ ist $\beta(v, -) \colon V \to K$ ein K-Vektorraumhomomorphismus.
- *Hermitizität.* Für $v, w \in V$ ist $\beta(w, v) = \overline{\beta(v, w)}$.

Beweis. Wenn β eine hermitesche Sesquilinearform ist, so erfüllt β insbesondere die beiden angegebenen Eigenschaften. Es sei also umgekehrt angenommen, dass für $v \in V$ stets $\beta(v, -) \colon V \to K$ ein K-Vektorraumhomomorphismus ist und dass für $v, w \in V$ stets $\overline{\beta(w, v)} = \beta(v, w)$ gilt. Um zu zeigen, dass β eine hermitesche Sesquilinearform auf V ist, verbleibt es die Semilinearität in der ersten Komponente zu verifizieren. Hierzu sei ein $w \in V$ gegeben. Für $v, v' \in V$ gilt dann

$$\beta(v + v', w) = \overline{\beta(w, v + v')} = \overline{\beta(w, v) + \beta(w, v')} = \overline{\beta(w, v)} + \overline{\beta(w, v')} = \beta(v, w) + \beta(v', w),$$

so dass $\beta(-, w) \colon V \to K$ nach Lemma (1.67) ein Homomorphismus abelscher Gruppen ist. Für $a \in K$, $v \in V$ gilt ferner

$$\beta(av, w) = \overline{\beta(w, av)} = \overline{a\beta(w, v)} = \overline{a}\overline{\beta(w, v)} = \overline{a}\beta(v, w).$$

Insgesamt ist β eine hermitesche Sesquilinearform auf V. □

Positive Definitheit

(4.11) Definition (positiv definit)**.** Es sei $K \in \{\mathbb{R}, \mathbb{C}\}$ gegeben.

(a) Es sei ein K-Vektorraum V gegeben. Eine Sesquilinearform β auf V heißt *positiv definit*, falls für $v \in V \setminus \{0\}$ stets

$$\beta(v, v) > 0$$

ist.

(b) Es sei $n \in \mathbb{N}_0$ gegeben. Ein $A \in K^{n\times n}$ heißt *positiv definit*, falls β_A positiv definit ist.

(4.12) Bemerkung. Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$, ein endlichdimensionaler K-Vektorraum V, eine parametrisierte Basis $s = (s_j)_{j\in[1,n]}$ von V und eine Sesquilinearform β auf V gegeben. Genau dann ist β positiv definit, wenn $\mathrm{G}_s(\beta)$ positiv definit ist.

Beweis. Nach Proposition (4.5) gilt $\beta(v, w) = \beta_{\mathrm{G}_s(\beta)}(\kappa_s(v), \kappa_s(w))$ für $v, w \in V$. Es ist aber $\kappa_s \colon V \to K^{n\times 1}$ ein Isomorphismus und damit insbesondere eine Bijektion. Folglich ist β genau dann positiv definit, wenn $\beta_{\mathrm{G}_s(\beta)}$ positiv definit ist, d.h. wenn $\mathrm{G}_s(\beta)$ positiv definit ist. □

Aufgaben

Aufgabe 100 (quadratische Formen)**.** Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$, ein K-Vektorraum V und eine hermitesche Sesquilinearform β auf V gegeben. Die Abbildung

$$\mathrm{q}_\beta \colon V \to K,\ v \mapsto \beta(v, v)$$

heißt die zu β *assoziierte quadratische Form*.
Zeigen Sie:

(a) Für $a \in K$, $v \in V$ gilt

$$\mathrm{q}_\beta(av) = |a|^2\, \mathrm{q}_\beta(v).$$

(b) Für $v, w \in V$ gilt

$$\mathrm{q}_\beta(v + w) + \mathrm{q}_\beta(v - w) = 2\mathrm{q}_\beta(v) + 2\mathrm{q}_\beta(w).$$

(c) Wenn $K = \mathbb{R}$ ist, so gilt für $v, w \in V$ stets

$$\beta(v, w) = \frac{1}{2}(\mathrm{q}_\beta(v + w) - \mathrm{q}_\beta(v) - \mathrm{q}_\beta(w)) = \frac{1}{4}(\mathrm{q}_\beta(v + w) - \mathrm{q}_\beta(v - w)).$$

Wenn $K = \mathbb{C}$ ist, so gilt für $v, w \in V$ stets

$$\beta(v, w) = \frac{1}{4}(\mathrm{q}_\beta(v + w) - \mathrm{q}_\beta(v - w)) + \mathrm{i}\frac{1}{4}(-\mathrm{q}_\beta(v + \mathrm{i}w) + \mathrm{q}_\beta(v - \mathrm{i}w)).$$

Aufgabe 101 (schiefhermitesche Sesquilinearformen)**.** Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$ und ein K-Vektorraum V gegeben. Eine Sesquilinearform β auf V heißt *schiefhermitesch*, falls für $v, w \in V$ stets

$$\beta(w, v) = -\overline{\beta(v, w)}$$

ist. Ist $K = \mathbb{R}$, so wird eine schiefhermitesche Sesquilinearform auf V auch schiefsymmetrische Bilinearform auf V genannt. Eine Sesquilinearform β auf V heißt *alternierend*, falls für $v \in V$ stets

$$\beta(v, v) = 0$$

ist.
Nun sei eine Sesquilinearform β auf V gegeben. Ferner bezeichne $V|_{\mathbb{R}}$ den $\mathbb{R}$-Vektorraum, der aus V durch Einschränkung der Skalarmultiplikation auf Skalare aus $\mathbb{R}$ entsteht.

(a) Die Abbildungen $\mathrm{Re} \circ \beta \colon V \times V \to \mathbb{R}$, $(v, w) \mapsto \mathrm{Re}\,\beta(v, w)$ und $\mathrm{Im} \circ \beta \colon V \times V \to \mathbb{R}$, $(v, w) \mapsto \mathrm{Im}\,\beta(v, w)$ sind Bilinearformen auf $V|_{\mathbb{R}}$.

(b) Zeigen Sie, dass die folgenden Bedingungen äquivalent sind.

(i) Die Sesquilinearform $\beta \colon V \times V \to K$ ist schiefhermitesch.

(ii) Die Bilinearform $\mathrm{Re} \circ \beta$ auf $V|_{\mathbb{R}}$ ist alternierend und die Bilinearform $\mathrm{Im} \circ \beta$ auf $V|_{\mathbb{R}}$ ist symmetrisch.

(c) Es sei $K = \mathbb{R}$. Zeigen Sie, dass die Bilinearform β genau dann schiefsymmetrisch ist, wenn sie alternierend ist.

Aufgabe 102 (positiv definite Matrizen)**.** Es seien $n \in \mathbb{N}_0$, $K \in \{\mathbb{R}, \mathbb{C}\}$, $A \in K^{n \times n}$ gegeben. Zeigen Sie: Wenn A positiv definit ist, dann gilt

$$A_{i,i} > 0$$

für $i \in [1, n]$.

2 Skalarprodukträume

Definition

(4.13) Definition (Skalarproduktraum)**.**

(a) Es sei $K \in \{\mathbb{R}, \mathbb{C}\}$ gegeben. Ein *K-Skalarproduktraum* (oder *K-Vektorraum mit Skalarprodukt* oder *K-Prähilbertraum*) besteht aus einem K-Vektorraum V zusammen mit einer positiv definiten, hermiteschen Sesquilinearform β auf V. Unter Missbrauch der Notation bezeichnen wir sowohl den besagten K-Skalarproduktraum als auch den unterliegenden K-Vektorraum mit V. Die Sesquilinearform β wird *Skalarprodukt* von V genannt.

Für einen K-Skalarproduktraum V mit Skalarprodukt β schreiben wir $\langle -, = \rangle = \langle -, = \rangle^V := \beta$ und $\langle v, w \rangle = \langle v, w \rangle^V := \beta(v, w)$ für $v, w \in V$.

(b) Ein *euklidischer Vektorraum* ist ein endlichdimensionaler $\mathbb{R}$-Skalarproduktraum. Ein *unitärer Vektorraum* ist ein endlichdimensionaler $\mathbb{C}$-Skalarproduktraum.

Wir listen die Axiome des Skalarprodukts eines Skalarproduktraums V über $K \in \{\mathbb{R}, \mathbb{C}\}$ in Standardnotation:

- *Verträglichkeit mit den Additionen.* Für $v, w, w' \in V$ ist $\langle v, w + w' \rangle = \langle v, w \rangle + \langle v, w' \rangle$. Für $v, v', w \in V$ ist $\langle v + v', w \rangle = \langle v, w \rangle + \langle v', w \rangle$.
- *Verträglichkeit der Nullelemente.* Für alle $v \in V$ ist $\langle v, 0 \rangle = \langle 0, v \rangle = 0$.
- *Verträglichkeit der negativen Elemente.* Für alle $v, w \in V$ ist $\langle v, -w \rangle = \langle -v, w \rangle = -\langle v, w \rangle$.
- *Verträglichkeit mit den Skalarmultiplikationen.* Für $a \in K$, $v, w \in V$ ist $\langle v, aw \rangle = a\langle v, w \rangle$. Für $a \in K$, $v, w \in V$ ist $\langle av, w \rangle = \overline{a}\langle v, w \rangle$. (Falls $K = \mathbb{R}$ ist, so bedeutet dies, dass für $a \in K$, $v, w \in V$ stets $\langle av, w \rangle = a\langle v, w \rangle$ ist.)
- *Hermitizität.* Für $v, w \in V$ gilt $\overline{\langle w, v \rangle} = \langle v, w \rangle$.
- *Positive Definitheit.* Für $v \in V \setminus \{0\}$ gilt $\langle v, v \rangle > 0$.

Nach Lemma (1.67) wissen wir, dass diese Axiome redundant sind.

(4.14) Beispiel. Es sei $n \in \mathbb{N}_0$ gegeben.

(a) Es wird $\mathbb{R}^{n \times 1}$ ein euklidischer Vektorraum, wobei das Skalarprodukt durch

$$\langle x, y \rangle = x^{\mathrm{tr}} y = \sum_{j \in [1,n]} x_j y_j$$

für $x, y \in \mathbb{R}^{n \times 1}$ gegeben ist.

(b) Es wird $\mathbb{C}^{n\times 1}$ ein unitärer Vektorraum, wobei das Skalarprodukt durch

$$\langle x, y\rangle = \overline{x}^{\mathrm{tr}} y = \sum_{j\in[1,n]} \overline{x_j} y_j$$

für $x, y \in \mathbb{C}^{n\times 1}$ gegeben ist.

Beweis. Es sei $K \in \{\mathbb{R}, \mathbb{C}\}$. Dann ist E_n positive definit und hermitesche. Folglich wird $K^{n\times 1}$ ein K-Skalarproduktraum mit $\langle -, = \rangle = \beta_{\mathrm{E}_n}$. Für $x, y \in K^{n\times 1}$ ist dann aber

$$\langle x, y\rangle = \beta_{\mathrm{E}_n}(x, y) = \overline{x}^{\mathrm{tr}} \mathrm{E}_n y = \overline{x}^{\mathrm{tr}} y = \sum_{j\in[1,n]} \overline{x_j} y_j. \qquad \square$$

(4.15) Konvention. Es sei $n \in \mathbb{N}_0$ gegeben.

(a) Sofern nicht anders erwähnt, betrachten wir ab jetzt $\mathbb{R}^{n\times 1}$ als euklidischen Vektorraum mit Skalarprodukt wie in Beispiel (4.14)(a).

(b) Sofern nicht anders erwähnt, betrachten wir ab jetzt $\mathbb{C}^{n\times 1}$ als unitären Vektorraum mit Skalarprodukt wie in Beispiel (4.14)(b).

(4.16) Beispiel. Es wird $\mathrm{C}([0,1], \mathbb{R})$ ein $\mathbb{R}$-Skalarproduktraum, wobei das Skalarprodukt durch

$$\langle f, g\rangle = \int_0^1 f(t) g(t)\, \mathrm{d}t$$

für $f, g \in \mathrm{C}([0,1], \mathbb{R})$ gegeben ist.

Ohne Beweis. $\square$

(4.17) Lemma (Cauchy-Schwarz-Ungleichung)**.** Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$, ein K-Skalarproduktraum V und $v, w \in V$ gegeben. Dann gilt

$$|\langle v, w\rangle|^2 \leq \langle v, v\rangle \langle w, w\rangle.$$

Genau dann gilt

$$|\langle v, w\rangle|^2 = \langle v, v\rangle \langle w, w\rangle,$$

wenn (v, w) linear abhängig in V ist.

Beweis. Ist $w = 0$, so gilt

$$|\langle v, w\rangle| = |\langle v, 0\rangle| = 0 = \|v\|\, \|0\| = \|v\|\, \|w\|$$

und (v, w) ist linear abhängig in V nach Korollar (2.100). Im Folgenden gelte daher $w \neq 0$. Dann erhalten wir

$$\begin{aligned} 0 &\leq \langle v - \frac{\langle w, v\rangle}{\langle w, w\rangle} w, v - \frac{\langle w, v\rangle}{\langle w, w\rangle} w\rangle = \langle v, v\rangle - \frac{\langle w, v\rangle}{\langle w, w\rangle}\langle v, w\rangle - \frac{\overline{\langle w, v\rangle}}{\langle w, w\rangle}\langle w, v\rangle + \frac{\overline{\langle w, v\rangle}}{\langle w, w\rangle}\frac{\langle w, v\rangle}{\langle w, w\rangle}\langle w, w\rangle \\ &= \langle v, v\rangle - \frac{\overline{\langle v, w\rangle}}{\langle w, w\rangle}\langle v, w\rangle = \langle v, v\rangle - \frac{|\langle v, w\rangle|^2}{\langle w, w\rangle} \end{aligned}$$

und damit $|\langle v, w\rangle|^2 \leq \langle v, v\rangle \langle w, w\rangle$.
Ist $|\langle v, w\rangle|^2 = \langle v, v\rangle \langle w, w\rangle$, so gilt $0 = \langle v - \frac{\langle w,v\rangle}{\langle w,w\rangle} w, v - \frac{\langle w,v\rangle}{\langle w,w\rangle} w\rangle$. Wegen der positiven Definitionheit folgt also $v - \frac{\langle w,v\rangle}{\|w\|^2} w = 0$ und damit die lineare Unabhängigkeit von (v, w).
Ist umgekehrt (v, w) linear abhängig, so ist v wegen $w \neq 0$ nach Bemerkung (2.104) und Proposition (2.105)(b) eine Linearkombination von (w), d.h. es gibt ein $a \in K$ mit $v = aw$. Es folgt

$$|\langle v, w\rangle|^2 = \langle v, w\rangle \overline{\langle v, w\rangle} = \langle v, w\rangle \langle w, v\rangle = \langle v, w\rangle \langle w, aw\rangle = a\langle v, w\rangle \langle w, w\rangle = \langle v, aw\rangle \langle w, w\rangle = \langle v, v\rangle \langle w, w\rangle$$

und damit $|\langle v, w\rangle|^2 = \langle v, v\rangle \langle w, w\rangle$. $\square$

Norm

(4.18) Definition (induzierte Norm)**.** Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$ und ein K-Skalarproduktraum V gegeben. Die Abbildung

$$\|-\| \colon V \to \mathbb{R},\ v \mapsto \sqrt{\langle v, v\rangle}$$

heißt die durch das Skalarprodukt *induzierte Norm* auf V.

(4.19) Beispiel. Es sei $n \in \mathbb{N}_0$ gegeben.

(a) Für $x \in \mathbb{R}^{n\times 1}$ gilt

$$\|x\| = \sqrt{\sum_{j\in[1,n]} x_j^2}.$$

(b) Für $x \in \mathbb{C}^{n\times 1}$ gilt

$$\|x\| = \sqrt{\sum_{j\in[1,n]} |x_j|^2}.$$

(4.20) Proposition. Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$ und ein K-Skalarproduktraum V gegeben.

(a) *Positive Definitheit.* Für $v \in V$ gilt

$$\|v\| \geq 0$$

und genau dann $\|v\| = 0$, wenn $v = 0$ ist.

(b) *Absolut-Homogenität.* Für $a \in K$, $v \in V$ gilt

$$\|av\| = |a|\,\|v\|.$$

(c) *Dreicksungleichung.* Für $v, w \in V$ gilt

$$\|v + w\| \leq \|v\| + \|w\|.$$

Beweis.

(a) Dies ist eine Umformulierung der positiven Definitheit des Skalarprodukts.

(b) Für $a \in K$, $v \in V$ gilt

$$\|av\|^2 = \langle av, av\rangle = \overline{a}a\langle v, v\rangle = |a|^2\,\|v\|^2 = (|a|\,\|v\|)^2$$

und damit $\|av\| = |a|\,\|v\|$.

(c) Für $v, w \in V$ gilt nach der Cauchy-Schwarz-Ungleichung (4.17) stets

$$(\operatorname{Re}\langle v, w\rangle)^2 \leq |\langle v, w\rangle|^2 \leq \langle v, v\rangle\langle w, w\rangle = \|v\|^2\,\|w\|^2,$$

also

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

und damit $\|v + w\| \leq \|v\| + \|w\|$. □

Die Cauchy-Schwarz-Ungleichung lässt sich mit Hilfe der induzierten Norm auch wie folgt umformulieren:

(4.21) Bemerkung (Cauchy-Schwarz-Ungleichung)**.** Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$, ein K-Skalarproduktraum V und $v, w \in V$ gegeben. Dann gilt

$$|\langle v, w\rangle| \leq \|v\| \, \|w\|.$$

Genau dann gilt

$$|\langle v, w\rangle| = \|v\| \, \|w\|,$$

wenn (v, w) linear abhängig in V ist.

Beweis. Dies folgt aus Lemma (4.17) und Definition (4.18). □

(4.22) Beispiel. Es sei $n \in \mathbb{N}_0$ gegeben.

(a) Für $x, y \in \mathbb{R}^{n\times 1}$ gilt

$$|\sum_{j=1}^{n} x_j y_j| \leq \sqrt{\sum_{j=1}^{n} x_j^2} \sqrt{\sum_{j=1}^{n} y_j^2}.$$

(b) Für $x, y \in \mathbb{C}^{n\times 1}$ gilt

$$|\sum_{j=1}^{n} \overline{x_j} y_j| \leq \sqrt{\sum_{j=1}^{n} |x_j|^2} \sqrt{\sum_{j=1}^{n} |y_j|^2}.$$

(4.23) Definition (normierter Vektor)**.** Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$ und ein K-Skalarproduktraum V gegeben. Ein Vektor v in V heißt *normiert*, wenn

$$\|v\| = 1$$

ist.

(4.24) Bemerkung. Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$ und ein K-Skalarproduktraum V gegeben. Für $v \in V \setminus \{0\}$ ist $\frac{1}{\|v\|} v$ normiert.

Beweis. Wegen der Absoluthomogenität der Norm, siehe Proposition (4.20)(b), gilt für $v \in V \setminus \{0\}$ stets

$$\|\frac{1}{\|v\|} v\| = |\frac{1}{\|v\|}| \, \|v\| = \frac{1}{\|v\|} \|v\| = 1,$$

d.h. $\frac{1}{\|v\|} v$ ist normiert. □

3 Orthogonalität

Definition

(4.25) Definition (Orthogonalität)**.** Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$ und ein K-Skalarproduktraum V gegeben. Für $v, w \in V$ sagen wir, dass v *orthogonal* zu w ist, geschrieben $v \perp w$, wenn

$$\langle v, w\rangle = 0$$

gilt.

(4.26) Bemerkung. Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$ und ein K-Skalarproduktraum V gegeben. Die Orthogonalitätsrelation $\perp$ auf V ist symmetrisch.

Beweis. Es seien $v, w \in V$ mit $v \perp w$ gegeben, d.h. es gelte $\langle v, w\rangle = 0$. Da das Skalarprodukt hermitesch ist, gilt dann auch $\langle w, v\rangle = \overline{\langle v, w\rangle} = \overline{0} = 0$, also $w \perp v$. □

(4.27) Proposition. Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$ und ein K-Skalarproduktraum V gegeben.

(a) Für $v, w, w' \in V$ gilt: Wenn $v \perp w$ und $v \perp w'$ gilt, dann auch $v \perp w + w'$.

(b) Für $v \in V$ gilt $v \perp 0$.

(c) Für $a \in K$, $v, w \in V$ gilt: Wenn $v \perp w$, dann auch $v \perp aw$.

Beweis.

(a) Es seien $v, w, w' \in V$ mit $v \perp w$ und $v \perp w'$ gegeben, d.h. es gelte $\langle v, w\rangle = 0$ und $\langle v, w'\rangle = 0$. Da $\langle v, -\rangle \colon V \to K$ ein K-Vektorraumhomomorphismus ist, folgt

$$\langle v, w + w'\rangle = \langle v, w\rangle + \langle v, w'\rangle = 0 + 0 = 0,$$

Somit gilt auch $v \perp w + w'$.

(b) Für $v \in V$ ist $\langle v, -\rangle \colon V \to K$ ein K-Vektorraumhomomorphismus, es gilt also $\langle v, 0\rangle = 0$ und damit $v \perp 0$.

(c) Es seien $a \in K$, $v, w \in V$ mit $v \perp w$ gegeben. Da $\langle v, -\rangle \colon V \to K$ ein K-Vektorraumhomomorphismus ist, folgt

$$\langle v, aw\rangle = a\langle v, w\rangle = a0 = 0.$$

Somit gilt auch $v \perp aw$. □

(4.28) Proposition (Satz des Pythagoras)**.** Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$, ein K-Skalarproduktraum V und $v, w \in V$ gegeben. Wenn $v \perp w$ ist, so gilt

$$\|v + w\|^2 = \|v\|^2 + \|w\|^2.$$

Beweis. Wenn $v \perp w$ ist, gilt $\langle v, w\rangle = \langle w, v\rangle = 0$ und damit

$$\|v + w\|^2 = \langle v + w, v + w\rangle = \langle v, v\rangle + \langle v, w\rangle + \langle w, v\rangle + \langle w, w\rangle = \langle v, v\rangle + \langle w, w\rangle = \|v\|^2 + \|w\|^2.$$ □

(4.29) Definition (Orthogonalität, Orthonormalität)**.** Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$ und ein K-Skalarproduktraum V gegeben.

(a) Eine Familie $s = (s_i)_{i \in I}$ in V heißt *orthogonal* (oder ein *Orthogonalsystem*), falls für $i, j \in I$ mit $i \neq j$ stets $s_i \perp s_j$ ist. Eine Familie $s = (s_i)_{i \in I}$ in V heißt *orthonormal* (oder *orthonormiert* oder ein *Orthonormalsystem*), falls sie orthogonal und s_i für jedes $i \in I$ normiert ist.

(b) Eine Teilmenge S von V heißt *orthogonal* (oder ein *Orthogonalsystem*), falls für $s, t \in S$ mit $s \neq t$ stets $s \perp t$ ist. Eine Teilmenge S von V heißt *orthonormal* (oder *orthonormiert* oder ein *Orthonormalsystem*), falls sie orthogonal und jedes $s \in S$ normiert ist.

(4.30) Bemerkung. Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$, ein K-Skalarproduktraum V und eine Familie $s = (s_i)_{i \in I}$ in V gegeben.

(a) Genau dann ist s orthogonal, wenn

$$\langle s_i, s_j\rangle = \delta_{i,j}\|s_i\|^2 = \delta_{i,j}\|s_j\|^2$$

für $i, j \in I$ gilt.

(b) Genau dann ist s ist orthonormal, wenn

$$\langle s_i, s_j\rangle = \delta_{i,j}$$

für $i, j \in I$ gilt.

(4.31) Proposition. Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$, ein K-Skalarproduktraum V und eine orthogonale Familie $s = (s_i)_{i \in I}$ in V mit $s_i \neq 0$ für alle $i \in I$ gegeben. Dann ist s linear unabhängig.

Beweis. Es sei $a \in K^{(I)}$ mit $\sum_{i\in I} a_i s_i = 0$ gegeben. Für $i \in I$ gilt dann

$$0 = \langle s_i, 0\rangle = \langle s_i, \sum_{j\in I} a_j s_j\rangle = \sum_{j\in I} a_j \langle s_i, s_j\rangle = \sum_{j\in I} a_j \delta_{i,j}\|s_j\|^2 = a_i\|s_i\|^2.$$

Da aber $s_i \neq 0$ für $i \in I$ ist, gilt $\|s_i\|^2 \neq 0$ und damit $a_i = 0$ für alle $i \in I$. Folglich ist s linear unabhängig. □

(4.32) Definition. Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$ und ein endlichdimensionaler K-Skalarproduktraum V gegeben.

(a) Eine Familie $s = (s_i)_{i\in I}$ in V heißt *Orthogonalbasis* von V, falls sie orthogonal und eine Basis von V ist. Eine Familie $s = (s_i)_{i\in I}$ in V heißt *Orthonormalbasis* von V, falls sie orthonormal und eine Basis von V ist.

(b) Eine Teilmenge S von V heißt *Orthogonalbasis* von V, falls sie orthogonal und eine Basis von V ist. Eine Teilmenge S von V heißt *Orthonormalbasis* von V, falls sie orthonormal und eine Basis von V ist.

(4.33) Bemerkung. Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$, ein endlichdimensionaler K-Skalarproduktraum V und eine parametrisierte Basis $s = (s_i)_{i\in[1,n]}$ von V gegeben.

(a) Genau dann ist s eine Orthogonalbasis von V, wenn $\mathrm{G}_s(\langle -, =\rangle)$ eine Diagonalmatrix ist.

(b) Genau dann ist s eine Orthonormalbasis von V, wenn $\mathrm{G}_s(\langle -, =\rangle) = \mathrm{E}_n$ ist.

(4.34) Bemerkung. Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$, ein endlichdimensionaler K-Skalarproduktraum V und eine parametrisierte Basis $s = (s_i)_{i\in[1,n]}$ von V gegeben. Genau dann ist s eine Orthonormalbasis von V, wenn für $v, w \in V$ stets

$$\langle v, w\rangle = \langle \kappa_s(v), \kappa_s(w)\rangle$$

ist.

Beweis. Ist s eine Orthonormalbasis von V, so gilt

$$\langle v, w\rangle = \overline{\kappa_s(v)}^{\mathrm{tr}} \mathrm{G}_s(\langle -, =\rangle)\kappa_s(w) = \overline{\kappa_s(v)}^{\mathrm{tr}} \kappa_s(w) = \langle \kappa_s(v), \kappa_s(w)\rangle$$

für $v, w \in V$ nach Proposition (4.5). Gilt umgekehrt $\langle v, w\rangle = \langle \kappa_s(v), \kappa_s(w)\rangle$ für $v, w \in V$, so ist insbesondere

$$\langle s_i, s_j\rangle = \langle \kappa_s(s_i), \kappa_s(s_j)\rangle = \langle \mathrm{e}_i, \mathrm{e}_j\rangle = \delta_{i,j}$$

für $i, j \in [1, n]$ und damit s eine Orthonormalbasis von V. □

Orthogonalraum

(4.35) Bemerkung. Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$ und ein K-Skalarproduktraum V gegeben. Für jede Teilmenge S von V ist

$$S^\perp = \{v \in V \mid s \perp v \text{ für alle } s \in S\}$$

ein K-Untervektorraum von V.

Beweis. Für $v, w \in S^\perp$ gilt $s \perp v$ und $s \perp w$ für alle $s \in S$, also auch $s \perp v + w$ für alle $s \in S$ nach Proposition (4.27)(a) und damit $v + w \in S^\perp$. Es gilt $s \perp 0$ für alle $s \in S$ nach Proposition (4.27)(b) und damit $0 \in S^\perp$. Für $a \in K$, $v \in S^\perp$ gilt $s \perp v$ für alle $s \in S$, also auch $s \perp av$ für alle $s \in S$ nach Proposition (4.27)(c) und damit $av \in S^\perp$. Nach dem Untervektorraumkriterium (2.52) ist $S^\perp$ ein Untervektorraum von V. □

(4.36) Definition (Orthogonalraum)**.** Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$, ein K-Skalarproduktraum V und eine Teilmenge S von V gegeben. Der K-Untervektorraum

$$S^\perp = \{v \in V \mid s \perp v \text{ für alle } s \in S\}$$

von V aus Bemerkung (4.35) heißt *Orthogonalraum* zu S in V.

(4.37) Bemerkung. Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$ und ein K-Vektorraum mit Skalarprodukt V gegeben. Dann ist

$$\emptyset^\perp = V.$$

(4.38) Bemerkung. Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$, ein K-Skalarproduktraum V und Teilmengen S und T von V mit $S \subseteq T$ gegeben. Dann ist

$$T^\perp \subseteq S^\perp.$$

Beweis. Für $v \in T^\perp$ gilt $t \perp v$ für alle $t \in T$, wegen $S \subseteq T$ also insbesondere $s \perp v$ für alle $s \in S$ und damit $v \in S^\perp$. Folglich ist $T^\perp \subseteq S^\perp$. □

(4.39) Bemerkung. Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$, ein K-Skalarproduktraum V und eine Teilmenge S von V gegeben. Dann ist

$$S \subseteq (S^\perp)^\perp.$$

Beweis. Es sei $s \in S$ gegeben. Für alle $v \in S^\perp$ gilt $s \perp v$, also auch $v \perp s$ nach Bemerkung (4.26), d.h. es ist $s \in (S^\perp)^\perp$. Folglich ist $S \subseteq (S^\perp)^\perp$. □

(4.40) Proposition. Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$ und ein K-Skalarproduktraum V gegeben. Für jede Teilmenge S von V gilt

$$S^\perp = \langle S \rangle^\perp.$$

Beweis. Da nach Bemerkung (2.70) stets $S \subseteq \langle S \rangle$ ist, gilt $\langle S \rangle^\perp \subseteq S^\perp$ nach Bemerkung (4.38). Umgekehrt gilt für $v \in S^\perp$ stets $s \perp v$ für alle $s \in S$, also auch $w \perp v$ für alle $w \in \langle S \rangle = \sum_{s \in S} Ks$ nach Bemerkung (4.26) und Proposition (4.27), und damit $v \in \langle S \rangle^\perp$. Folglich ist auch $S^\perp \subseteq \langle S \rangle^\perp$. Insgesamt gilt $S^\perp = \langle S \rangle^\perp$. □

(4.41) Proposition. Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$ und ein K-Skalarproduktraum V gegeben. Dann ist

$$V^\perp = \{0\}.$$

Beweis. Es sei $v \in V^\perp$ gegeben. Dann gilt $w \perp v$ für alle $w \in V$, also insbesondere $v \perp v$. Dies bedeutet jedoch, dass $\langle v, v \rangle = 0$ ist, was bereits $v = 0$ impliziert. Da $V^\perp$ nach Bemerkung (4.35) ein Untervektorraum von V ist, gilt außerdem stets $0 \in V$. Folglich ist $V^\perp = \{0\}$. □

Das Gram-Schmidtsche Orthonormalisierungsverfahren

(4.42) Lemma. Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$, ein K-Skalarproduktraum V und ein endliches Orthonormalsystem S in V gegeben. Für $v \in V$ ist

$$v - \sum_{s \in S} \langle s, v \rangle s \in S^\perp.$$

Beweis. Es sei $v \in V$ gegeben. Für alle $t \in S$ gilt dann

$$\langle t, v - \sum_{s \in S} \langle s, v \rangle s \rangle = \langle t, v \rangle - \sum_{s \in S} \langle s, v \rangle \langle t, s \rangle = \langle t, v \rangle - \sum_{s \in S} \langle s, v \rangle \delta_{t,s} = \langle t, v \rangle - \langle t, v \rangle = 0,$$

also $t \perp v - \sum_{s \in S} \langle s, v \rangle s$. Folglich ist $v - \sum_{s \in S} \langle s, v \rangle s \in S^\perp$. □

Mit Hilfe dieses Lemmas lassen sich die Koeffizienten eines Vektors bezüglich einer Orthonormalbasis leicht bestimmen:

(4.43) Korollar (Parsevalscher Entwicklungssatz)**.** Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$, ein endlichdimensionaler K-Skalarproduktraum V und eine Orthonormalbasis S von V gegeben. Für $v \in V$ gilt

$$v = \sum_{s \in S} \langle s, v \rangle s.$$

Beweis. Es sei $v \in V$ gegeben. Nach Lemma (4.42) ist $v - \sum_{s\in S}\langle s, v\rangle s \in S^\perp$. Nun ist aber

$$S^\perp = \langle S\rangle^\perp = V^\perp = \{0\},$$

nach Proposition (4.40) und Proposition (4.41), also $v - \sum_{s\in S}\langle s, v\rangle s = 0$ und damit $v = \sum_{s\in S}\langle s, v\rangle s$. □

(4.44) Korollar (Parsevalsche Gleichung)**.** Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$, ein endlichdimensionaler K-Skalarproduktraum V und eine Orthonormalbasis S von V gegeben. Für $v \in V$ gilt

$$\|v\|^2 = \sum_{s\in S} |\langle s, v\rangle|^2.$$

Beweis. Nach dem Parsevalschen Entwicklungssatz, dem Satz des Pythagoras und der Absolut-Homogenität der Norm (4.20)(b) gilt für $v \in V$ stets

$$\|v\|^2 = \|\sum_{s\in S}\langle s, v\rangle s\|^2 = \sum_{s\in S}\|\langle s, v\rangle s\|^2 = \sum_{s\in S}|\langle s, v\rangle|^2\,\|s\|^2 = \sum_{s\in S}|\langle s, v\rangle|^2.$$ □

(4.45) Satz. Es seien $n \in \mathbb{N}_0$, $K \in \{\mathbb{R}, \mathbb{C}\}$, ein K-Skalarproduktraum V und eine linear unabhängige Familie $s = (s_j)_{j\in[1,n]}$ in V gegeben. Ferner seien n-Tupel $t' = (t'_j)_{j\in[1,n]}$ und $t = (t_j)_{j\in[1,n]}$ in V rekursiv definiert durch

$$t'_j := s_j - \sum_{i\in[1,j-1]} \frac{\langle t'_i, s_j\rangle}{\langle t'_i, t'_i\rangle} t'_i = s_j - \sum_{i\in[1,j-1]} \langle t_i, s_j\rangle t_i,$$
$$t_j := \frac{1}{\|t'_j\|} t'_j$$

für $j \in [1, n]$. Dann ist $t' = (t'_j)_{j\in[1,n]}$ orthogonal, $t = (t_j)_{j\in[1,n]}$ orthonormal und es gilt

$$\langle s_j \mid j \in [1, n]\rangle = \langle t'_j \mid j \in [1, n]\rangle = \langle t_j \mid j \in [1, n]\rangle.$$

Beweis. Wir führen Induktion nach n, wobei für $n = 0$ nichts zu zeigen ist. Es sei also $n \in \mathbb{N}$ und es gelte die Behauptung für $n - 1$. Nach Bemerkung (2.99) ist $(s_j)_{j\in[1,n-1]}$ linear unabhängig und damit $(t'_j)_{j\in[1,n-1]}$ orthogonal, $t = (t_j)_{j\in[1,n-1]}$ orthonormal und $\langle s_j \mid j \in [1, n-1]\rangle = \langle t'_j \mid j \in [1, n-1]\rangle = \langle t_j \mid j \in [1, n-1]\rangle$ nach Induktionsvoraussetzung. Ferner ist

$$t'_n = s_n - \sum_{i\in[1,n-1]} \langle t_i, s_n\rangle t_i \in \langle t_j \mid j \in [1, n-1]\rangle^\perp = \langle t'_j \mid j \in [1, n-1]\rangle^\perp$$

nach Lemma (4.42), es gilt also $t'_j \perp t'_n$ für $j \in [1, n-1]$. Folglich ist sogar $t' = (t'_j)_{j\in[1,n]}$ orthogonal und $t = (t_j)_{j\in[1,n]}$ orthonormal nach Proposition (4.27)(c) und Bemerkung (4.24). Nach Proposition (2.82) und Proposition (2.84) gilt schließlich

$$\langle s_j \mid j \in [1, n]\rangle = \langle \{t'_j \mid j \in [1, n-1]\} \cup \{s_n\}\rangle = \langle \{t'_j \mid j \in [1, n-1]\} \cup \{s_n - \sum_{i\in[1,n-1]} \frac{\langle t'_i, s_j\rangle}{\langle t'_i, t'_i\rangle} t'_i\}\rangle$$
$$= \langle \{t'_j \mid j \in [1, n]\}\rangle = \langle \{t_j \mid j \in [1, n]\}\rangle.$$ □

(4.46) Korollar. Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$ und ein endlichdimensionaler K-Skalarproduktraum V gegeben. Dann gibt es eine Orthonormalbasis von V.

Beweis. Nach Korollar (2.122) gibt es eine Basis $s = (s_j)_{j\in[1,\dim V]}$ von V, welche als solche nach Bemerkung (2.108) insbesondere linear unabhängig ist. Es seien n-Tupel $t' = (t'_j)_{j\in[1,\dim V]}$ und $t = (t_j)_{j\in[1,\dim V]}$ in V rekursiv definiert durch

$$t'_j := s_j - \sum_{i\in[1,j-1]} \frac{\langle t'_i, s_j\rangle}{\langle t'_i, t'_i\rangle} t'_i = s_j - \sum_{i\in[1,j-1]} \langle t_i, s_j\rangle t_i,$$
$$t_j := \frac{1}{\|t'_j\|} t'_j$$

für $j \in [1, \dim V]$. Nach Satz (4.45) ist $t = (t_j)_{j\in[1,\dim V]}$ orthonormal, also insbesondere linear unabhängig nach Bemerkung (4.31). Ferner gilt auch $\langle t_j \mid j \in [1, \dim V]\rangle = \langle s_j \mid j \in [1, \dim V]\rangle = V$ nach Bemerkung (4.31), d.h. $t = (t_j)_{j\in[1,\dim V]}$ ist zudem ein Erzeugendensystem von V. Insgesamt ist $t = (t_j)_{j\in[1,\dim V]}$ nach Bemerkung (2.108) eine Basis von V. □

(4.47) Algorithmus (Gram-Schmidtsches Orthonormalisierungsverfahren)**.**

- Eingabe: linear unabhängiges n-Tupel $s = (s_j)_{j\in[1,n]}$ in einem Skalarproduktraum V über $K \in \{\mathbb{R}, \mathbb{C}\}$, wobei $n \in \mathbb{N}_0$
- Ausgabe: orthonormales n-Tupel $t = (t_j)_{j\in[1,n]}$ in V
- Verfahren:

```
function orthonormalbasis(s)
    for j from 1 to n do
        t'_j := s_j − Σ_{i∈[1,j−1]} ⟨t_i, s_j⟩ t_i;
        t_j := 1/‖t'_j‖ t'_j;
    end for;

    return t;
end function;
```

(4.48) Beispiel. Es seien $s = (s_1, s_2, s_3)$ und $t = (t_1, t_2, t_3)$ in $\mathbb{R}^{3\times 1}$ gegeben durch

$$s = (\begin{pmatrix}1\\2\\2\end{pmatrix}, \begin{pmatrix}1\\0\\1\end{pmatrix}, \begin{pmatrix}0\\-1\\1\end{pmatrix}),\ t = (\frac{1}{3}\begin{pmatrix}1\\2\\2\end{pmatrix}, \frac{1}{3}\begin{pmatrix}2\\-2\\1\end{pmatrix}, \frac{1}{3}\begin{pmatrix}-2\\-1\\2\end{pmatrix}).$$

Dann ist t eine Orthonormalbasis von $\mathbb{R}^{3\times 1}$ und es gilt $\langle s_1\rangle = \langle t_1\rangle$, $\langle s_1, s_2\rangle = \langle t_1, t_2\rangle$, $\langle s_1, s_2, s_3\rangle = \langle t_1, t_2, t_3\rangle$.

Beweis. Wir benutzen das Gram-Schmidtsche Orthonormalisierungsverfahren (4.47):

$$t'_1 := s_1 = \begin{pmatrix}1\\2\\2\end{pmatrix},$$
$$\langle t'_1, t'_1\rangle = 1^2 + 2^2 + 2^2 = 9,$$
$$\frac{1}{\|t'_1\|}t'_1 = \frac{1}{3}\begin{pmatrix}1\\2\\2\end{pmatrix} = t_1,$$
$$t'_2 := s_2 - \frac{\langle t'_1, s_2\rangle}{\langle t'_1, t'_1\rangle}t'_1 = \begin{pmatrix}1\\0\\1\end{pmatrix} - \frac{1\cdot 1 + 2\cdot 0 + 2\cdot 1}{9}\begin{pmatrix}1\\2\\2\end{pmatrix} = \frac{1}{3}\begin{pmatrix}2\\-2\\1\end{pmatrix},$$
$$\langle t'_2, t'_2\rangle = \frac{2^2 + (-2)^2 + 1^2}{3^2} = 1,$$
$$\frac{1}{\|t'_2\|}t'_2 = \frac{1}{3}\begin{pmatrix}2\\-2\\1\end{pmatrix} = t_2,$$
$$t'_3 := s_3 - \frac{\langle t'_1, s_3\rangle}{\langle t'_1, t'_1\rangle}t'_1 - \frac{\langle t'_2, s_3\rangle}{\langle t'_2, t'_2\rangle}t'_2$$
$$= \begin{pmatrix}0\\-1\\1\end{pmatrix} - \frac{1\cdot 0 + 2\cdot(-1) + 2\cdot 1}{9}\begin{pmatrix}1\\2\\2\end{pmatrix} - \frac{2\cdot 0 + (-2)\cdot(-1) + 1\cdot 1}{9}\begin{pmatrix}2\\-2\\1\end{pmatrix} = \frac{1}{3}\begin{pmatrix}-2\\-1\\2\end{pmatrix},$$
$$\langle t'_3, t'_3\rangle = \frac{(-2)^2 + (-1)^2 + 2^2}{3^2} = 1,$$
$$\frac{1}{\|t'_3\|}t'_3 = \frac{1}{3}\begin{pmatrix}-2\\-1\\2\end{pmatrix} = t_3.$$

□

Aufgaben

Aufgabe 103 (Orthogonalraum)**.** Es sei U der $\mathbb{R}$-Untervektorraum von $\mathbb{R}^{4\times 1}$ gegeben durch

$$U = \langle \begin{pmatrix} 0 \\ 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 0 \\ 1 \end{pmatrix} \rangle.$$

Bestimmen Sie eine Orthonormalbasis von U (bzgl. des eingeschränkten Skalarprodukts) und eine Basis von $U^\perp$.

Aufgabe 104 (reelles Skalarprodukt)**.** Es sei $A \in \mathbb{R}^{3\times 3}$ gegeben durch

$$A = \begin{pmatrix} 2 & -1 & 1 \\ -1 & 2 & -1 \\ 1 & -1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & -1 \\ 1 & -1 & 0 \end{pmatrix}^2.$$

(a) Zeigen Sie, dass A positiv definit ist.

(b) Es sei V der euklidische Vektorraum mit unterliegendem $\mathbb{R}$-Vektorraum $\mathbb{R}^{3\times 1}$ und dessen Skalarprodukt die Gram-Matrix A bzgl. der Standardbasis e hat. Bestimmen Sie eine Orthonormalbasis von V.

Aufgabe 105 (komplexes Skalarprodukt)**.** Es seien $A \in \mathbb{C}^{3\times 3}$ und $s = (s_1, s_2, s_3)$ in $\mathbb{C}^{3\times 1}$ gegeben durch

$$A = \begin{pmatrix} 1 & -\mathrm{i} & \mathrm{i} \\ \mathrm{i} & 2 & -1+\mathrm{i} \\ -\mathrm{i} & -1-\mathrm{i} & 3 \end{pmatrix}, \; s = (\begin{pmatrix} 2-\mathrm{i} \\ -1-\mathrm{i} \\ 0 \end{pmatrix}, \begin{pmatrix} 1-2\mathrm{i} \\ 1-2\mathrm{i} \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}).$$

Ferner sei V der unitäre Vektorraum mit unterliegendem $\mathbb{C}$-Vektorraum $\mathbb{C}^{3\times 1}$ und Skalarprodukt gegeben durch

$$\langle x, y\rangle = \beta_A(x, y) = \overline{x}^{\mathrm{tr}} A y$$

für $x, y \in \mathbb{C}^{3\times 1}$.

(a) Bestimmen Sie die Gram-Matrix von β_A zur Basis s.

(b) Bestimmen Sie mit Hilfe des Gram-Schmidtschen Orthonormalisierungsverfahrens eine Orthonormalbasis $t = (t_1, t_2, t_3)$ von V.

Aufgabe 106 (Rechnen in abstrakten euklidischen Vektorräumen)**.** Es seien ein euklidischer Vektorraum V und eine Basis $s = (s_1, s_2, s_3)$ von V gegeben. Ferner sei $A \in \mathbb{R}^{3\times 3}$ gegeben durch

$$A = \begin{pmatrix} 3 & -1 & 1 \\ -1 & 5 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

die Gram-Matrix des Skalarprodukts bzgl. s. Schließlich sei die Basis $t = (t_1, t_2, t_3)$ in V gegeben durch

$$t = (s_3, s_1 - s_3, s_1 + 2s_2 - s_3).$$

(a) Zeigen Sie, dass $s_2 \perp s_3$ und $s_2 \perp 5s_1 + s_2$ ist.

(b) Berechnen Sie die Gram-Matrix des Skalarprodukts bzgl. t.

Aufgabe 107 (Eigenwerte hermitescher Endomorphismen)**.** Es seien $K \in \{\mathbb{R}, \mathbb{C}\}$ und ein K-Skalarproduktraum V gegeben. Ein Endomorphismus φ von V heißt *hermitesch* (oder *selbstadjungiert*), falls

$$\langle \varphi(v), w\rangle = \langle v, \varphi(w)\rangle$$

ist. Ist $K = \mathbb{R}$, so heißt ein hermitescher Endomorphismus von V auch *symmetrisch*.
Nun sei ein hermitescher Endomorphismus φ von V gegeben. Zeigen Sie:

(a) Jeder Eigenwert von φ ist reell.

(b) Für alle verschiedene Eigenwerte a und b von φ, jeden Eigenvektor v von φ zum Eigenwert a und jeden Eigenvektor w von φ zum Eigenwert b ist $v \perp w$.