Lineare Algebra und Analytische Geometrie

Manuel Kauers

Institut für Algebra
Johannes Kepler Universität

Version: 16. Dezember 2015

Inhalt

Teil I

Algebraische Strukturen

1 Mengen

Die Aufgabe der Mathematik ist es, „Zusammenhänge“ zwischen „Eigenschaften“ von (abstrakten) „Objekten“ zu erkennen und zu beschreiben. Objekte sind z. B. Zahlen, Funktionen, Punkte usw. Eigenschaften sind z. B. gerade/ungerade, prim, negativ, stetig, usw. Ein Zusammenhang ist z. B. $x > y \wedge y > z \Rightarrow x > z$ (wenn x größer ist als y und y seinerseits größer als z, dann folgt daraus, dass x auch größer als z ist).

Objekte werden zu „Mengen“ (engl. *set*) zusammengefasst. („Sei A die Menge aller Objekte mit der Eigenschaft ...“.) Man schreibt $x \in A$, falls x ein Objekt ist, das die Eigenschaft hat und $x \notin A$, falls nicht. Im Fall $x \in A$ sagt man, x ist ein *Element* der Menge A.

Mengen sind selbst auch abstrakte Objekte, können also in anderen Mengen enthalten sein. Zum Beispiel gilt $1 \in \{1\}$, $\{1\} \in \{\{1\}\}$, jedoch $1 \notin \{\{1\}\}$ und $\{1\} \notin \{1\}$.

Bei der Konstruktion von Mengen muss man aufpassen, dass man sich nicht in Widersprüche verwickelt.

Beispiel. Sei A die Menge aller Mengen M mit der Eigenschaft $M \notin M$. Für die Menge A gilt dann

$$A \in A \iff A \notin A$$

Also: A ist genau dann selbst in A enthalten, wenn A nicht in A enthalten ist.

Das kann nicht sein. Haben wir hier etwas verbotenes getan? Für Juristen gilt der Grundsatz *Was nicht explizit verboten ist, ist erlaubt.* In der Mathematik gilt dagegen: *Was nicht explizit erlaubt ist, ist verboten!* Wir müssen also, wenn wir mit Mengen hantieren wollen, vorher festlegen, welche Gesetze für die Theorie der Mengen gelten sollen. Die folgenden haben sich als zweckmäßig erwiesen:

Axiom.

1. Sind $a_1, \dots, a_n$ endlich viele Objekte, dann existiert eine Menge A mit der Eigenschaft

   $$x \in A \iff x = a_1 \vee x = a_2 \vee \cdots \vee x = a_n.$$

   Notation: $\{a_1, \dots, a_n\} := A$. Im Fall $n = 0$ schreibt man $\emptyset := \{\}$ und nennt diese Menge die *leere Menge.*

2. Die Menge $\mathbb{N} := \{0, 1, 2, \dots\}$ der natürlichen Zahlen existiert.

3. Ist A eine Menge von Mengen (d. h. jedes Element von A ist eine Menge), so existieren die Mengen $\bigcup_{a \in A} a$ und $\bigcap_{a \in A} a$ mit

   $$x \in \bigcup_{a \in A} a \iff \exists\, a \in A : x \in a,$$
   $$x \in \bigcap_{a \in A} a \iff \forall\, a \in A : x \in a.$$

   Die Menge $\bigcup_{a \in A} a$ heißt die *Vereinigung* (engl. *union*) der Mengen in A, die Menge $\bigcap_{a \in A} a$ heißt der *Schnitt* (engl. *intersection*) der Mengen in A. Ist $A = \{a_1, \dots, a_n\}$ eine endliche Menge von Mengen, so schreibt man statt $\bigcup_{a \in A} a$ und $\bigcap_{a \in A} a$ auch $\bigcup_{i=1}^{n} a_i$ oder $a_1 \cup a_2 \cup \cdots \cup a_n$ bzw. $\bigcap_{i=1}^{n} a_i$ oder $a_1 \cap \cdots \cap a_n$.

4. Seien A, B Mengen, $f\colon A \to B$ eine Funktion (siehe Abschnitt 3), und $p\colon A \to \{\mathrm{T}, \mathrm{F}\}$. Dann existiert eine Menge C mit

$$y \in C \iff \exists\, x \in A : p(x) = \mathrm{T} \wedge f(x) = y.$$

   Notation: $\{\, f(x) : x \in A \wedge p(x) \,\} := C$; im Fall $f = \mathrm{id}$ auch $\{\, x \in A : p(x) \,\} := C$.

5. Seien $A_1, \ldots, A_n$ Mengen. Dann existiert auch die Menge C mit

$$z \in C \iff \exists\, x_1 \in A_1 \ \cdots\ \exists\, x_n \in A_n : z = (x_1, \ldots, x_n)$$

   Dabei ist $(x_1, \ldots, x_n)$ das *Tupel* bestehend aus den *Komponenten* $x_1, \ldots, x_n$. Notation: $A_1 \times A_2 \cdots \times A_n := C$. Man nennt die Menge C das *kartesische Produkt* der Mengen $A_1, \ldots, A_n$. Statt $A \times A \times \cdots \times A$ schreibt man auch A^n.

Beispiel.

1. $\{1, 1, 2\} = \{1, 2\} = \{2, 1\} = \{1, 2, 2, 2, 2, 1\}$
2. $\{1, 3, 4, 5\} \cup \{3, 5, 7, 8\} = \{1, 3, 4, 5, 7, 8\}$
3. $\{1, 3, 4, 5\} \cap \{3, 5, 7, 8\} = \{3, 5\}$
4. $\{\, x^2 : x \in \mathbb{N} \wedge x \text{ prim} \,\} = \{4, 9, 25, 49, 121, \ldots\}$
5. $\{\, \text{Geburtsdatum}(S) : S \text{ ist Vorlesungsteilnehmer} \,\}$
6. $\{1, 2\} \times \{a, b\} = \{(1, a), (2, a), (1, b), (2, b)\}$
7. $\{a, b\} \times \{1, 2\} = \{(a, 1), (a, 2), (b, 1), (b, 2)\}$

Definition 1. Seien A, B Mengen.

1. Die Mengen A, B heißen *(zueinander) gleich* (engl. *equal*), geschrieben $A = B$, falls gilt

$$\forall\, x : (x \in A \iff x \in B).$$

2. A heißt *Teilmenge* (engl. *subset*) von B, notiert $A \subseteq B$, falls $\forall\, x : x \in A \Rightarrow x \in B$.
3. A heißt *Obermenge* (engl. *superset*) von B, notiert $A \supseteq B$, falls $\forall\, x : x \in B \Rightarrow x \in A$.
4. A und B heißen *(zueinander) disjunkt* (engl. *disjoint*), falls $A \cap B = \emptyset$.
5. $A \setminus B := \{\, a \in A : a \notin B \,\}$ heißt das *Komplement* von B in A.

Satz 1. Seien A, B, C Mengen.

1. Wenn $A \subseteq B$ und $B \subseteq C$, dann $A \subseteq C$
2. $A = B \iff A \subseteq B \wedge B \subseteq A$
3. Ist $B \neq \emptyset$ eine Menge von Mengen, so gilt $A \cap \bigcup_{b \in B} b = \bigcup_{b \in B}(A \cap b)$
4. Ist $B \neq \emptyset$ eine Menge von Mengen, so gilt $A \cup \bigcap_{b \in B} b = \bigcap_{b \in B}(A \cup b)$
5. Ist $B \neq \emptyset$ eine Menge von Mengen, so gilt $A \setminus \bigcap_{b \in B} b = \bigcup_{b \in B}(A \setminus b)$ und $A \setminus \bigcup_{b \in B} b = \bigcap_{b \in B}(A \setminus b)$.
6. $A \cap B \subseteq A \subseteq A \cup B$
7. $A = B \iff B = A$, $A \cap B = B \cap A$, $A \cup B = B \cup A$

Beweis.

1. Annahmen: $A \subseteq B$ und $B \subseteq C$

   zu zeigen: $A \subseteq C$.

   Sei $x \in A$ beliebig. Nach Annahme $A \subseteq B$ folgt per Definition von „$\subseteq$“, dass $x \in B$. Daraus folgt nach Annahme $B \subseteq C$ per Definition von „$\subseteq$“, dass $x \in C$.

   Da x ein beliebiges Objekt von A war, ist also gezeigt: $\forall\, x : (x \in A \Rightarrow x \in C)$. Also gilt $A \subseteq C$, was zu zeigen war.

2. Aussagen der Form $A \iff B$ zeigt man, indem man zunächst $A \Rightarrow B$ und dann $B \Rightarrow A$ zeigt.

   „$\Rightarrow$“ Annahme: $A = B$

   zu zeigen: $A \subseteq B \wedge B \subseteq A$.

   Aus Symmetriegründen genügt es, $A \subseteq B$ zu zeigen. Das Argument für $B \subseteq A$ geht dann genauso.

   Sei $x \in A$ beliebig. Nach Annahme $A = B$ und per Definition von „$=$“ gilt $x \in B$. Da x beliebig war, folgt $x \in B$.

   „$\Leftarrow$“ Annahmen: $A \subseteq B$ und $B \subseteq A$.

   zu zeigen: $A = B$.

   Nach Definition von „$=$“ ist zu zeigen $\forall\, x : (x \in A \iff x \in B)$.

   Sei x ein beliebiges Objekt. Aus der Annahme $A \subseteq B$ folgt $x \in A \Rightarrow x \in B$ und aus der Annahme $B \subseteq A$ folgt $x \in B \Rightarrow x \in A$. Beides zusammen gibt $x \in A \iff x \in B$.

3. Wegen Punkt 2 kann man die Gleichheit zweier Mengen zeigen, indem man zeigt, dass jede eine Teilmenge der anderen ist.

   „$\subseteq$“ Sei $x \in A \cap \bigcup_{b \in B} b$ beliebig. Wir zeigen $x \in \bigcup_{b \in B}(A \cap b)$.

   Dazu ist zu zeigen $\exists\, b \in B : x \in A \cap b$. Nach Annahme gilt $x \in A$ und $x \in \bigcup_{b \in B} b$, d. h. $\exists\, b \in B : x \in b$.

Wähle ein $b \in B$ mit $x \in b$. Dann ist wegen $x \in A$ auch $x \in A \cap b$. Es folgt $\exists\, b \in B : x \in A \cap b$, und damit die Behauptung.

„$\supseteq$“ Sei $x \in \bigcup_{b\in B}(A \cap b)$ beliebig. Wir zeigen $x \in A \cap \bigcup_{b\in B} b$.

Dazu ist zu zeigen $x \in A$ und $x \in \bigcup_{b\in B} b$, d. h. $\exists\, b \in B : x \in b$.

Wähle $b \in B$ mit $x \in A \cap b$. Dann gilt $x \in A$ und $x \in b$. Also $\exists\, b \in B : x \in b$, also $x \in \bigcup_{b\in B} b$, also $x \in A \cap \bigcup_{b\in B} b$.

4. „$\subseteq$“ Sei $x \in A \cup \bigcap_{b\in B} b$ beliebig. Wir zeigen $x \in \bigcap_{b\in B}(A \cup b)$.

   Dazu ist zu zeigen $\forall\, b \in B : x \in A \cup b$. Nach Annahme gilt $x \in A$ oder $x \in \bigcap_{b\in B} b$, d. h. $\forall\, b \in B : x \in b$.

   Für beliebiges $b \in B$ gilt also $x \in A$ oder $x \in b$, also $x \in A \cup b$. Da $b \in B$ beliebig war, folgt $\forall\, b \in B : x \in A \cup b$, und damit die Behauptung.

   „$\supseteq$“ Sei $x \in \bigcap_{b\in B}(A \cup b)$ beliebig. Wir zeigen $x \in A \cup \bigcap_{b\in B} b$.

   Dazu ist zu zeigen $x \in A$ oder $x \in \bigcap_{b\in B} b$, d. h. $x \in A$ oder $\forall\, b \in B : x \in b$. Wir zeigen: Wenn $x \notin A$ ist, dann muss $\forall\, b \in B : x \in b$ gelten.

   Sei $b \in B$ beliebig. Dann gilt nach Voraussetzung $x \in A \cup b$, und daraus folgt $x \in A$ oder $x \in b$. Nach Annahme gilt $x \notin A$, also $x \in b$. Da b beliebig war, folgt also $\forall\, b \in B : x \in b$, und damit die Behauptung.

5., 6., 7. Übung. ∎

Beispiel. $A = \{x, y, z\}$, $B = \{1, 2, 3, 4\}$

$$A \left\{ \begin{array}{c|cccc} x & (x,1) & (x,2) & (x,3) & (x,4) \\ y & (y,1) & (y,2) & (y,3) & (y,4) \\ z & (z,1) & (z,2) & (z,3) & (z,4) \end{array} \right\} A \times B$$

$$\begin{array}{c|c} & \underbrace{1 \qquad 2 \qquad 3 \qquad 4}_{B} \end{array}$$

Satz 2. Seien A, B, C Mengen.

1. $(A \cap B) \times C = (A \times C) \cap (B \times C)$
2. $(A \cup B) \times C = (A \times C) \cup (B \times C)$

Beweis.

1. „$\subseteq$“ Sei $x \in (A \cap B) \times C$ beliebig. Zu zeigen: $x \in (A \times C) \cap (B \times C)$.

   Nach Definition von $\times$ gilt $x = (x_1, x_2)$ für gewisse x_1, x_2 mit $x_1 \in A \cap B$ und $x_2 \in C$. Aus $x_1 \in A \cap B$ folgt $x_1 \in A$ und $x_1 \in B$. Demnach gilt $(x_1, x_2) \in A \times C$ und $(x_1, x_2) \in B \times C$, also $(x_1, x_2) \in (A \times C) \cap (B \times C)$.

   „$\supseteq$“ Sei $x \in (A \cap C) \times (B \times C)$ beliebig. Zu zeigen: $x \in (A \cap B) \times C$.

Nach Definition gilt $x \in A \times C$ und $x \in B \times C$.

$$\begin{array}{ccc} \Downarrow & & \Downarrow \\ x = (x_1, x_2) \text{ mit} & & x = (x_1, x_2) \text{ mit} \\ x_1 \in A, x_2 \in C & & x_1 \in B, x_2 \in C \end{array}$$

$$\Rightarrow \quad \underbrace{x_1 \in A \wedge x_1 \in B}_{\Downarrow} \wedge x_2 \in C$$

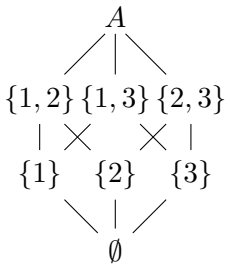
$$\Rightarrow \quad x_1 \in A \cap B$$

$$\Rightarrow \quad x = (x_1, x_2) \in (A \cap B) \times C$$

2. Übung. ∎

Axiom. Sei A eine Menge. Dann existiert eine Menge B mit $\forall\, x : x \in B \iff x \subseteq A$. Man schreibt $\mathcal{P}(A) := B$ und nennt diese Menge die *Potenzmenge* (engl. *power set*) von A.

Beispiel. Für $A = \{1, 2, 3\}$ ist $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.



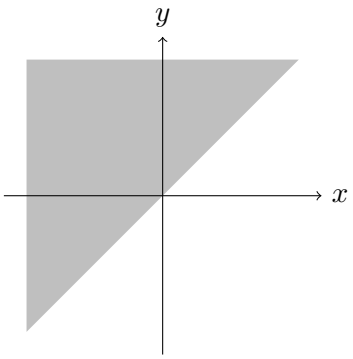
Ein weiteres Axiom zur Mengenlehre kommt später in Abschnitt 14. Darüber hinaus gibt es einige weitere, die wir nicht brauchen werden, zum Beispiel eines, das besagt, dass jede Kette $a \in b$, $b \in c$, $c \in d$, $d \in e$, ... nach endlich vielen Schritten abbrechen muss, d. h. die „Schachtelungstiefe“ bei Mengen von Mengen von Mengen von... darf nicht unendlich werden.

2 Relationen

Definition 2. Sei A eine Menge. Eine Teilmenge $R \subseteq A \times A$ heißt *Relation* auf A. Statt $(x, y) \in R$ schreibt man xRy.

Beispiel.

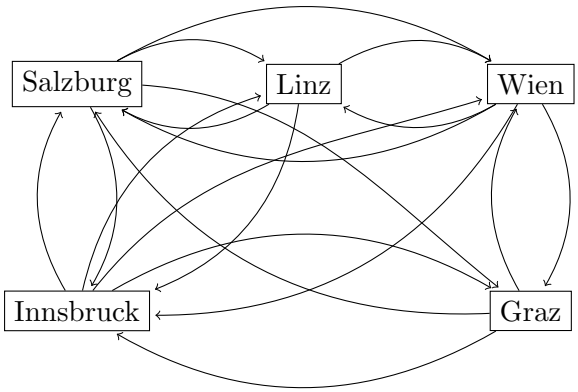
1. $\leq = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x \text{ ist kleiner oder gleich } y\}$



2. A die Menge aller Städte in Österreich mit mehr als 100000 Einwohnern (2015).

   R die Menge aller $(x, y) \in A \times A$ für die gilt: es gibt eine direkte Zugverbindung von x nach y.

   In der Informatik nennt man so etwas einen *Graph*. Ein Graph ist also ein Paar $G = (V, E)$, wobei V eine Menge und E eine Relation auf V ist. Elemente von V nennt man *Knoten* (engl. *vertex*) und Elemente von E *Kanten* (engl. *edge*).



3. A die Menge der Teilnehmer der Vorlesungsklausur,

   R die Menge aller $(x, y) \in A \times A$ für die gilt, dass x und y die gleiche Note bekommen.

4. *Teilbarkeit* (engl. *divisibility*): $A = \mathbb{Z}$, $R = \{(x, y) \in A \times A : \exists\, z \in \mathbb{Z} : x \cdot z = y\}$. Statt xRy schreibt man typischerweise $x \mid y$. Zum Beispiel gilt $3 \mid 15$, aber $4 \nmid 15$.

5. $\subseteq$ ist eine Relation auf $\mathcal{P}(A)$:

$$\subseteq = \{(U, V) \in \mathcal{P}(A) \times \mathcal{P}(A) : U \subseteq V\}$$

6. M die Menge aller Menschen, $\heartsuit := \{(x, y) \in M \times M : x \text{ mag } y\}$, z. B. Heinz $\heartsuit$ Erika.

Definition 3. Sei A eine Menge und R eine Relation auf A.

1. R heißt *reflexiv,* falls gilt $\forall\, x \in A : xRx$ und *irreflexiv,* falls gilt $\forall\, x \in A : \neg(xRx)$.
2. R heißt *symmetrisch,* falls gilt:

   $$\forall\, x, y \in A : xRy \Rightarrow yRx$$

   und *antisymmetrisch,* falls

   $$\forall\, x, y \in A : (xRy \wedge yRx) \Rightarrow x = y$$

3. R heißt *transitiv,* falls gilt

   $$\forall\, x, y, z \in A : (xRy \wedge yRz) \Rightarrow xRz.$$

4. R heißt *total,* falls gilt

   $$\forall\, x, y \in A : xRy \vee yRx$$

Beispiel. Die Relationen aus dem vorangegangenen Beispiel haben folgende Eigenschaften:

Bsp	1	2	3	4	5	6
reflexiv	ja	nein	ja	ja	ja	unklar
irreflexiv	nein	ja	nein	nein	nein	nein
symmetrisch	nein	ja	ja	nein	nein	nein
antisymmetrisch	ja	nein	nein	ja	ja	nein
transitiv	ja	nein	ja	ja	ja	nein
total	ja	nein	nein	nein	nein	nein

Definition 4. Sei A eine Menge und $R \subseteq A \times A$ eine Relation auf A. Wenn R reflexiv, transitiv und antisymmetrisch ist, dann heißt R eine *Halbordnung* auf A. Ist R außerdem total, so heißt R *(Total-)Ordnung* (engl. *order(ing)*) auf A.

Beispiel.

1. $\subseteq$, $\leq$ und $|$ sind Halbordnungen auf $\mathcal{P}(A), \mathbb{R}, \mathbb{N}$. $\leq$ ist sogar eine Totalordnung, aber $|$ und $\subseteq$ sind es nicht.
2. Auf $M = \mathbb{Z} \times \mathbb{Z}$ wird eine Halbordnung $\leq$ definiert durch

   $$(a_1, a_2) \leq (b_1, b_2) :\Longleftrightarrow a_1 \leq b_1 \wedge a_2 \leq b_2,$$

   wobei mit $\leq$ auf der rechten Seite die übliche Ordnung auf $\mathbb{Z}$ gemeint ist.

   Es gilt dann zum Beispiel $(3, 5) \leq (7, 8)$. Bei dieser Halbordnung handelt es sich nicht um eine Totalordnung, weil zum Beispiel die Elemente $(3, 7)$ und $(5, 3)$ nicht miteinander vergleichbar sind, d.h. es gilt weder $(3, 7) \leq (5, 3)$ noch $(5, 3) \leq (3, 7)$.

Definition 5. Sei A eine Menge und $R \subseteq A \times A$ eine Relation auf A. Wenn R reflexiv, symmetrisch und transitiv ist, dann heißt R eine *Äquivalenzrelation.*

Beispiel.

1. Für jede Menge A ist die Gleichheitsrelation $=$ eine Äquivalenzrelation, denn für alle Objekte x, y, z gilt $x = x$ (Reflexivität), $x = y \iff y = x$ (Symmetrie) und $x = y \wedge y = z \Rightarrow x = z$ (Transitivität).

   Im allgemeinen darf man sich eine Äquivalenzrelation vorstellen als eine abgeschwächte Variante der Gleichheitsrelation, bei der bestimmte irrelevante Eigenschaften ignoriert werden.

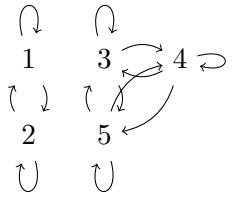
2. Sei $A = \{\square, \blacksquare, \square, \square, \blacksquare, \circ, \bullet, \bullet, \bullet, \triangle, \blacktriangle, \blacktriangle, \triangle\}$. Man kann sich für diese Menge verschiedene Äquivalenzrelationen vorstellen. Hier sind ein paar Möglichkeiten:

   - $x \sim y$, falls x und y die gleiche Form haben – dann gilt z. B. $\square \sim \blacksquare$ und $\square \not\sim \circ$.
   - $x \sim y$, falls x und y die gleiche Farbe haben – dann gilt z. B. $\square \sim \circ$ und $\square \not\sim \blacksquare$.
   - $x \sim y$, falls x und y die gleiche Höhe haben – dann gilt z. B. $\square \sim \blacktriangle$ und $\square \not\sim \triangle$.
   - $x \sim y$, falls x und y sich höchstens in der Farbe unterscheiden – dann gilt z. B. $\square \sim \blacksquare$ und $\square \not\sim \bullet$.

3. Sei $m \in \mathbb{Z}$ und $\equiv_m := \{\, (x, y) \in \mathbb{Z}^2 : m \mid x - y \,\}$. Dann ist $\equiv_m$ eine Äquivalenzrelation auf $\mathbb{Z}$. Es gilt zum Beispiel:

$$\begin{aligned} 0 \equiv_3 3 \equiv_3 6 \equiv_3 \ 9 \equiv_3 -3 \equiv_3 -6 \equiv_3 15 \equiv_3 \cdots \\ 1 \equiv_3 4 \equiv_3 7 \equiv_3 10 \equiv_3 -2 \equiv_3 -5 \equiv_3 16 \equiv_3 \cdots \\ 2 \equiv_3 5 \equiv_3 8 \equiv_3 11 \equiv_3 -1 \equiv_3 -4 \equiv_3 17 \equiv_3 \cdots \end{aligned}$$

4. Die Kantenmenge V des Graphs $G = (E, V)$, der durch folgendes Diagramm gegeben ist, ist eine Äquivalenzrelation auf $E = \{1, 2, 3, 4, 5\}$.



5. Ist A die Menge aller Schüler einer Volksschule und

$$R = \{(x, y) \in A \times A : x \text{ und } y \text{ gehen in dieselbe Klasse}\},$$

   dann ist R eine Äquivalenzrelation auf A. Klassenbildung ist symptomatisch für Äquivalenzrelationen.

Definition 6. Ist $\sim$ eine Äquivalenzrelation auf A und ist $x \in A$, so heißt

$$[x]_\sim := \{y \in A : x \sim y\}$$

die *Äquivalenzklasse* von x (bezüglich $\sim$). Man schreibt $A/\sim := \{\, [x]_\sim : x \in A \,\}$ für die Menge aller Äquivalenzklassen von Elementen von A.

Beispiel. Was sind bei den Äquivalenzrelationen aus dem vorherigen Beispiel die Äquivalenzklassen?

1. Bezüglich $=$ ist die Äquivalenzklasse eines Elementes $x \in A$ genau die Menge $\{x\}$, die nur dieses Element enthält.

2. Die genannten Äquivalenzrelationen auf $A = \{\square, \blacksquare, \square, \square, \blacksquare, \circ, \bullet, \bullet, \bullet, \triangle, \blacktriangle, \blacktriangle, \triangle\}$ teilen A in folgende Äquivalenzklassen auf:

   - gleiche Form: $\{\square, \blacksquare, \square, \square, \blacksquare\}$, $\{\circ, \bullet, \bullet, \bullet\}$, $\{\triangle, \blacktriangle, \blacktriangle, \triangle\}$
   - gleiche Farbe: $\{\square, \square, \circ, \triangle, \triangle\}$, $\{\blacksquare, \blacksquare, \bullet, \bullet, \blacktriangle\}$, $\{\square, \bullet, \blacktriangle\}$
   - gleiche Höhe: $\{\square, \blacksquare, \square, \circ, \triangle, \blacktriangle, \blacktriangle\}$, $\{\square, \blacksquare, \bullet, \bullet, \triangle\}$
   - gleich bis auf Farbe: $\{\square, \blacksquare, \square\}$, $\{\square, \blacksquare\}$, $\{\circ, \bullet\}$, $\{\bullet, \bullet\}$, $\{\triangle, \blacktriangle, \blacktriangle\}$, $\{\triangle\}$

3. Die beiden Zusammenhangskomponenten $\{1, 2\}$ und $\{3, 4, 5\}$ sind die Äquivalenzklassen.

4. Wir haben

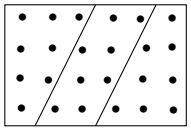
$$\begin{aligned}
[0]_{\equiv_3} &= \{\ldots, -3, 0, 3, 6, 9, \ldots\} \\
[1]_{\equiv_3} &= \{\ldots, -2, 1, 4, 7, 10, \ldots\} \\
[2]_{\equiv_3} &= \{\ldots, -1, 2, 5, 8, 11, \ldots\} \\
[3]_{\equiv_3} &= [0]_{\equiv_3} \\
[4]_{\equiv_3} &= [1]_{\equiv_3}
\end{aligned}$$

   und so weiter.

5. In diesem Fall sind die Äquivalenzklassen genau die Schulklassen.

Satz 3. Es seien A eine Menge, $\sim$ eine Äquivalenzrelation auf A, und $x, y \in A$. Dann gilt:

1. $x \sim y \iff [x]_\sim = [y]_\sim$
2. $x \not\sim y \iff [x]_\sim \cap [y]_\sim = \emptyset$
3. $A = \bigcup_{C \in A/\sim} C$



Beweis.

1. „⇒“ Annahme $x \sim y$, zu zeigen: $[x]_\sim = [y]_\sim$.

   Aus Symmetriegründen genügt es, $[x]_\sim \subseteq [y]_\sim$ zu zeigen.

   Sei also $z \in [x]_\sim$. Dann gilt:

$$\begin{aligned} z \in [x]_\sim &\overset{\text{Def.}}{\Longrightarrow} x \sim z \\ &\overset{\text{Sym.}}{\Longrightarrow} z \sim x \\ &\overset{\text{Ann. + Trans.}}{\Longrightarrow} z \sim y \\ &\overset{\text{Sym.}}{\Longrightarrow} y \sim z \\ &\overset{\text{Def.}}{\Longrightarrow} z \in [y]_\sim. \end{aligned}$$

   „⇐“ Annahme: $[x]_\sim = [y]_\sim$, zu zeigen: $x \sim y$.

   Wegen Reflexivität gilt jedenfalls $x \in [x]_\sim$. Wegen $[x]_\sim = [y]_\sim$ also auch $y \in [x]_\sim$, und damit nach Definition auch $x \sim y$.

2. „⇒“ Annahme: $x \not\sim y$, zu zeigen: $[x]_\sim \cap [y]_\sim = \emptyset$.

   Widerspruchsbeweis: wäre $[x]_\sim \cap [y]_\sim \neq \emptyset$, so gäbe es ein $z \in [x]_\sim \cap [y]_\sim$. Für dieses z gilt dann $z \sim x$ und $z \sim y$, also wegen Symmetrie und Transitivität auch $x \sim y$, im Widerspruch zur Annahme $x \not\sim y$.

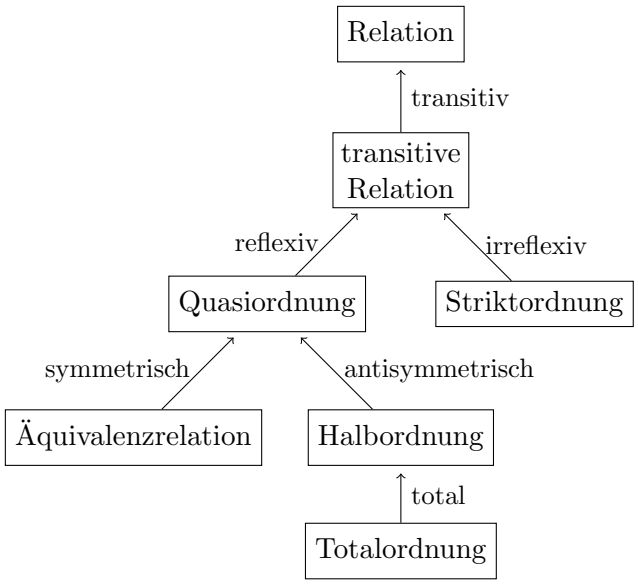
   „⇐“ Annahme: $[x]_\sim \cap [y]_\sim = \emptyset$, zu zeigen: $x \not\sim y$.

   Wäre $x \sim y$, dann wäre $[x]_\sim = [y]_\sim$ nach Teil 1, also $[x]_\sim \cap [y]_\sim = [x]_\sim \neq \emptyset$, da zumindest $x \in [x]_\sim$ (wegen Reflexivität). Damit ist $x \sim y$ ausgeschlossen und es bleibt nur $x \not\sim y$.

3. „⊆“ Sei $y \in A$. Zu zeigen: $y \in \bigcup_{[x]_\sim \in A/\sim} [x]_\sim$. Das folgt direkt aus $y \in [y]_\sim \in A/\sim$.

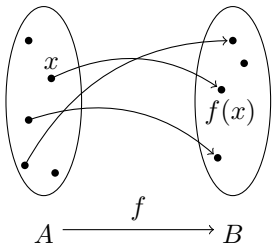
   „⊇“ Sei $y \in \bigcup_{[x]_\sim \in A/\sim} [x]_\sim$. Dann gibt es ein $[x]_\sim \in A/\sim$ mit $y \in [x]_\sim$. Wegen $[x]_\sim \subseteq A$ folgt $y \in A$. ∎

Wir haben in Definition 3 verschiedene Eigenschaften eingeführt, die eine Relation haben kann oder auch nicht. In den Definitionen 4 und 5 haben wir Relationen betrachtet, die mehrere dieser Eigenschaften zugleich erfüllen. Eine Übersicht über weitere Arten von Relationen und ihre Beziehungen zueinander gibt das folgende Diagramm. Ein Pfeil $A \overset{e}{\to} B$ zwischen zwei Relationsarten bedeutet, dass jede Relation vom Typ A eine Relation vom Typ B mit der Eigenschaft e ist.



3 Funktionen

Idee: Objekte anderen Objekten zuordnen.



Definition 7. Seien A, B Mengen und $R \subseteq A \times B$.

1. R heißt *linkseindeutig,* falls gilt:

$$\forall\ (x_1, y_1), (x_2, y_2) \in R : y_1 = y_2 \Rightarrow x_1 = x_2$$

2. R heißt *rechtseindeutig,* falls gilt:

$$\forall\ (x_1, y_1), (x_2, y_2) \in R : x_1 = x_2 \Rightarrow y_1 = y_2$$

3. R heißt *linkstotal,* falls gilt:

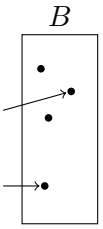
$$\forall\ x \in A\ \exists\ y \in B : (x, y) \in R$$

4. R heißt *rechtstotal,* falls gilt:

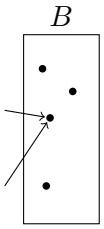
$$\forall\ y \in B\ \exists\ x \in A : (x, y) \in R$$

Beispiel.

1. Linkseindeutig:

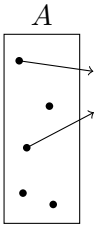


erlaubt

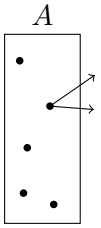


nicht erlaubt

2. Rechtseindeutig:

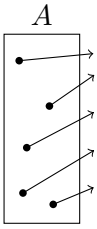


erlaubt

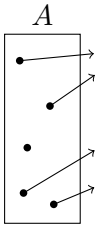


nicht erlaubt

3. Linkstotal:

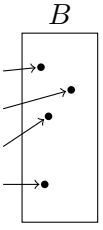


erlaubt

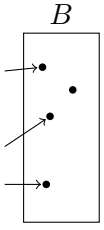


nicht erlaubt

4. Rechtstotal:



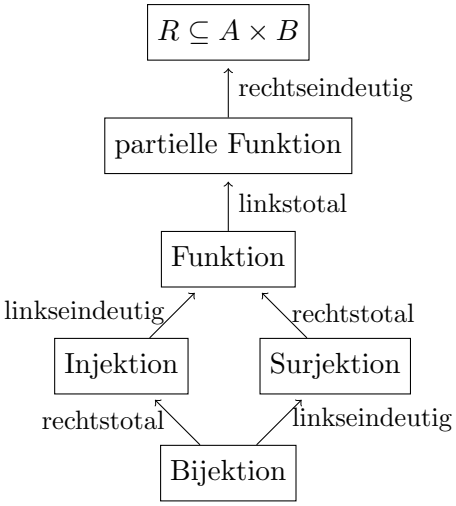
erlaubt



nicht erlaubt

Definition 8. Seien A, B Mengen, $R \subseteq A \times B$.

1. Ist R rechtseindeutig, so heißt R eine *partielle Funktion* und statt $(x, y) \in R$ schreibt man $y = R(x)$.
2. Ist R außerdem linkstotal, so heißt R *Funktion* oder *Abbildung* (engl. *map*) und statt $R \subseteq A \times B$ schreibt man $R\colon A \to B$. Für die Menge aller Funktionen $R\colon A \to B$ schreibt man B^A.
3. Eine linkseindeutige Funktion heißt *injektiv*.
4. Eine rechtstotale Funktion heißt *surjektiv*.
5. Eine Funktion, die sowohl injektiv als auch surjektiv ist, heißt *bijektiv*.



Beispiel.

1. Die *Identitätsfunktion* $\mathrm{id}_A\colon A \to A$ mit $\mathrm{id}_A(x) = x$ für alle $x \in A$ ist eine Funktion.
2. $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = \frac{1}{x}$ ist eine partielle Funktion, aber keine Funktion. Man sollte deshalb besser schreiben $f = \{(x, y) \in \mathbb{R}^2 : y = \frac{1}{x}\}$.
3. $f\colon \mathbb{R} \setminus \{0\} \to \mathbb{R}$, $f(x) = \frac{1}{x}$ ist eine Funktion.

   Diese Funktion ist injektiv. Zum Beweis betrachtet man $x_1, x_2 \in \mathbb{R} \setminus \{0\}$ mit $f(x_1) = f(x_2)$ und zeigt, dass dann $x_1 = x_2$ sein muss. In der Tat bedeutet $f(x_1) = f(x_2)$, dass $\frac{1}{x_1} = \frac{1}{x_2}$, und also $x_1 = x_2$, wie gefordert.
4. $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$ ist eine Funktion.

   Diese Funktion ist nicht injektiv, weil z. B. $y = 4$ zwei verschiedene Urbilder hat (nämlich $x = 2$ und $x = -2$).

   Sie ist auch nicht surjektiv, weil z. B. $y = -1$ gar kein Urbild hat.
5. $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = \mathrm{e}^x$ ist injektiv, aber nicht surjektiv.

6. $f\colon \mathbb{R} \to \{\, x \in \mathbb{R} : x > 0 \,\}$, $f(x) = \mathrm{e}^x$ ist injektiv und surjektiv, also bijektiv.

7. $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x + \frac{1}{1+x^2}$ ist surjektiv, aber nicht injektiv.

8. $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^3$ ist bijektiv.

Für eine Funktion ist es nicht wesentlich, dass man sie durch einen Funktionsausdruck beschreiben kann. Tatsächlich lassen sich fast alle Funktionen nicht durch eine endlich große Formel beschreiben. Auch (und vor allem) solche Funktionen sind immer mitgemeint, wenn es heißt „Sei f eine (beliebige) Funktion“.

Eine bijektive Funktion von A nach B existiert offenbar genau dann, wenn A und B gleich viele Elemente haben. Man spricht bei einer Bijektion deshalb auch von einer 1:1-Zuordnung. Für eine Menge A kann man an dieser Stelle die *Mächtigkeit* (engl. *cardinality*) $|A|$ dadurch definieren, dass man sagt $|A| := n$, falls es eine bijektive Abbildung $f\colon A \to \{1, 2, \ldots, n\}$ gibt.

Gibt es für ein bestimmtes $n \in \mathbb{N}$ eine solche Abbildung, so sagt man, A ist *endlich* (engl. *finite*). Anderenfalls sagt man, A ist *unendlich* (engl. *infinite*) und schreibt $|A| = \infty$. Wenn A und B beide endlich sind und $|A| = |B|$ gilt, dann gibt es immer eine Bijektion $f\colon A \to B$. Aber Vorsicht: aus $|A| = |B| = \infty$ folgt im allgemeinen **nicht,** dass es eine Bijektion $f\colon A \to B$ gibt. Man kann zum Beispiel zeigen, dass es keine Bijektion von $\mathbb{Q}$ nach $\mathbb{R}$ gibt, obwohl beide Mengen unendlich sind.

Definition 9. Sind $f\colon A \to B$ und $g\colon B \to C$ Funktionen, so heißt $g \circ f\colon A \to C$ mit $(g \circ f)(x) := g(f(x))$ die *Verkettung* (oder *Komposition*) von f und g.

Satz 4.

1. Die Verkettung injektiver Funktionen ist injektiv.

2. Die Verkettung surjektiver Funktionen ist surjektiv.

3. Die Verkettung bijektiver Funktionen ist bijektiv.

Beweis.

1. Seien $f\colon A \to B$ und $g\colon B \to C$ injektive Funktionen und $h = g \circ f$.

   Zu zeigen: h ist injektiv, also $\forall\, x_1, x_2 \in A : h(x_1) = h(x_2) \Rightarrow x_1 = x_2$.

   Seien also $x_1, x_2 \in A$ mit $h(x_1) = h(x_2)$, d. h. $g(f(x_1)) = g(f(x_2))$. Da g nach Annahme injektiv ist, folgt zunächst $f(x_1) = f(x_2)$. Und daraus folgt, da nach Annahme auch f injektiv ist, $x_1 = x_2$, was zu zeigen war.

2., 3. Übung. ∎

Satz 5. $f\colon A \to B$ ist genau dann bijektiv, wenn es eine Funktion $g\colon B \to A$ gibt mit $g \circ f = \mathrm{id}_A$ und $f \circ g = \mathrm{id}_B$.

Diese Funktion g ist dann eindeutig bestimmt und ihrerseits bijektiv.

Beweis. „⇒“ Annahme: $f\colon A \to B$ ist bijektiv, zu zeigen: Es gibt $g\colon B \to A$ mit $g \circ f = \mathrm{id}_A$.
Betrachte $g = \{\, (y, x) \in B \times A : (x, y) \in f \subseteq A \times B \,\}$.

1. g ist rechtseindeutig, weil f nach Annahme injektiv und damit linkseindeutig ist.
2. g ist linkstotal, weil f nach Annahme surjektiv und damit rechtstotal ist.

Damit ist g eine Funktion.
Für jedes $x \in A$ gilt $(x, f(x)) \in f$ und $(f(x), x) \in g$, also $g(f(x)) = x$. Damit ist gezeigt $g \circ f = \mathrm{id}_A$.
Für jedes $y \in B$ gibt es ein $x \in A$ mit $f(x) = y$, weil f surjektiv ist. Nach Definition von g gilt dann $g(y) = x$ und damit $f(g(y)) = y$. Damit ist gezeigt $f \circ g = \mathrm{id}_B$.

„⇐“ Annahme: Es gibt ein $g\colon B \to A$ mit $g \circ f = \mathrm{id}_A$ und $f \circ g = \mathrm{id}_B$. zu zeigen: f ist bijektiv, d. h. injektiv und surjektiv.
Injektiv: Seien $x_1, x_2 \in A$ mit $f(x_1) = f(x_2)$. Dann gilt $\underbrace{g(f(x_1))}_{=x_1} = \underbrace{g(f(x_2))}_{=x_2}$.
Surjektiv: Sei $y \in B$. Nach Annahme gilt $f(g(y)) = y$, also existiert ein $x \in A$, nämlich $x = g(y)$ mit $f(x) = y$.

Eindeutigkeit: Sind $g, \tilde{g}\colon B \to A$ zwei verschiedene Funktionen mit $g \circ f = \tilde{g} \circ f = \mathrm{id}_A$, dann gibt es zumindest ein $y \in B$ mit $g(y) \neq \tilde{g}(y)$.
Wähle so ein $y \in B$ und setze $x_1 := g(y)$ und $x_2 := \tilde{g}(y)$.
Da f surjektiv ist, existiert $x \in A$ mit $f(x) = y$. Wegen $g \circ f = \tilde{g} \circ f = \mathrm{id}_A$ gilt

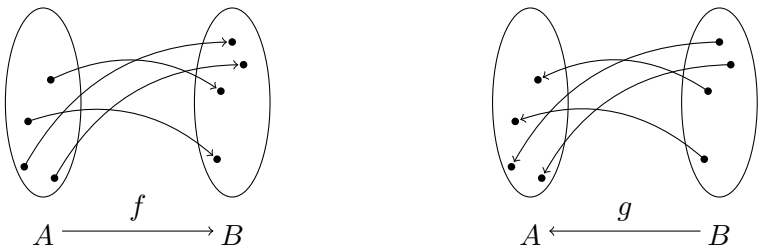
$$\underbrace{g(\underbrace{f(x)}_{=y})}_{=x_1} = x \qquad \text{und} \qquad \underbrace{\tilde{g}(\underbrace{f(x)}_{=y})}_{=x_2} = x,$$

also $x_1 = x_2$. Das ist ein Widerspruch zu der Annahme, dass g und $\tilde{g}$ verschiedene Funktionen sind.

Bijektivität: Zu zeigen ist, dass g injektiv und surjektiv ist.

1. g ist linkseindeutig (also injektiv) weil f rechtseindeutig (da Funktion) ist.
2. g ist rechtstotal (also surjektiv) weil f linkstotal (da Funktion) ist. ∎

Beispiel.



Das Schaubild für g ergibt sich aus dem Schaubild für f, indem man alle Pfeile umkehrt. Nach dem Satz ist f genau dann bijektiv, wenn dabei wieder eine Funktion herauskommt.

Definition 10. Sei $f\colon A \to B$ eine Funktion.

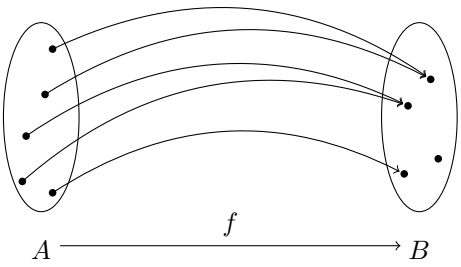
1. Für $U \subseteq A$ definiert man
$$f(U) := \{\, y \in B \mid \exists\, x \in U : f(x) = y \,\} \subseteq B$$
und nennt diese Menge das *Bild* (engl. *image*) von U unter f.

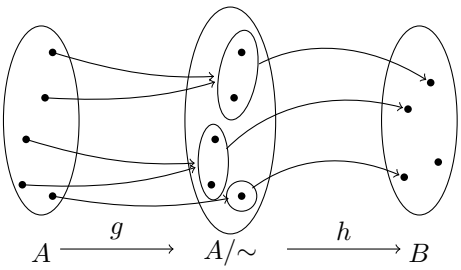
2. Für $V \subseteq B$ definiert man
$$f^{-1}(V) := \{\, x \in A \mid \exists\, y \in V : f(x) = y \,\} \subseteq A$$
und nennt diese Menge das *Urbild* (engl. *preimage*) von V unter f.

3. Ist f bijektiv und $g\colon B \to A$ wie im vorherigen Satz, dann heißt $f^{-1} := g$ die *Umkehrfunktion* (oder *Inverse*) von f.

Satz 6. (Homomorphiesatz für Mengen) Sei $f\colon A \to B$ eine Funktion.

1. Durch $x \sim y \iff f(x) = f(y)$ wird eine Äquivalenzrelation auf A definiert.
2. Die Funktion $g\colon A \to A/\!\sim$, $g(x) = [x]_\sim$ ist surjektiv.
3. Es gibt eine injektive Funktion $h\colon A/\!\sim \to B$ so dass $f = h \circ g$.
4. Diese Funktion h ist eindeutig bestimmt.
5. f ist genau dann surjektiv, wenn h bijektiv ist.





Beweis.

1., 2. Übung

3. Betrachte die Funktion $g\colon A \to A/\!\sim$ mit $g(x) = [x]_\sim$ für alle $x \in A$ und „definiere“ die Funktion $h\colon A/\!\sim \to B$ durch $h([x]_\sim) = f(x)$. Das ist möglich, weil $[x]_\sim = [y]_\sim \iff x \sim y \iff f(x) = f(y)$. (Man sagt, die Definition ist „repräsentantenunabhängig“, oder „h ist wohldefiniert“.)

   h ist injektiv, denn wenn $[x]_\sim, [y]_\sim \in A/\!\sim$ so sind, dass $h([x]_\sim) = h([y]_\sim)$ gilt, dann $f(x) = f(y)$, und dann $x \sim y$, und dann $[x]_\sim = [y]_\sim$.

   Es gilt $f = h \circ g$, denn für alle $x \in A$ gilt $h(g(x)) = h([x]_\sim) = f(x)$.

4. Wenn $\bar{h}\colon A/\!\sim \to B$ eine andere Funktion mit $f = \bar{h} \circ g$ ist, müsste es ein $[x]_\sim \in A/\!\sim$ geben mit $h([x]_\sim) \neq \bar{h}([x]_\sim)$, obwohl doch $h([x]_\sim) = h(g(x)) = f(x) = \bar{h}(g(x)) = \bar{h}([x]_\sim)$ gelten soll.

5. Übung ∎

Beispiel.

1. Seien $A = \{1,2,3,4,5,6\}$, $B = \{a,b,c\}$ und

$$f\colon \begin{array}{c|c|c|c|c|c} 1 & 2 & 3 & 4 & 5 & 6 \\ \hline a & b & a & c & c & a \end{array}.$$

   Dann ist

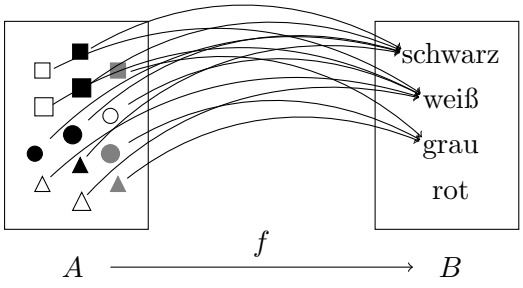
$$A/\!\sim = \big\{\{1,3,6\},\{2\},\{4,5\}\big\}$$

   Die Funktionen g und h aus dem Satz sind gegeben durch

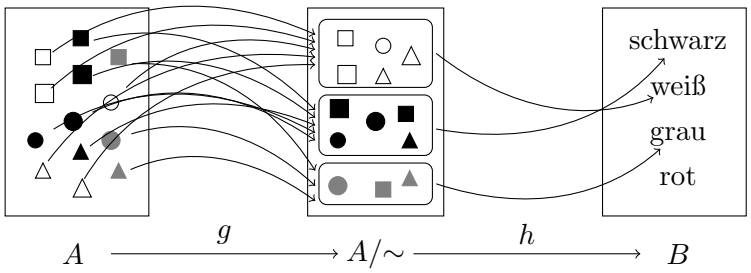
$$g\colon \begin{array}{c|c|c|c|c|c} 1 & 2 & 3 & 4 & 5 & 6 \\ \hline \{1,3,6\} & \{2\} & \{1,3,6\} & \{4,5\} & \{4,5\} & \{1,3,6\} \end{array}$$

$$h\colon \begin{array}{c|c|c} \{1,3,6\} & \{2\} & \{4,5\} \\ \hline a & b & c \end{array}$$

2. Seien $A = \{\square, \blacksquare, \blacksquare, \square, \blacksquare, \circ, \bullet, \bullet, \bullet, \triangle, \blacktriangle, \blacktriangle, \triangle\}$, $B = \{\text{schwarz}, \text{weiß}, \text{grau}, \text{rot}\}$, und sei $f\colon A \to B$ die Funktion, die jedem Element aus A dessen Farbe zuordnet:



Die Zerlegung von f in $f = h \circ g$ sieht dann wie folgt aus:



3. Sei A die Menge der Teilnehmer der Vorlesungsklausur, $B = \{1, 2, 3, 4, 5\}$ die Menge der erreichbaren Noten, $f\colon A \to B$ die Funktion, die jedem Teilnehmer seine Beurteilung zuordnet.

   In diesem Fall gruppiert $\sim$ die Teilnehmer entsprechend ihrer Note. Wenn jede Note mindestens einmal vergeben wird, wenn also f surjektiv ist, dann ist

   $$A/\sim = \{f^{-1}(\{1\}), f^{-1}(\{2\}), f^{-1}(\{3\}), f^{-1}(\{4\}), f^{-1}(\{5\})\}.$$

   Wenn dagegen z. B. nur die Noten 1 und 5 vergeben werden, dann ist $A/\sim = \{f^{-1}(\{1\}), f^{-1}(\{5\})\}$, weil dann $f^{-1}(\{2\}) = f^{-1}(\{3\}) = f^{-1}(\{4\}) = \emptyset$ keine Äquivalenzklassen sind. (Äquivalenzklassen sind niemals leer.)

   Jedenfalls bildet die Funktion g aus dem Satz jeden Klausurteilnehmer $t \in A$ auf die Menge $[t]_\sim$ aller Teilnehmer ab, die die gleiche Note wie t bekommen. Die Funktion h bildet dann jede dieser Mengen auf die Note ab, die die Teilnehmer dieser Menge bekommen.

4 Gruppen

Definition 11. Sei A eine Menge. Eine Funktion $\circ\colon A \times A \to A$ heißt *Verknüpfung.* Statt $\circ(x, y)$ schreibt man $x \circ y$.
Sei $\circ\colon A \times A \to A$ eine Verknüpfung.

1. $\circ$ heißt *assoziativ,* falls $\forall\ x, y, z \in A : (x \circ y) \circ z = x \circ (y \circ z)$
2. $\circ$ heißt *kommutativ,* falls $\forall\ x, y \in A : x \circ y = y \circ x$
3. $e \in A$ heißt *Neutralelement* (bezüglich $\circ$), falls gilt: $\forall\ x \in A : x \circ e = e \circ x = x$.
4. Ist $e \in A$ ein Neutralelement, so heißt $x \in A$ *invertierbar,* falls

   $$\exists\ y \in A : x \circ y = y \circ x = e.$$

   Ein solches Element y heißt dann ein *Inverses* von x.

Beispiel.

1. Sei $A = \{1, 2, 3\}$ und die Verknüpfung $\circ\colon A \times A \to A$ gegeben durch

$\circ$	1	2	3
1	2	3	1
2	1	3	2
3	3	2	1

   .

   Dann gilt $(1 \circ 1) \circ 2 = 3$ und $1 \circ (1 \circ 2) = 1$. Diese Verknüpfung ist also nicht assoziativ.

2. $+$ und $\cdot$ sind Verknüpfungen auf $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, etc.

   Diese Verknüpfungen sind assoziativ und kommutativ.

   0 ist ein Neutralelement bezüglich $+$ und 1 ist ein Neutralelement bezüglich $\cdot$.

3. Sei A eine Menge und A^A die Menge aller Funktionen $f\colon A \to A$. Dann ist die Komposition eine Verknüpfung auf A^A, die assoziativ aber im allgemeinen nicht kommutativ ist. Die Identitätsfunktion $\mathrm{id}_A \in A^A$ ist ein Neutralelement, und eine Funktion $f \in A^A$ ist genau dann invertierbar, wenn sie bijektiv ist.

4. $\cap$ und $\cup$ sind Verknüpfungen auf $\mathcal{P}(A)$.

Satz 7. Sei $\circ\colon A \times A \to A$ eine assoziative Verknüpfung.

1. Sind e_1, e_2 Neutralelemente von $\circ$, so gilt $e_1 = e_2$.

2. Ist e ein Neutralelement von $\circ$, $x \in A$ invertierbar, und sind y_1, y_2 Inverse von x, so gilt $y_1 = y_2$.

   Notation: $x^{-1} := y_1 = y_2$.

3. Ist $x \in A$ invertierbar, so ist auch x^{-1} invertierbar und es gilt $(x^{-1})^{-1} = x$.

4. Sind $x, y \in A$ invertierbar, so ist auch $x \circ y$ invertierbar und es gilt $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$.

Beweis.

1. Nach Definition gilt $\forall\, x \in A : x \circ e_1 = e_1 \circ x = x$ und $\forall\, x \in A : x \circ e_2 = e_2 \circ x = x$.

   Aus dem ersten folgt mit $x = e_2$, dass $e_2 \circ e_1 = e_1 \circ e_2 = e_2$ ist, und aus dem zweiten folgt mit $x = e_1$, dass $e_1 \circ e_2 = e_2 \circ e_1 = e_1$ ist.

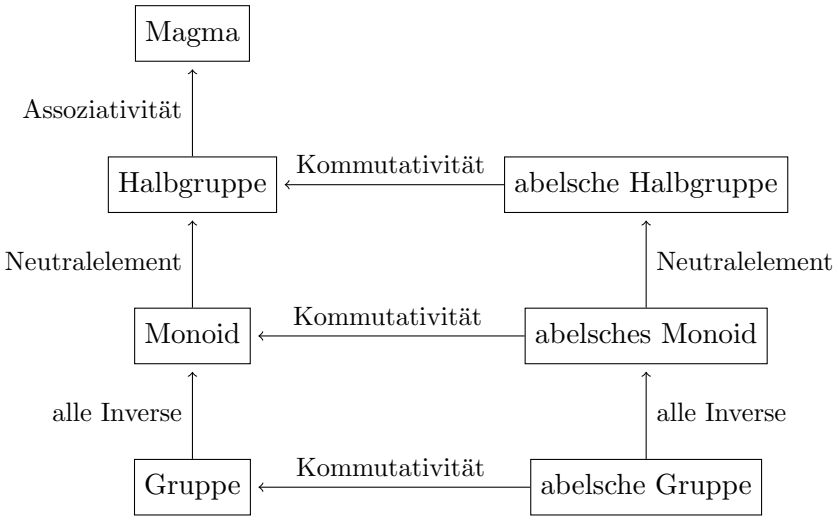
   Aus beidem zusammen folgt $e_1 = e_1 \circ e_2 = e_2$, wie behauptet.

2. Es gilt $x \circ y_1 = e$, also $y_2 \circ (x \circ y_1) = y_2 \circ e$, also $(y_2 \circ x) \circ y_1 = y_2$, also $e \circ y_1 = y_2$, also $y_1 = y_2$.

3., 4. Übung.

Definition 12. Sei A eine Menge und $\circ\colon A \times A \to A$ eine Verknüpfung.

1. Das Paar $(A, \circ)$ heißt *Magma.*
2. Ist $\circ$ assoziativ, so heißt $(A, \circ)$ eine *Halbgruppe* (engl. *semi group*).
3. Eine Halbgruppe mit Neutralelement heißt *Monoid.*
4. Ein Monoid, in dem jedes Element invertierbar ist, heißt *Gruppe* (engl. *group*).
5. Ein[e] Halbgruppe/Monoid/Gruppe heißt *abelsch,* wenn $\circ$ kommutativ ist.



Typischerweise verwendet man $\circ$ und $*$ als Symbole für Verknüpfungen, wenn man allgemein über Gruppen spricht. Bei konkreten Beispielen für Gruppen ist es üblich, das Symbol $+$ für die Verknüpfung zu wählen, wenn es sich um eine abelsche Gruppe handelt. In diesem Fall schreibt man $-x$ statt x^{-1} für das Inverse von x, und man kann auch z. B. $5x$ statt $x + x + x + x + x$ schreiben. Für das Neutralelement verwendet man dann typischerweise das Symbol 0 (Null).

Handelt es sich nicht um eine abelsche Gruppe, und sind $\circ$ und $*$ zu unhandlich, dann kann man auch den Multiplikationspunkt $\cdot$ als Verknüpfungssymbol verwenden. Statt $x \cdot y$ schreibt man dann auch einfach xy, und statt $xxxxx$ schreibt man dann x^5. Für das Neutralelement bietet sich in diesem Fall das Symbol 1 (Eins) an.

Ist $(G, \circ)$ eine Gruppe, dann nennt man G die *Trägermenge* der Gruppe. Wenn die Verknüpfung aus dem Zusammenhang klar ist, sagt man auch einfach, „G ist eine Gruppe“.

Beispiel.

1. Die erste Verknüpfung im vorherigen Beispiel ist nur ein Magma.
2. $(\{3, 4, 5, \dots\}, +)$ ist eine Halbgruppe, aber kein Monoid.
3. $(\mathbb{N}, +)$, $(\mathbb{N} \setminus \{0\}, \cdot)$, $(\mathbb{Z} \setminus \{0\}, \cdot)$.
4. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, etc. sind abelsche Gruppen.

5. Die Menge $\{ x \in \mathbb{Q} : x > 0 \}$ aller positiven rationalen Zahlen bildet zusammen mit der Multiplikation eine Gruppe. Ebenso die Menge aller positiven reellen Zahlen.

6. Ist A eine Menge, so sind $(\mathcal{P}(A), \cup)$, $(\mathcal{P}(A), \cap)$ Monoide, aber keine Gruppen. Definiert man auf $\mathcal{P}(A)$ die Verknüpfung

$$\oplus\colon \mathcal{P}(A) \times \mathcal{P}(A) \to \mathcal{P}(A), \quad U \oplus V := (U \cup V) \setminus (U \cap V),$$

so ist $(\mathcal{P}(A), \oplus)$ eine abelsche Gruppe. Das Neutralelement ist dann die leere Menge $\emptyset$ und jedes Element $U \in \mathcal{P}(A)$ ist zu sich selbst invers.

7. Ist A eine Menge, so ist $(A^A, \circ)$ ein Monoid, aber keine Gruppe. Aber die Menge $S(A) := \{ f \in A^A : f \text{ ist bijektiv} \}$ bildet zusammen mit der Verkettung als Verknüpfung eine Gruppe. Diese Gruppe ist nicht kommutativ. Man nennt sie Gruppe die *symmetrische Gruppe.* Statt $S(\{1, 2, \ldots, n\})$ schreibt man auch S_n und nennt dann die Elemente *Permutationen.* Bsp.:

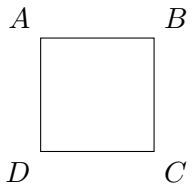
$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix}, \quad \pi^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix}$$

und

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$
$$\neq \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Mehr über Permutationen in Abschnitt 12.

8. Betrachte ein Quadrat mit den Eckpunkten A, B, C, D.



Eine Symmetrie lässt sich auffassen als eine Funktion $\{A, B, C, D\} \to \{A, B, C, D\}$, die das Quadrat als Ganzes fest lässt.

Das Quadrat hat folgende Symmetrien:

- $\sigma = \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}$ – das ist die Spiegelung an der horizontalen Achse
- $\rho = \begin{pmatrix} A & B & C & D \\ B & C & D & A \end{pmatrix}$ – das ist die Rotation um 90° entgegen dem Uhrzeigersinn

sowie einige weitere, die sich aus diesen durch Komposition bilden lassen. Die komplette Liste lautet:

$$G = \{\mathrm{id}, \rho, \rho^2, \rho^3, \sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3\}.$$

Diese Menge G bildet zusammen mit der Komposition eine Gruppe, die sogenannte *Symmetriegruppe* des Quadrats. Die Gruppe ist nicht abelsch; es gilt aber zum Beispiel $\sigma\rho = \rho^3\sigma$.

9. Sei $m \in \mathbb{N} \setminus \{0\}$ und definiere $\equiv_m$ durch $a \equiv_m b \iff m \mid a - b$ für alle $a, b \in \mathbb{Z}$. Dies ist eine Äquivalenzrelation, die $\mathbb{Z}$ in m Äquivalenzklassen aufteilt:

$$\mathbb{Z}_m := \mathbb{Z}/\equiv_m = \{\, [0]_{\equiv_m}, [1]_{\equiv_m}, \ldots, [m-1]_{\equiv_m} \}.$$

Definiere $+, \cdot \colon \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$ durch

$$[x]_{\equiv_m} + [y]_{\equiv_m} := [x + y]_{\equiv_m}, \qquad [x]_{\equiv_m} \cdot [y]_{\equiv_m} := [x \cdot y]_{\equiv_m}.$$

Diese Definitionen sind repräsentantenunabhängig, d. h. für x, x' und y, y' mit $x \equiv_m x'$ und $y \equiv_m y'$ gilt stets $(x + y) \equiv_m (x' + y')$ und $(x \cdot y) \equiv_m (x' \cdot y')$. (Beweis: Übung.)

$(\mathbb{Z}_m, +)$ ist eine Gruppe.

$(\mathbb{Z}_m \setminus \{[0]_{\equiv_m}\}, \cdot)$ ist ein Monoid. Man kann zeigen, dass dieses Monoid genau dann eine Gruppe ist, wenn m eine Primzahl ist.

10. Betrachte die sechs Funktionen $f_i \colon \mathbb{R} \setminus \{0, 1\} \to \mathbb{R} \setminus \{0, 1\}$ definiert durch

$$f_1(x) = x, \qquad f_2(x) = \frac{1}{1-x}, \quad f_3(x) = \frac{1}{x},$$
$$f_4(x) = \frac{x-1}{x}, \quad f_5(x) = 1 - x, \quad f_6(x) = \frac{x}{x-1}.$$

Die Menge $G = \{f_1, \ldots, f_6\}$ bildet zusammen mit der Komposition eine Gruppe.

11. Sei $G = \{\, x \in \mathbb{R} : -1 < x < 1 \,\}$ und definiere

$$x \oplus y := \frac{x + y}{1 + xy},$$

wobei die Symbole auf der rechten Seite die übliche Bedeutung haben. Dann ist $(G, \oplus)$ eine abelsche Gruppe. Man sieht sofort, dass $\oplus$ kommutativ ist, dass 0 ein neutrales Element ist, und dass $-x$ das Inverse von x ist. Assoziativität lässt sich leicht nachrechnen:

$$(x \oplus y) \oplus z = \frac{\frac{x+y}{1+xy} + z}{1 + \frac{x+y}{1+xy} z} = \frac{x + y + z + xyz}{1 + xy + xz + yz} = \frac{x + \frac{y+z}{1+yz}}{1 + x\frac{y+z}{1+yz}} = x \oplus (y \oplus z).$$

Jetzt muss man sich aber auch noch davon überzeugen, dass $\oplus$ tatsächlich eine Verknüpfung ist. Dazu ist zu zeigen, dass $1 + xy \neq 0$ für alle $x, y \in G$ (sonst wäre für manche $x, y \in G$ der Ausdruck auf der rechten Seite nicht definiert), und dass $|\frac{x+y}{1+xy}| < 1$ für jede Wahl von $x, y \in G$ (sonst würde uns die Verknüpfung von manchen $x, y \in G$ aus der Gruppe herauswerfen).

Zunächst ist klar, dass mit $|x| < 1$ und $|y| < 1$ auch $|xy| < 1$ ist, und damit $xy > -1$, und damit $1 + xy > 0$, also insbesondere $1 + xy \neq 0$.

Als nächstes gilt mit $|x| < 1$ und $|y| < 1$ insbesondere $1 - x > 0$ und $1 - y > 0$, und also auch $(1-x)(1-y) > 0$. Nun ist $(1-x)(1-y) = 1 - x - y + xy$. Also $1 + xy > x + y$, also $1 > \frac{x+y}{1+xy}$ (denn wir haben ja vorher schon gezeigt, dass $1 + xy > 0$ ist). Auf ähnliche Weise zeigt man $\frac{x+y}{1+xy} > -1$.

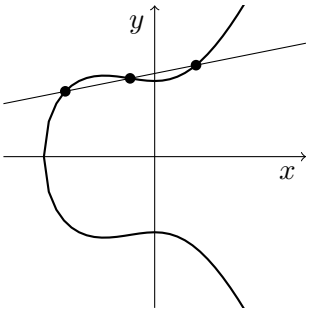
Die Gruppe $(G, \oplus)$ erklärt die Addition von Geschwindigkeiten in der speziellen Relativitätstheorie.

12. Betrachte die Menge

$$E = \{\, (x, y) \in \mathbb{R}^2 : y^2 = x^3 + x^2 + 1 \,\} \cup \{\mathcal{O}\},$$

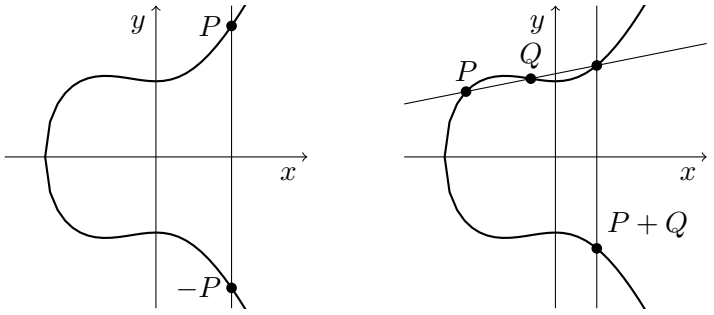
die aus den Punkten einer Kurve in der Ebene sowie dem zusätzlichen Symbol $\mathcal{O}$ besteht. Jede Gerade durch zwei Punkte dieser Kurve schneidet die Kurve in einem dritten Punkt, wenn man

- tangentiale Berührungen doppelt zählt, und
- bei senkrechten Geraden das spezielle Symbol $\mathcal{O}$ als den dritten Punkt ansieht.



Auf E lässt sich eine Verknüpfung $+$ definieren, indem man fordert, dass gelte $P + Q + R = \mathcal{O}$ für je drei Punkte $P, Q, R \in E$, die auf einer Geraden liegen.

Mit dieser Verknüpfung wird E zu einer abelschen Gruppe. Das Neutralelement ist $\mathcal{O}$. Inverse bekommt man durch Spiegelung an der horizontalen Achse. Die Verknüpfung führt man durch, indem man zu gegebenen P und Q zunächst den zugehörigen dritten Punkt bestimmt, und diesen dann noch an der horizontalen Achse spiegelt.



Die Gruppe E ist ein Beispiel für eine sogenannte *elliptische Kurve.* Solche Gruppen werden in der Kryptographie eingesetzt.

13. Seien $A = \{a_1, \ldots, a_n\}$, $\bar{A} = \{\bar{a}_1, \ldots, \bar{a}_n\}$ zwei disjunkte (d. h. $A \cap \bar{A} = \emptyset$) Mengen mit $|A| = |\bar{A}| = n$.

Betrachte die Elemente von $A \cup \bar{A}$ als Buchstaben und Tupel von Elementen als Wörter, z. B. $(a_1, a_3, \bar{a}_1, a_2)$, $(a_3, \bar{a}_1, \bar{a}_2)$, etc.

Es sei $W(A)$ die Menge all solcher Tupel (von beliebiger aber stets endlicher Länge), in denen nie a_i und $\bar{a}_i$ (mit dem selben Index) unmittelbar nebeneinander stehen.

Definiere $\circ\colon W(A) \times W(A) \to W(A)$ so, dass $w_1 \circ w_2$ durch Aneinanderhängen von w_1 und w_2 und anschliessendes Löschen aller Vorkommen $(a_i, \bar{a}_i)$ und $(\bar{a}_i, a_i)$ entsteht, zum Beispiel:

$$(a_1, \bar{a}_2, \bar{a}_3) \circ (a_3, \bar{a}_1, a_2) = (a_1, \bar{a}_2, \bar{a}_1, a_2).$$

Dann ist $(W(A), \circ)$ eine Gruppe, die sogenannte *freie Gruppe* über A.

Das Neutralelement ist das „leere Wort“ ().

Inverse ergeben sich durch Rückwärtslesen des Tupels und Vertauschen aller a_i mit den zugehörigen $\bar{a}_i$, zum Beispiel:

$$(a_1, \bar{a}_2, a_3)^{-1} = (\bar{a}_3, a_2, \bar{a}_1).$$

14. Seien $(A, \circ), (B, *)$ zwei Gruppen [zwei Halbgruppen, zwei Monoide] und $G = A \times B$. Auf G wird durch
$$(a_1, b_1) \odot (a_2, b_2) := (a_1 \circ a_2, b_1 * b_2)$$
eine Verknüpfung $\odot\colon G \times G \to G$ definiert, mit der G zu einer Gruppe [einer Halbgruppe, einem Monoid] wird.

Definition 13. Sei $(G, \circ)$ eine Gruppe. $U \subseteq G$ heißt eine Untergruppe, falls gilt $U \neq \emptyset$ und $\forall\, u, v \in U : u \circ v \in U \wedge u^{-1} \in U$.

Beispiel.

1. $(\mathbb{Z}, +)$ ist eine Untergruppe von $(\mathbb{Q}, +)$; $(\mathbb{Q}, +)$ ist eine Untergruppe von $(\mathbb{R}, +)$.
2. $(\{\, x \in \mathbb{Q} : x > 0 \,\}, \cdot)$ ist eine Untergruppe von $(\mathbb{Q} \setminus \{0\}, \cdot)$; $(\mathbb{Q} \setminus \{0\}, \cdot)$ und $(\{\, x \in \mathbb{R} : x > 0 \,\}, \cdot)$ sind Untergruppen von $(\mathbb{R} \setminus \{0\}, \cdot)$.
3. Die Symmetriegruppe des Rechtecks ist eine Untergruppe der Symmetriegruppe des Quadrats.
4. S_3 lässt sich auffassen als Untergruppe von S_5, wenn man sich jede Funktion
$$f\colon \{1, 2, 3\} \to \{1, 2, 3\}$$
aus S_3 zu einer Funktion $f\colon \{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\}$ mit $f(4) = 4$ und $f(5) = 5$ fortgesetzt denkt.

Definition 14. Seien $(G_1, \circ)$ und $(G_2, *)$ Gruppen. Eine Funktion $h\colon G_1 \to G_2$ heißt *Homomorphismus,* falls gilt:

$$\forall\, x, y \in G_1 : h(x \circ y) = h(x) * h(y).$$

Sei e_2 das Neutralelement von G_2. Die Menge

$$\ker h := h^{-1}(\{e_2\}) = \{\, x \in G_1 : h(x) = e_2 \,\} \subseteq G_1$$

heißt der *Kern* (engl. *kernel*) und

$$\operatorname{im} h := h(G_1) = \{\, h(x) : x \in G_1 \,\} \subseteq G_2$$

heißt das *Bild* (engl. *image*) von h.

Ein bijektiver Homomorphismus heißt *Isomorphismus.* Wenn es einen Isomorphismus von G_1 nach G_2 gibt, sagt man, G_1 und G_2 sind (zueinander) *isomorph.* Notation in diesem Fall: $G_1 \cong G_2$.

Beispiel.

1. Die Abbildung $h\colon S_3 \to S_5$, die im vorigen Beispiel beschrieben wurde, ist ein Homomorphismus. Statt zu sagen, S_3 ist eine Untergruppe von S_5, wäre es sauberer zu sagen $h(S_3)$ ist eine Untergruppe von S_5.

2. Die Abbildung $f\colon \mathbb{Z} \to \mathbb{Z}_m$, $x \mapsto [x]_{\equiv_m}$ ist ein Homomorphismus zwischen den Gruppen $(\mathbb{Z}, +)$ und $(\mathbb{Z}_m, +)$.

   Es gilt $\ker f = [0]_{\equiv_m} = m\mathbb{Z} = \{0, m, -m, 2m, -2m, \dots\}$.

   Der Homomorphismus ist auch mit der Multiplikation verträglich, d. h. es gilt $[xy]_{\equiv_m} = [x]_{\equiv_m}[y]_{\equiv_m}$ für alle $x, y \in \mathbb{Z}$.

3. Die Abbildung $f\colon \mathbb{R} \to \mathbb{R}$, $x \mapsto \exp(x)$ ist ein Homomorphismus zwischen $(\mathbb{R}, +)$ und $(\mathbb{R} \setminus \{0\}, \cdot)$.

4. Sind $(A, \circ), (B, *)$ zwei Gruppen und $G = A \times B$ zusammen mit

   $$(a_1, b_1) \odot (a_2, b_2) := (a_1 \circ a_2, b_1 * b_2).$$

   Dann ist $h\colon G \to A$, $(a, b) \mapsto a$ ein Homomorphismus.

5. Die Abbildung $f\colon \mathbb{Z} \to \mathbb{Z}_7 \setminus \{[0]_{\equiv_7}\}$,

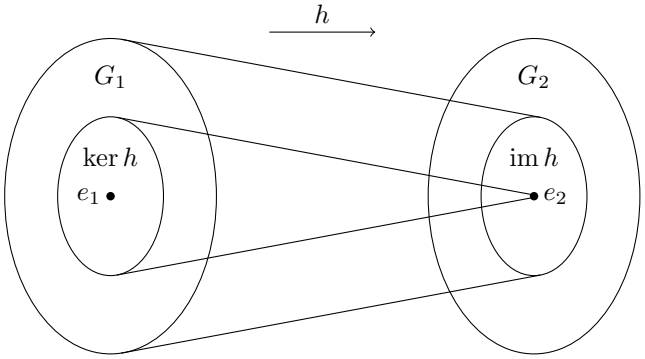
   $$x \mapsto [2]^x_{\equiv_7} := \begin{cases} [2]^x_{\equiv_7} & \text{falls } x > 0 \\ [1]_{\equiv_7} & \text{falls } x = 0 \\ ([2]^{-1}_{\equiv_7})^{|x|} & \text{falls } x < 0 \end{cases}$$

   ist ein Homomorphismus von $(\mathbb{Z}, +)$ nach $(\mathbb{Z}_7 \setminus \{[0]_{\equiv_7}\}, \cdot)$.

   Es gilt $\operatorname{im} f = \{[1]_{\equiv_7}, [2]_{\equiv_7}, [4]_{\equiv_7}\} \subseteq \mathbb{Z}_7 \setminus \{[0]_{\equiv_7}\}$ und $\ker f = \{0, 3, -3, 6, -6, \dots\} \subseteq \mathbb{Z}$.

Satz 8. Sei $h\colon G_1 \to G_2$ ein Homomorphismus. Dann gilt:

1. Ist e_1 das Neutralelement von G_1 und e_2 das Neutralelement von G_2, so gilt $h(e_1) = e_2$.
2. $\ker h$ ist eine Untergruppe von G_1.
3. $\operatorname{im} h$ ist eine Untergruppe von G_2.



Beweis.

1. Es gilt $h(e_1) = h(e_1 \circ e_1) = h(e_1) * h(e_1)$. Multipliziert man diese Gleichung mit dem Inversen von $h(e_1)$ in G_2, so erhält man $e_2 = h(e_1)$.

2. Nach Teil 1 gilt zunächst $e_1 \in \ker h$ und damit insbesondere $\ker h \neq \emptyset$. Darüber hinaus bleibt zu zeigen: für alle $u, v \in \ker h$ gilt $u \circ v \in \ker h$ und $u^{-1} \in \ker h$.

   Seien $u, v \in \ker h$ beliebig. Es gilt $h(u) = h(v) = e_2$, weil $u, v \in \ker h$. Folglich gilt:

   $$h(u \circ v) = h(u) * h(v) = e_2 * e_2 = e_2,$$

   und also $u \circ v \in \ker h$.

   Es gilt $e_2 = h(e_1) = h(u \circ u^{-1}) = h(u) * h(u^{-1}) = e_2 * h(u^{-1}) = h(u^{-1})$.

   (Daraus folgt übrigens auch $h(u)^{-1} = h(u^{-1})$.)

3. Nach Teil 1 gilt zunächst $e_2 \in \operatorname{im} h$. Darüber hinaus bleibt zu zeigen: für alle $u, v \in \operatorname{im} h$ gilt $u * v \in \operatorname{im} h$ und $u^{-1} \in \operatorname{im} h$.

   Seien $u, v \in \operatorname{im} h$ beliebig. Dann gibt es $a, b \in G_1$ mit $u = h(a)$ und $v = h(b)$.

   Es gilt $u * v = h(a) * h(b) = h(a \circ b) \in \operatorname{im} h$.

   Außerdem $u^{-1} = h(a)^{-1} = h(a^{-1}) \in \operatorname{im} h$. ∎

Satz 9. Sei $(G, +)$ eine abelsche Gruppe und H eine Untergruppe von G, und sei $\sim$ definiert durch $a \sim b \iff a + (-b) \in H$.

Dann ist $\sim$ eine Äquivalenzrelation auf G und $G/H := G/\sim$ zusammen mit $*\colon G/H \times G/H \to G/H$, $[x]_\sim * [y]_\sim := [x + y]_\sim$ ist wieder eine abelsche Gruppe.

Beweis. Dass $\sim$ eine Äquivalenzrelation ist, kann man sich zur Übung selbst überlegen.

Wir zeigen, dass $*$ wohldefiniert ist. Zu zeigen ist, dass für $x, x', y, y' \in G$ mit $x \sim x'$ und $y \sim y'$ gilt $x + y \sim x' + y'$.

Aus $x \sim x'$ und $y \sim y'$ folgt $x + (-x') \in H$ und $y + (-y') \in H$. Da H eine Untergruppe von G ist, folgt $x + (-x') + y + (-y') \in H$. Da G abelsch ist, ist $x + (-x') + y + (-y') = x + y + (-x') + (-y') = (x + y) + (-(x' + y'))$, also gilt $x + y \sim x' + y'$, wie behauptet.

Um schließlich zu zeigen, dass G/H eine Gruppe ist, überzeugt man sich, dass die nötigen Gesetze erfüllt sind. Assoziativität folgt zum Beispiel aus

$$[x] * ([y] * [z]) = [x] * [y + z] = [x + (y + z)] = [(x + y) + z] = [x + y] * [z] = ([x] * [y]) * [z].$$

Die Rechnungen für die anderen Gesetze sind ähnlich und bleiben zur Übung überlassen. ∎

Beispiel. Sei $m \in \mathbb{N} \setminus \{0\}$. Dann ist $m\mathbb{Z} = \{\, mx : x \in \mathbb{Z} \,\} = \{\dots, -m, 0, m, 2m, \dots\}$ eine Untergruppe von $(\mathbb{Z}, +)$. Es gilt $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$.

Satz 10. (Homomorphiesatz für abelsche Gruppen) Es seien $(G_1, +), (G_2, \oplus)$ abelsche Gruppen und $f\colon G_1 \to G_2$ ein Homomorphismus.

1. Die Funktion
$$g\colon G_1 \to G_1/\ker f, \quad g(x) := [x]_\sim$$
ist ein surjektiver Homomorphismus.

2. Es existiert genau ein injektiver Homomorphismus $h\colon G_1/\ker f \to G_2$ mit $f = h \circ g$.

3. Dieser Homomorphismus h ist genau dann bijektiv, wenn f surjektiv ist.
Insbesondere gilt immer $G_1/\ker f \cong \operatorname{im} f$.

Beweis. Nach Satz 6 ist bloß noch zu zeigen, dass die Funktionen g und h Homomorphismen sind. (Beachte: $x \sim y \iff x + (-y) \in \ker f \iff f(x + (-y)) = e \iff f(x) \oplus f(-y) = e \iff f(x) \oplus f(y)^{-1} = e \iff f(x) = f(y)$, d. h. die hier verwendete Äquivalenzrelation ist ein Spezialfall der Relation aus Satz 6.)

Seien $x, y \in G$.

Wir zeigen zuerst: $g(x + y) = g(x) * g(y)$. In der Tat folgt $g(x + y) = [x + y]_\sim = [x]_\sim * [y]_\sim$ direkt aus der Definition von $*$ aus Satz 9. Damit ist g ein Homomorphismus.

Wir zeigen nun: $h(x*y) = h(x) \oplus h(y)$. In der Tat gilt: $h([x]_\sim * [y]_\sim) = h([x+y]_\sim) = f(x+y) = f(x) \oplus f(y) = h([x]_\sim) \oplus h([y]_\sim)$. Damit ist h ein Homomorphismus. ∎

Beispiel. Sei $f\colon \mathbb{Z} \to \mathbb{Z}_7$, $f(x) = [3]^x_{\equiv_7}$. Es gilt $\ker f = 6\mathbb{Z}$ und $\operatorname{im} f = \mathbb{Z}_7 \setminus \{[0]_{\equiv_7}\}$. Die Gruppe $(\mathbb{Z}_6, +)$ ist also isomorph zur Gruppe $(\mathbb{Z}_7 \setminus \{[0]_{\equiv_7}\}, \cdot)$ und der Isomorphismus h aus dem Satz erlaubt es, die Multiplikation in $\mathbb{Z}_7$ auf die Addition in $\mathbb{Z}_6$ zurückzuführen.

Wählt man $f\colon \mathbb{Z} \to \mathbb{Z}_7$, $f(x) = [2]^x_{\equiv_7}$, so ist $\ker f = 3\mathbb{Z}$ und $\operatorname{im} f = (\{[1]_{\equiv_7}, [2]_{\equiv_7}, [4]_{\equiv_7}\}, \cdot)$. In diesem Fall ist f nicht surjektiv, und der Satz liefert nur einen Isomorphismus zwischen $(\mathbb{Z}_3, +)$ und der Untergruppe $(\{[1]_{\equiv_7}, [2]_{\equiv_7}, [4]_{\equiv_7}\}, \cdot)$ von $(\mathbb{Z}_7 \setminus \{[0]_{\equiv_7}\}, \cdot)$.

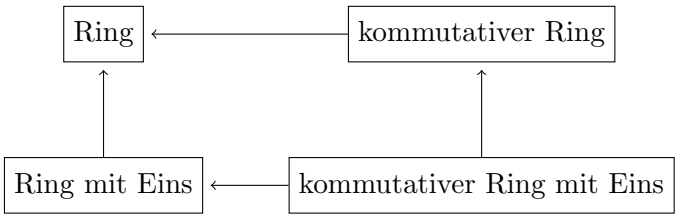
5 Ringe

Definition 15. Sei R eine Menge, $+\colon R \times R \to R$ und $\cdot\colon R \times R \to R$ seien zwei Verknüpfungen, so dass $(R, +)$ eine abelsche Gruppe ist. Ihr Neutralelement nennen wir *Null* (Symbol: 0), und das Inverse von $x \in R$ bezüglich $+$ schreiben wir $-x$. Statt $x + (-y)$ schreibt man $x - y$. Statt $x \cdot y$ schreibt man auch xy.

1. $(R, +, \cdot)$ heißt *Ring,* falls $(R, \cdot)$ eine Halbgruppe ist und gilt
$$\forall\, x, y, z \in R : (x + y) \cdot z = x \cdot z + y \cdot z$$
$$\forall\, x, y, z \in R : x \cdot (y + z) = x \cdot y + x \cdot z.$$

2. Wenn außerdem $(R\setminus\{0\}, \cdot)$ ein Monoid ist, nennt man das Neutralelement *Eins* (Symbol: 1) und $(R, +, \cdot)$ einen *Ring mit Eins.*

3. Ein Ring (mit oder ohne Eins) heißt *kommutativ,* falls $\cdot$ kommutativ ist.



Wenn man in einer Definition einen Begriff einführt, dann ist man normalerweise bemüht, für den Begriff ein Wort aus der Umgangssprache zu verwenden, das den Sachverhalt der Definition treffend beschreibt. Zum Beispiel haben wir vorher definiert, dass eine Relation R „symmetrisch“ zu nennen ist, wenn gilt $xRy \iff yRx$, und „reflexiv“, wenn gilt xRx. Theoretisch hätten wir auch das Wort „reflexiv“ für die Eigenschaft $xRy \iff yRx$ und das Wort „symmetrisch“ für die Eigenschaft xRx vergeben können, es wäre bloß sehr verwirrend, wenn die gemeinte Eigenschaft nicht mit der üblichen Bedeutung des Wortes zusammenpasst.

Der Begriff „Ring“, der oben eingeführt wurde, ist von zentraler Bedeutung in der Algebra. Es besteht allerdings kein offensichtlicher Zusammenhang mit der umgangssprachlichen Bedeutung des Wortes. Man hätte genauso gut „Haus“ oder „Baum“ als Wort verwenden können.

Satz 11. Sei $(R, +, \cdot)$ ein Ring mit Eins, und sei $x \in R$. Dann gilt $x0 = 0 = 0x$ und $-x = (-1)x$.

Beweis. Sei $x \in R$ beliebig.

Es gilt $x0 = x(0 + 0) = x0 + x0$. Addiert man auf beiden Seiten $-(x0)$, so bekommt man $x0 + (-x0) = x0 + x0 + (-x0)$, also $0 = x0 + 0 = x0$, wie behauptet. Der Beweis von $0x = 0$ geht analog.

Als nächstes gilt $0 = 0x = (1+(-1))x = 1x+(-1)x = x+(-1)x$. Damit ist $(-1)x$ ein Inverses von x bezüglich $+$, und wegen der Eindeutigkeit der Inversen muss gelten $(-1)x = -x$. ∎

Beispiel.

1. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ sind kommutative Ringe mit Eins. Aber $(\mathbb{N}, +, \cdot)$ ist kein Ring, weil $(\mathbb{N}, +)$ keine Gruppe ist.

2. Ist A eine Menge, so ist $(\mathcal{P}(A), \oplus, \cap)$ ein Ring mit Eins. Dabei ist wie zuvor $U \oplus V := (U \cup V) \setminus (U \cap V)$ definiert. Die Null ist $\emptyset$ und die Eins ist A.

3. Für jedes $m \in \mathbb{N} \setminus \{0\}$ ist $(\mathbb{Z}_m, +, \cdot)$ ein kommutativer Ring mit Eins, der sogenannte *Restklassenring* (engl. *residue class ring*) modulo m.

4. Sei $m \in \mathbb{N} \setminus \{0, 1\}$ und $m\mathbb{Z} = \{\, mx : x \in \mathbb{Z} \,\} = \{\dots, -m, 0, m, 2m, \dots\}$. Dann ist $(m\mathbb{Z}, +, \cdot)$ ein kommutativer Ring, aber ohne Eins.

5. Sei $(R, +, \cdot)$ ein Ring. Die Menge $\mathbb{R}^{\mathbb{N}}$ aller Funktionen $f\colon \mathbb{N} \to R$ (d. h. aller Folgen in R) bildet einen Ring, wenn man definiert

$$\begin{aligned} (f + g)\colon \mathbb{N} \to R, &\quad (f + g)(n) := f(n) + g(n) \\ (f \cdot g)\colon \mathbb{N} \to R, &\quad (f \cdot g)(n) := f(n)g(n). \end{aligned}$$

   Allgemeiner kann man statt $\mathbb{N}$ hier auch irgendeine andere Menge nehmen.

6. Die Menge $\mathbb{R}^{\mathbb{N}}$ bildet auch einen Ring, wenn man $+$ wie vorher definiert, und $\cdot$ durch

$$(a_0, a_1, a_2, \dots) \cdot (b_0, b_1, b_2, \dots) := (c_0, c_1, c_2, \dots)$$

mit $c_n := \sum_{k=0}^{n} a_k b_{n-k}$. (Beweis durch Nachrechnen der nötigen Gesetze.)

Zum Beispiel gilt

$$(1, 2, 3, \dots) \cdot (1, 2, 3, \dots) := (c_0, c_1, c_2, \dots)$$

mit

$$\begin{aligned} c_0 &= \sum_{k=0}^{0} a_k b_{n-k} = a_0 b_0 = 1 \\ c_1 &= \sum_{k=0}^{1} a_k b_{n-k} = a_0 b_1 + a_1 b_0 = 4 \\ c_2 &= \sum_{k=0}^{2} a_k b_{n-k} = a_0 b_2 + a_1 b_1 + a_2 b_1 = 10. \end{aligned}$$

Definiert man $X := (0, 1, 0, 0, \dots)$, so bietet es sich an, eine Folge $(a_n)_{n=0}^{\infty} \in R^{\mathbb{N}}$ in der Form $\sum_{n=0}^{\infty} a_n X^n$ zu schreiben. Man beachte, dass

$$\begin{aligned} X^0 &= (1, 0, 0, \dots) = 1 \\ X^1 &= (0, 1, 0, 0, \dots) \\ X^2 &= (0, 0, 1, 0, 0, \dots) \\ &\vdots \\ X^n &= (0, \dots, 0, \underset{\substack{\uparrow \\ \text{Index } n}}{1}, 0, 0, \dots). \end{aligned}$$

Die oben definierte Multiplikation entspricht dann genau dem üblichen Multiplikationsgesetz für Potenzreihen, freilich ohne dass dabei irgendwo von Konvergenz die Rede ist.

Statt $R^{\mathbb{N}}$ schreibt man auch $R[[X]]$ und nennt die Elemente *formale Potenzreihen* (engl. *formal power series*).

7. Die Teilmenge

$$R[X] := \Big\{ \sum_{n=0}^{\infty} a_n X^n \in R[[X]] : \exists\ N \in \mathbb{N}\ \forall\ n \geq N : a_n = 0 \Big\}$$

ist abgeschlossen unter $+$ und $\cdot$ und bildet deshalb selbst auch einen Ring. Man sagt, $R[X]$ ist ein *Unterring* von $R[[X]]$.

Die Elemente von $R[X]$ heißen *Polynome* über R.

Beispiel:

$$\begin{aligned}&(a_0 + a_1X + a_2X^2)(b_0 + b_1X)\\ &= a_0b_0 + (a_0b_1 + a_1b_0)X + (a_2b_0 + a_1b_1)X^2 + a_2b_1X^3\end{aligned}$$

Das Nullpolynom ist das Polynom $p = \sum_{n=0}^{\infty} a_nX^n \in R[X]$ mit $a_n = 0$ für alle $n \in \mathbb{N}$. Für alle anderen Polynome gibt es genau einen Index $n \in \mathbb{N}$, so dass $a_n \neq 0$ und $a_k = 0$ für alle $k > n$ ist. Diesen Index nennt man den *Grad* des Polynoms (engl. *degree*), geschrieben $\deg p := n$. Für das Nullpolynom definiert man $\deg 0 := -\infty$.

Mehr über Polynome in Abschnitt 31.

8. Sei R ein Ring und G ein Monoid.

   Betrachte die Menge $R[G]$ aller Funktionen $c\colon G \to R$ mit der Eigenschaft $c(g) \neq 0$ für höchstens endlich viele $g \in G$.

   Für $c_1, c_2 \in R[G]$ definiere

   $$(c_1 + c_2)\colon G \to R, \quad g \mapsto c_1(g) + c_2(g)$$

   und

   $$(c_1 \cdot c_2)\colon G \to R, \quad g \mapsto \sum_{h_1,h_2 \in G : h_1 \cdot h_2 = g} c_1(h_1) \cdot c_2(h_2).$$

   Dann ist $(R[G], +, \cdot)$ ein Ring.

   Schreibt man die Funktionen $c \in R[G]$ in der Form

   $$c = \alpha_1 \cdot g_1 + \alpha_2 \cdot g_2 + \cdots + \alpha_n \cdot g_n,$$

   wenn $c(g_1) = \alpha_1$, $c(g_2) = \alpha_2$, …, $c(g_n) = \alpha_n$ und $c(g) = 0$ für alle $g \in G \setminus \{g_1, \ldots, g_n\}$, dann entsprechen die obigen Definitionen von $+$ und $\cdot$ gerade den gewohnten Rechnenregeln. (Aber Vorsicht: wenn G nicht abelsch ist, ist $\cdot$ nicht kommutativ!)

   Beispiel. Sei $R = \mathbb{Z}$ und $G = \{a, b, c\}$ mit der Verknüpfung $\circ$, die durch folgende Tabelle definiert ist:

$\circ$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

   Dann gilt zum Beispiel

   $$\begin{aligned}(2a + 3b)(3c - 5b) &= 6(a \circ c) - 10(a \circ b) + 9(b \circ c) - 15(b \circ b)\\ &= 6c - 10b + 9a - 15c\\ &= 9a - 10b - 9c.\end{aligned}$$

6 Körper

Definition 16. Ein kommutativer Ring $(K, +, \cdot)$ heißt *Körper* (engl. *field*), falls $(K \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist.

Genau wie im Fall der Ringe ist nicht unmittelbar klar, warum sich der Begriff „Körper“ für diese Struktur eingebürgert hat. Es besteht jedenfalls kein offensichtlicher Zusammenhang zu den Körpern der Geometrie (Würfel, Kugeln, usw.). Der englische Begriff *field* ist auch nicht besonders gut motiviert. Der Hintergrund ist wahrscheinlich einfach, dass es in der Umgangssprache kein Wort gibt, das den Sachverhalt treffend beschreibt.

Satz 12. Sei $(K, +, \cdot)$ ein Körper und $x, y \in K$. Dann gilt $xy = 0 \Rightarrow x = 0 \vee y = 0$.

Beweis. Seien $x, y \in K$ mit $xy = 0$. Zu zeigen, $x = 0$ oder $y = 0$. Wir nehmen an, dass $x \neq 0$ ist, und zeigen, dass dann $y = 0$ sein muss. Da K ein Körper ist, gibt es in $K \setminus \{0\}$ zu jedem Element ein Inverses bezüglich $\cdot$. Da x nach Annahme nicht Null ist, existiert also x^{-1}. Aus $xy = 0$ folgt dann $x^{-1}xy = x^{-1}0$, also $1y = 0$, also $y = 0$, wie behauptet. ∎

Beispiel.

1. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ sind Körper, aber $(\mathbb{Z}, +, \cdot)$ nicht, da z. B. $2 \in \mathbb{Z}$ nicht bezüglich $\cdot$ invertierbar ist. ($2 \in \mathbb{Q}$ natürlich schon).

2. $(\mathbb{Z}_m, +, \cdot)$ ist genau dann ein Körper, wenn m eine Primzahl ist.

3. Sei $\mathbb{Q}(\sqrt{2}) := \{\, a + b\sqrt{2} : a, b \in \mathbb{Q} \,\} \subseteq \mathbb{R}$. Zusammen mit der üblichen Addition und Multiplikation aus $\mathbb{R}$ bildet $\mathbb{Q}(\sqrt{2})$ einen Ring, denn

$$\underbrace{(a + b\sqrt{2})}_{\in\mathbb{Q}(\sqrt{2})} + \underbrace{(c + d\sqrt{2})}_{\in\mathbb{Q}(\sqrt{2})} = \underbrace{(a + c) + (b + d)\sqrt{2}}_{\in\mathbb{Q}(\sqrt{2})}$$

   und

$$\underbrace{(a + b\sqrt{2})}_{\in\mathbb{Q}(\sqrt{2})}\underbrace{(c + d\sqrt{2})}_{\in\mathbb{Q}(\sqrt{2})} = \underbrace{(ac + 2bd) + (bc + ad)\sqrt{2}}_{\in\mathbb{Q}(\sqrt{2})},$$

   d. h. $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ ist abgeschlossen unter $+$ und $\cdot$ und damit ein Unterring von $\mathbb{R}$.

   Es ist außerdem ein Körper, denn

$$\begin{aligned}\frac{1}{a + b\sqrt{2}} &= \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} \\ &= \underbrace{\underbrace{\frac{a}{a^2 - 2b^2}}_{\in\mathbb{Q}} - \underbrace{\frac{b}{a^2 - 2b^2}}_{\in\mathbb{Q}}\sqrt{2}}_{\in\mathbb{Q}(\sqrt{2})}.\end{aligned}$$

   Beachte dabei, dass für $a, b \neq 0$ immer gilt $a^2 - 2b^2 \neq 0$, weil $\sqrt{2} \notin \mathbb{Q}$.

4. Sei $\mathbb{C} := \mathbb{R} \times \mathbb{R}$ mit

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

Dann ist $\mathbb{C}$ ein Körper. Man hat dort $\underset{\in\mathbb{C}}{1} = (\underset{\in\mathbb{R}}{1}, 0)$ und definiert $\mathrm{i} := (0,1)$, so dass

$$\mathbb{C} = \{\, a + b\mathrm{i} : a, b \in \mathbb{R} \,\}.$$

Beachte: $\mathrm{i}^2 = (0,1)\cdot(0,1) = (-1,0) = -1$, also „$\mathrm{i} = \sqrt{-1}$“.

Die Elemente von $\mathbb{C}$ nennt man *komplexe Zahlen.* Das Element $\mathrm{i} \in \mathbb{C}$ nennt man die *imaginäre Einheit.* Für eine komplexe Zahl $c = a + b\mathrm{i} \in \mathbb{C}$ mit $a, b \in \mathbb{R}$ nennt man $\mathrm{Re}(c) := a$ den *Realteil* und $\mathrm{Im}(c) := b$ den *Imaginärteil.*

5. Sei K ein Körper und $R = K[X]$ der Ring der Polynome über K. Dieser Ring ist kein Körper, aber man kann sich einen Körper überlegen, der $K[X]$ enthält. Und zwar so:

   Auf $R \times (R \setminus \{0\})$ wird durch

   $$(p_1, p_2) \sim (q_1, q_2) \iff \exists\, u, v \in R \setminus \{0\} : (up_1, up_2) = (vq_1, vq_2)$$

   eine Äquivalenzrelation definiert. (Beweis: Übung.) Die Elemente von $K(X) := (R \times (R \setminus \{0\}))/\!\sim$ heißen *rationale Funktionen.*

   Statt $[(p_1, p_2)]_\sim$ schreibt man $\frac{p_1}{p_2}$ und statt $\frac{p_1}{1}$ einfach p_1.

   Rationale Funktionen sind also Brüche von Polynomen, und die Äquivalenzrelation gewährleistet das Kürzen und Erweitern von Brüchen.

   Beachte: Rationale Funktionen sind **nicht** Funktionen im Sinn von Abschnitt 3, sondern heißen bloß so. In Wahrheit handelt es sich um rein algebraische Gebilde. Es ist deshalb auch egal, ob der Nenner für eine bestimmte „Belegung“ von X mit einem Element von K Null wird. Das Symbol X steht hier nicht für eine Variable, sondern für das Element $(0,1,0,0,\dots) \in K[X]$ (vgl. Bsp. 7 nach Def. 15).

   Jedenfalls gilt: $K(X)$ ist ein Körper, wenn man Addition und Multiplikation definiert durch

   $$\frac{p_1}{p_2} + \frac{q_1}{q_2} = \frac{p_1q_2 + p_2q_1}{q_1q_2},$$
   $$\frac{p_1}{p_2} \cdot \frac{q_1}{q_2} = \frac{p_1p_2}{q_1q_2}.$$

   In ganz ähnlicher Weise wie $K(X)$ aus $K[X]$ erzeugt wird, erhält man den Körper $\mathbb{Q}$ aus dem Ring $\mathbb{Z}$.

6. Sei K ein Körper und $R = K[[X]]$ der Ring der formalen Potenzreihen über K. Dieser Ring ist kein Körper, da nicht jedes $a \in R \setminus \{0\}$ ein multiplikatives Inverses in $K[[X]]$ hat. Zum Beispiel ist $a = X$ nicht invertierbar. Man kann aber zeigen, dass eine formale Potenzreihe $\sum_{n=0}^{\infty} a_n X^n$ genau dann invertierbar ist, wenn $a_0 \neq 0$ ist. Das motiviert folgende Konstruktion:

   Betrachte die Menge

   $$K((X)) := \{0\} \cup \Big\{ \sum_{n=0}^{\infty} a_n X^n \in K[[X]] : a_0 \neq 0 \Big\} \times \mathbb{Z}$$

Wir schreiben $X^e \sum_{n=0}^{\infty} a_n X^n$ oder $\sum_{n=e}^{\infty} a_{n-e} X^n$ statt $\left(\sum_{n=0}^{\infty} a_n X^n, e\right)$ und definieren Addition und Multiplikation in der Weise, die durch diese Notation suggeriert wird, also insbesondere $(X^{e_1} a_1) \cdot (X^{e_2} a_2) := X^{e_1+e_2}(a_1 a_2)$, wobei $a_1 a_2$ das Produkt in $K[[X]]$ bezeichnet. (Beachte: der Koeffizient von X^0 in $a_1 a_2$ ist genau das Produkt der Koeffizienten von X^0 in a_1 und a_2, also von Null verschieden.)

Von 0 verschiedene Elemente $X^e a \in K((X))$ kann man dann immer in $K((X))$ invertieren: $(X^e a)^{-1} = X^{-e} a^{-1}$, wobei a^{-1} das multiplikative Inverse von a in $K[[X]]$ ist.

Die Elemente von $K((X))$ heißen *formale Laurent-Reihen*.

$K((X))$ ist ein Körper.

Allgemein bedeutet „K ist ein Körper“, dass man mit den Elementen von K in gewohnter Weise rechnen kann, d. h. dass es in K eine Addition, eine Subtraktion, eine Multiplikation und eine Division gibt, die den gewohnten Rechenregeln gehorchen. Das allein ist für die Theorie der Linearen Algebra entscheidend. Es ist unbedeutend, ob wir in $\mathbb{Q}$ oder in $\mathbb{R}$ oder in irgendeinem anderen Körper rechnen. Wir werden Definitionen und Sätze deshalb für einen beliebigen Körper $\mathbb{K}$ formulieren, anstatt mehrmals für verschiedene konkrete Körper. In Beispielen betrachten wir meist $\mathbb{K} = \mathbb{Q}$ oder $\mathbb{K} = \mathbb{R}$.

Teil II

Vektoren und Matrizen

7 Vektoren

Ab jetzt sei $\mathbb{K} = (\mathbb{K}, +, \cdot)$ immer ein (beliebiger) Körper.

Definition 17. Ein Element von $\mathbb{K}^n = \mathbb{K} \times \cdots \times \mathbb{K}$ heißt *Vektor* (im engeren Sinne, vgl. Def. 29). Die *Addition* von Vektoren ist definiert durch

$$+ \colon \mathbb{K}^n \times \mathbb{K}^n \to \mathbb{K}^n, \quad (a_1, \ldots, a_n) \underset{\uparrow}{+} (b_1, \ldots, b_n) := (a_1 \underset{\uparrow}{+} b_1, a_2 + b_2, \ldots, a_n + b_n).$$

Vektor-Addition — Körper-Addition

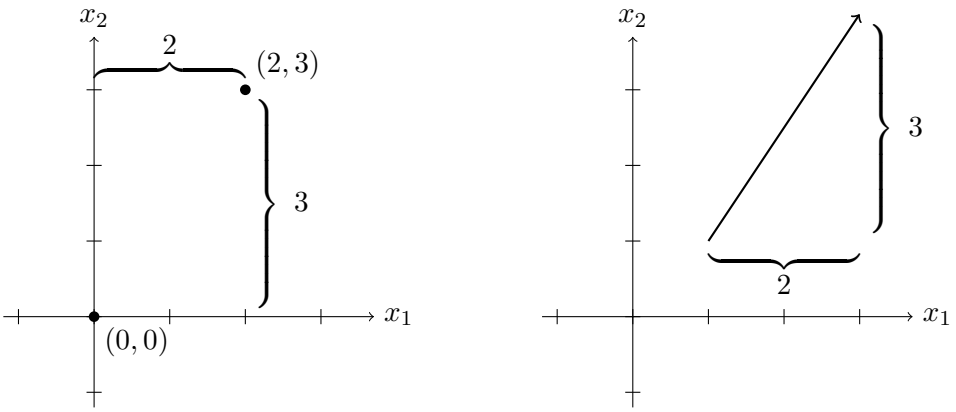
Die *Skalarmultiplikation* ist definiert durch

$$\cdot \colon \mathbb{K} \times \mathbb{K}^n \to \mathbb{K}^n, \quad \alpha \underset{\uparrow}{\cdot} (a_1, \ldots, a_n) := (\alpha \underset{\uparrow}{\cdot} a_1, \alpha\, a_2, \ldots, \alpha\, a_n).$$

Skalarmultipliation — Körper-Multiplikation

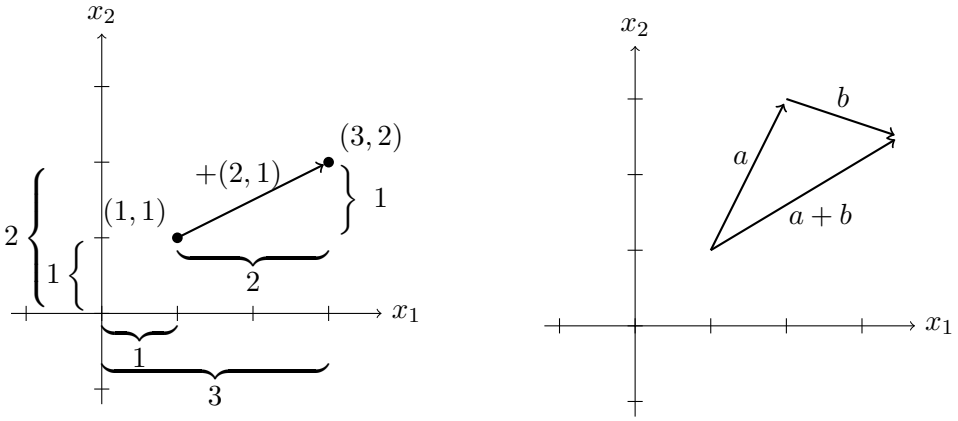
Statt $(a_1, \ldots, a_n)$ schreibt man auch $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$.

Beispiel. $\mathbb{K} = \mathbb{R}$, $n = 2$. Vektoren repräsentieren Punkte in der Ebene oder „Richtungen“.

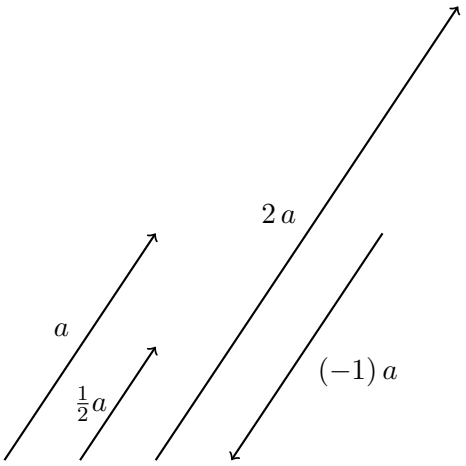


Bei der Interpretation von Richtungen als Pfeilen ist der Startpunkt des Pfeils ohne Bedeutung. Pfeile, die gleich lang sind und in die gleiche Richtung zeigen, veranschaulichen den gleichen Vektor, selbst wenn ihre Startpunkte verschieden sind.

Addition mit einem Vektor entspricht der Verschiebung eines Punktes bzw. der Kombination zweier Richtungen.



Skalarmultiplikation entspricht der Streckung oder Stauchung eines Vektors.



Für $n > 2$ ist die geometrische Anschauung entsprechend, wenn auch weniger angenehm zu zeichnen.

Satz 13. $(\mathbb{K}^n, +)$ ist eine abelsche Gruppe. Ihr Neutralelement ist $0 := (0, \ldots, 0)$.

Beweis. Folgt unmittelbar aus der Definition von $+$ und der Tatsache, dass $(\mathbb{K}, +)$ eine abelsche Gruppe mit Neutralelement 0 ist. ∎

Satz 14. Für alle $\alpha, \beta \in \mathbb{K}$ und alle $v, w \in \mathbb{K}^n$ gilt:

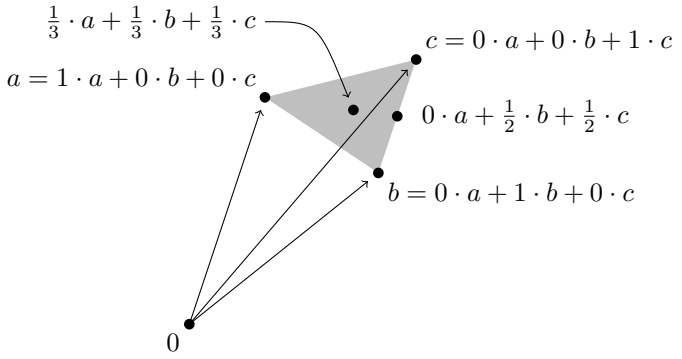
1. $(\alpha + \beta) \cdot v = \alpha \cdot v + \beta \cdot v$
2. $(\alpha\beta) \cdot v = \alpha \cdot (\beta \cdot v)$
3. $\alpha \cdot (v + w) = \alpha \cdot v + \alpha \cdot w$
4. $1 \cdot v = v$, $(-1) \cdot v = -v$
5. $\alpha v = 0 \Rightarrow \alpha = 0 \vee v = 0$

Beweis. Übung. ∎

Mit Vektoren kann man geometrische Objekte beschreiben. Zum Beispiel ist

$$\Delta(a,b,c) := \{\, \alpha a + \beta b + \gamma c : \alpha,\beta,\gamma \in [0,1], \alpha+\beta+\gamma = 1 \,\}$$

das Dreieck mit den Eckpunkten $a, b, c \in \mathbb{R}^n$:

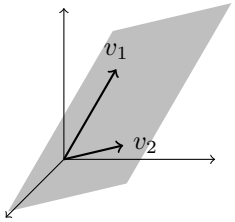


Ein Ausdruck der Form

$$\alpha_1 v_1 + \cdots + \alpha_m v_m$$

mit $\alpha_1, \ldots, \alpha_m \in \mathbb{K}$ und $v_1, \ldots, v_m \in \mathbb{K}^n$ heißt *Linearkombination* von $v_1, \ldots, v_m$. Von besonderem Interesse in der linearen Algebra sind die geometrischen Objekte, die aus allen Linearkombinationen von bestimmten gegebenen Vektoren bestehen.

Sind zum Beispiel v_1, v_2 zwei Vektoren im $\mathbb{R}^3$, so ist $\{\, \alpha v_1 + \beta v_2 : \alpha, \beta \in \mathbb{R} \,\}$ eine Ebene durch die Punkte $(0,0)$, v_1 und v_2, ...



... *es sei denn,* dass für ein bestimmtes Paar $(\alpha, \beta) \in \mathbb{R}^2 \setminus \{(0,0)\}$ gilt $\alpha v_1 + \beta v_2 = 0$. In diesem Fall wäre $\{\, \alpha v_1 + \beta v_2 : \alpha, \beta \in \mathbb{R} \,\} = \{\alpha v_1 : \alpha \in \mathbb{R}\}$ bloß eine Gerade durch die Punkte $(0,0)$ und v_1 (und v_2 ein Punkt irgendwo auf dieser Gerade), *es sei denn,* dass sogar $v_1 = v_2 = 0$ ist. In diesem Fall wäre $\{\, \alpha v_1 + \beta v_2 : \alpha, \beta \in \mathbb{R} \,\} = \{(0,0)\}$ bloß ein isolierter Punkt.

Definition 18. $v_1, \ldots, v_m \in \mathbb{K}^n$ heißen *linear abhängig,* falls es $\alpha_1, \ldots, \alpha_m \in \mathbb{K}$ gibt, von denen mindestens eins von 0 verschieden ist, und für die gilt $\alpha_1 v_1 + \cdots + \alpha_m v_m = 0$. Anderenfalls heißen $v_1, \ldots, v_m$ *linear unabhängig.*

Beispiel. Die Vektoren

$$\begin{pmatrix}1\\2\\3\end{pmatrix}, \quad \begin{pmatrix}4\\5\\6\end{pmatrix}, \quad \begin{pmatrix}7\\8\\9\end{pmatrix}$$

sind linear abhängig, weil

$$1 \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + (-2) \cdot \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} + 1 \cdot \begin{pmatrix} 7 \\ 8 \\ 9 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Achtung: Aus der paarweisen linearen Unabhängigkeit von v_i und v_j für alle i, j folgt im allgemeinen **nicht,** dass $v_1, \ldots, v_m$ insgesamt linear unabhängig sind. Im vorliegenden Beispiel sind $\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$ und $\begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix}$ linear unabhängig, und $\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$ und $\begin{pmatrix} 7 \\ 8 \\ 9 \end{pmatrix}$ sind linear unabhängig, und $\begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix}$ und $\begin{pmatrix} 7 \\ 8 \\ 9 \end{pmatrix}$ sind linear unabhängig, aber alle drei Vektoren miteinander sind abhängig.

Für Teilmengen $A \subseteq B \subseteq \mathbb{K}^n$ gilt nur: wenn A linear abhängig ist, dann auch B, und wenn B linear unabhängig ist, dann auch A. Aber aus der linearen Unabhängigkeit von A folgt nichts über die lineare Unabhängigkeit von B, und aus der linearen Abhängigkeit von B folgt nichts über die lineare Abhängigkeit von A (vgl. Satz 38 in Abschnitt 14).

Anschauung: Wenn $v_1, v_2, v_3 \in \mathbb{R}^3$ linear abhängig sind, dann liegt der Punkt v_3 in der Ebene durch die Punkte $(0, 0, 0)$, v_1 und v_2.

Satz 15. Seien $v_1, \ldots, v_m \in \mathbb{K}^n$ und

$$U := \{\, \alpha_1 v_1 + \cdots + \alpha_m v_m : \alpha_1, \ldots, \alpha_m \in \mathbb{K} \,\} \subseteq \mathbb{K}^n$$

die Menge aller Linearkombinationen von $v_1, \ldots, v_m$. Dann ist $(U, +)$ eine Untergruppe von $(\mathbb{K}^n, +)$.

Beweis. Zu zeigen: (a) $U \neq \emptyset$, (b) $\forall\ a, b \in U : a + b \in U$, (c) $\forall\ a \in U : -a \in U$.

zu (a): $0 = 0v_1 + \cdots + 0v_m \in U$.

zu (b): Seien $a, b \in U$. Nach Definition von U gibt es dann $\alpha_1, \ldots, \alpha_m \in \mathbb{K}$ und $\beta_1, \ldots, \beta_m \in \mathbb{K}$ mit

$$a = \alpha_1 v_1 + \cdots + \alpha_m v_m$$
$$b = \beta_1 v_1 + \cdots + \beta_m v_m.$$

Daraus folgt durch Addition der beiden Gleichungen

$$a + b = \underbrace{(\alpha_1 + \beta_1)}_{\in \mathbb{K}} v_1 + \cdots + \underbrace{(\alpha_m + \beta_m)}_{\in \mathbb{K}} v_m \in U.$$

zu (c): Sei $a \in U$, etwa $a = \alpha_1 v_1 + \cdots + \alpha_m v_m$ für gewisse $\alpha_1, \ldots, \alpha_m \in \mathbb{K}$. Dann gilt auch $-a = -(\alpha_1 v_1 + \cdots + \alpha_m v_m) = (-\alpha_1)v_1 + \cdots + (-\alpha_m)v_m \in U$. ∎

8 Matrizen

Definition 19. Seien $n, m, k \in \mathbb{N}$. Eine *Matrix* ist ein Element von $\mathbb{K}^{n\times m} := (\mathbb{K}^m)^n$. Schreibweise:

$$A = ((a_{i,j}))_{i=1,j=1}^{n,m} = \begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{pmatrix} \in \mathbb{K}^{n\times m}.$$

Der Vektor $\begin{pmatrix} a_{1,j} \\ \vdots \\ a_{n,j} \end{pmatrix} \in \mathbb{K}^n$ heißt die *j-te Spalte* von A, der Vektor $(a_{i,1}, \ldots, a_{i,m}) \in \mathbb{K}^m$ heißt die *i-te Zeile* von A.

Konvention: Bei einem Doppelindex (i, j) bezieht sich immer die erste Komponente auf die Zeile und die zweite auf die Spalte, in der der Matrixeintrag $a_{i,j}$ steht. Insbesondere hat eine $(n \times m)$-Matrix stets n Zeilen und m Spalten.

Für

$$A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{pmatrix} \in \mathbb{K}^{n\times m} \quad \text{und} \quad B = \begin{pmatrix} b_{1,1} & \cdots & b_{1,k} \\ \vdots & \ddots & \vdots \\ b_{m,1} & \cdots & b_{m,k} \end{pmatrix} \in \mathbb{K}^{m\times k}$$

wird das *Matrixprodukt*

$$A \cdot B := \begin{pmatrix} c_{1,1} & \cdots & c_{1,k} \\ \vdots & \ddots & \vdots \\ c_{n,1} & \cdots & c_{n,k} \end{pmatrix} \in \mathbb{K}^{n\times k}$$

definiert durch $c_{i,j} := \sum_{\ell=1}^{m} a_{i,\ell} b_{\ell,j}$ $(i = 1, \ldots, n,\ j = 1, \ldots, k)$.

Beispiel.

1.
$$\begin{pmatrix} \boxed{1 & 2 & 3} \\ 4 & 5 & 6 \end{pmatrix} \begin{pmatrix} \boxed{1} & -1 \\ \boxed{3} & 0 \\ \boxed{2} & 4 \end{pmatrix} = \begin{pmatrix} \boxed{1\cdot 1 + 2\cdot 3 + 3\cdot 2} & 1\cdot(-1) + 2\cdot 0 + 3\cdot 4 \\ 4\cdot 1 + 5\cdot 3 + 6\cdot 2 & 4\cdot(-1) + 5\cdot 0 + 6\cdot 4 \end{pmatrix}$$
$$= \begin{pmatrix} 13 & 11 \\ 31 & 20 \end{pmatrix} \in \mathbb{R}^{2\times 2}.$$

2.
$$\begin{pmatrix} 1 & -1 \\ \boxed{3 & 0} \\ 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & \boxed{3} \\ 4 & 5 & \boxed{6} \end{pmatrix} = \begin{pmatrix} 1\cdot 1 + (-1)\cdot 4 & 1\cdot 2 + (-1)\cdot 5 & 1\cdot 3 + (-1)\cdot 6 \\ 3\cdot 1 + 0\cdot 4 & 3\cdot 2 + 0\cdot 5 & \boxed{3\cdot 3 + 0\cdot 6} \\ 2\cdot 1 + 4\cdot 4 & 2\cdot 2 + 4\cdot 5 & 2\cdot 3 + 4\cdot 6 \end{pmatrix}$$
$$= \begin{pmatrix} -3 & -3 & -3 \\ 3 & 6 & 9 \\ 18 & 24 & 30 \end{pmatrix} \in \mathbb{R}^{3\times 3}$$

3. Das Matrixprodukt
$$\begin{pmatrix} 1 & 3 & 0 \\ -1 & 2 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$$
ist nicht definiert. Die Formate passen nicht. In einem Matrixprodukt $A \cdot B$ muss A genau so viele Spalten haben wie B Zeilen hat.

4. Vektoren (d. h. Elemente von $\mathbb{K}^n$) lassen sich als spezielle Matrizen auffassen, je nach Bedarf als Elemente von $\mathbb{K}^{1\times n}$ (dann spricht man von Zeilenvektoren) oder von $\mathbb{K}^{n\times 1}$ (dann spricht man von Spaltenvektoren). Insbesondere kann man Matrizen mit Vektoren multiplizieren, wenn die Formate passen. Zum Beispiel:

$$\begin{pmatrix}1 & 2 & 3\\ 4 & 5 & 6\\ 7 & 8 & 9\end{pmatrix}\begin{pmatrix}1\\ -1\\ 2\end{pmatrix} = \begin{pmatrix}1\cdot 1+2\cdot(-1)+3\cdot 2\\ 4\cdot 1+5\cdot(-1)+6\cdot 2\\ 7\cdot 1+8\cdot(-1)+9\cdot 2\end{pmatrix} = \begin{pmatrix}5\\ 11\\ 17\end{pmatrix}$$

$$(1,-1,2)\cdot\begin{pmatrix}1 & 2 & 3\\ 4 & 5 & 6\\ 7 & 8 & 9\end{pmatrix} = (11,13,15).$$

   Für Vektoren in $\mathbb{K}^n$ wollen wir uns nicht festlegen, ob sie nun Zeilen- oder Spaltenvektoren sein sollen. Es sind einfach Vektoren. Wenn es auf eine bestimmte Interpretation ankommt, wird immer aus dem Zusammenhang klar sein, welche gemeint ist.

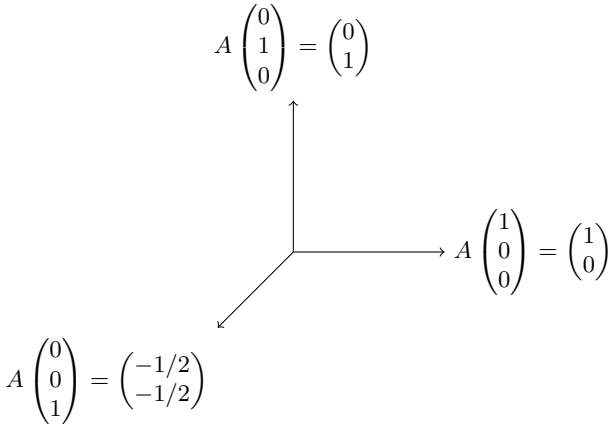
   Insbesondere wollen wir folgende notationelle Konvention machen: Sind $v_1,\dots,v_m \in \mathbb{K}^n$ Vektoren, so bezeichnet $(v_1, v_2, \dots, v_m) \in \mathbb{K}^{n\times m}$ die Matrix, deren Spalten die $v_1,\dots,v_m$ sind. (Dabei werden die v_j also als Spaltenvektoren interpretiert.) Dagegen soll mit der Notation $\begin{pmatrix}v_1\\ \vdots\\ v_m\end{pmatrix} \in \mathbb{K}^{m\times n}$ die Matrix gemeint sein, deren Zeilen die $v_1,\dots,v_m$ sind. (Dabei werden die v_i also als Zeilenvektoren interpretiert.)

Eine Matrix $A \in \mathbb{K}^{n\times m}$ beschreibt eine Funktion $\phi\colon \mathbb{K}^m \to \mathbb{K}^n$, $\phi(v) := A\cdot v$. Diese Funktion „transformiert“ den Raum $\mathbb{K}^m$ auf eine bestimmte Weise in (eine Teilmenge von) $\mathbb{K}^n$. Eine klassische Anwendung ist das Zeichnen von dreidimensionalen Objekten auf zweidimensionalem Papier. Hierbei ist $m = 3$, $n = 2$, und eine mögliche Matrix ist

$$A = \begin{pmatrix}1 & 0 & -1/2\\ 0 & 1 & -1/2\end{pmatrix}.$$

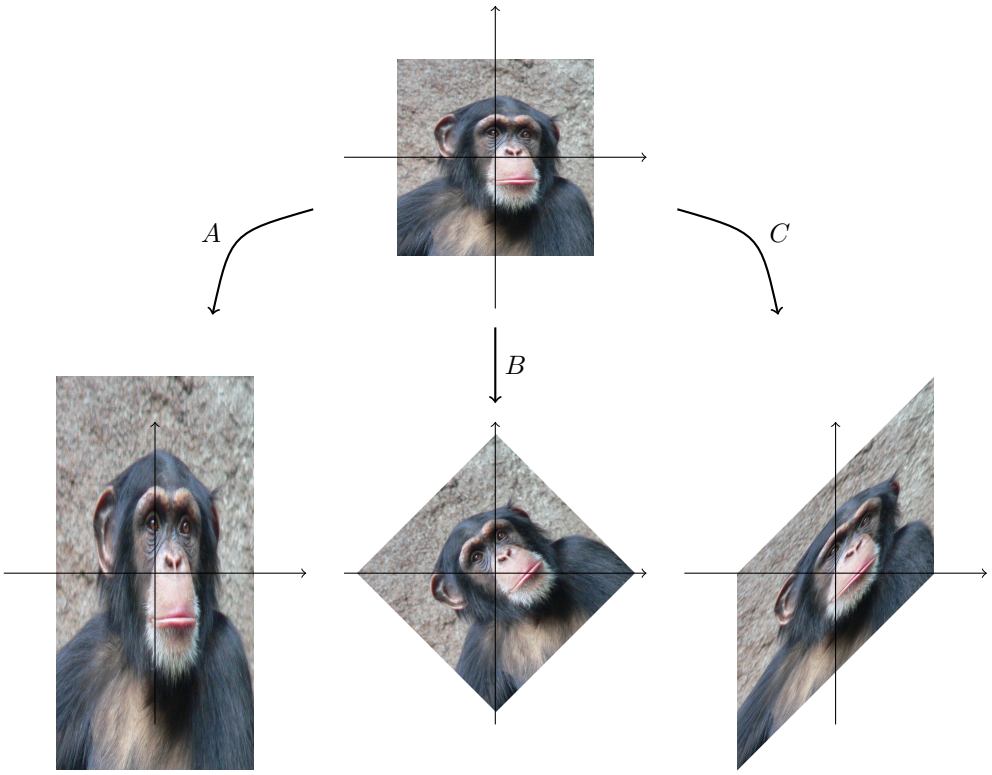
Ein Punkt $(x, y, z) \in \mathbb{R}^3$ wird von A auf den Punkt $(x - \frac{1}{2}z, y - \frac{1}{2}z) \in \mathbb{R}^2$ abgebildet. Beachte, dass mehrere Punkte der Ebene dasselbe Urbild im dreidimensionalen Raum haben koennen. Zum Beispiel ist $(1, 1, 0) \neq (2, 2, 2)$, aber $\phi(1, 1, 0) = \phi(2, 2, 2) = (1, 1)$.

Ist $A \in \mathbb{K}^{n\times m}$ und ist $e_i = (0,\dots,0,1,0,\dots,0)$ der i-te *Einheitsvektor,* also der Vektor, an dessen i-ter Komponente eine 1 steht und dessen andere Komponenten alle 0 sind, so ist $A \cdot e_j$ genau die j-te Spalte von A und $e_i \cdot A$ die i-te Zeile. Die Spalten von A zeigen also an, auf welche Punkte die Einheitsvektoren abgebildet werden.



Weitere Beispiele im Fall $n = m = 2$:

- $A = \begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}$ dehnt die Ebene in vertikaler Richtung.
- $B = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}$ dreht die Ebene um 45 Grad entgegen dem Uhrzeigersinn.
- $C = \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$ bewirkt eine sogenannte *Scherung* der Ebene.



Satz 16. Für alle $A \in \mathbb{K}^{n\times m}$, $B \in \mathbb{K}^{m\times k}$, $C \in \mathbb{K}^{k\times \ell}$ gilt $(A \cdot B) \cdot C = A \cdot (B \cdot C)$.

Beweis. Seien $A = ((a_{i,j}))_{i=1,j=1}^{n,m}$, $B = ((b_{i,j}))_{i=1,j=1}^{m,k}$, $C = ((c_{i,j}))_{i=1,j=1}^{k,\ell}$. Der (i,j)-te Eintrag von $(A \cdot B) \cdot C$ lautet dann

$$\sum_{u=1}^{k}\left(\sum_{v=1}^{m} a_{i,v}b_{v,u}\right)c_{u,j} = \sum_{u=1}^{k}\sum_{v=1}^{m} a_{i,v}b_{v,u}c_{u,j} = \sum_{v=1}^{m}\sum_{u=1}^{k} a_{i,v}b_{v,u}c_{u,j} = \sum_{v=1}^{m}\left(a_{i,v}\sum_{u=1}^{k} b_{v,u}c_{u,j}\right),$$

und letzteres ist gerade der (i,j)-te Eintrag von $A \cdot (B \cdot C)$. Da alle Einträge von $(A \cdot B) \cdot C$ und $A \cdot (B \cdot C)$ übereinstimmen, folgt die Behauptung. ∎

Daraus folgt insbesondere, dass Matrixmultiplikation der Verkettung der entsprechenden Funktionen entspricht. Außerdem folgt, dass $(\mathbb{K}^{n\times n}, \cdot)$ ein Monoid ist, mit der sogenannten *Einheitsmatrix*

$$I_n := \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

als Neutralelement. Ist es auch eine Gruppe?

Beispiel.

1. $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ ist invertierbar: für $B = \begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix}$ gilt
$$A \cdot B = B \cdot A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2.$$

2. $A = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ ist nicht invertierbar, denn gäbe es eine Inverse $B = \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix}$, dann müsste gelten:
$$\begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b_{1,1}+b_{1,2} & 0 \\ b_{2,1}+b_{2,2} & 0 \end{pmatrix} \stackrel{!}{=} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$
also
$$\begin{aligned} b_{1,1}+b_{1,2} &= 1 \qquad & 0 &= 0 \\ b_{2,1}+b_{2,2} &= 0 \qquad & 0 &= 1. \end{aligned}$$
Die vierte Gleichung ist offensichtlich nicht zu erfüllen, egal wie wir die $b_{i,j}$ wählen.

Definition 20. $\mathrm{GL}(n,\mathbb{K}) := \{\, A \in \mathbb{K}^{n\times n} : \exists\, B \in \mathbb{K}^{n\times n} : AB = BA = I_n \,\}$ heißt die *lineare Gruppe* der Größe n über dem Körper $\mathbb{K}$.
Die Matrix B mit $AB = BA = I_n$ heißt *Inverse* von A. Notation: $A^{-1} = B$.

Wegen Satz 16 ist klar, dass $\mathrm{GL}(n,\mathbb{K})$ zusammen mit der Matrixmultiplikation eine Gruppe bildet. Diese Gruppe ist nicht kommutativ, z. B. gilt

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix} = \begin{pmatrix} 19 & 22 \\ 43 & 50 \end{pmatrix},$$
$$\begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 23 & 34 \\ 31 & 46 \end{pmatrix}.$$

In diesem Zusammenhang sei an die Rechenregel $(AB)^{-1} = B^{-1}A^{-1}$ erinnert.

Satz 17.

1. $\mathbb{K}^{n\times n}$ bildet zusammen mit der Addition

$$\begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{pmatrix} + \begin{pmatrix} b_{1,1} & \cdots & b_{1,m} \\ \vdots & \ddots & \vdots \\ b_{n,1} & \cdots & b_{n,m} \end{pmatrix} := \begin{pmatrix} a_{1,1}+b_{1,1} & \cdots & a_{1,m}+b_{1,m} \\ \vdots & \ddots & \vdots \\ a_{n,1}+b_{n,1} & \cdots & a_{n,m}+b_{n,m} \end{pmatrix}$$

und der Matrixmultiplikation einen (nicht-kommutativen!) Ring mit Eins.

2. Für die Skalarmultiplikation

$$\cdot\colon \mathbb{K}\times\mathbb{K}^{n\times m}\to\mathbb{K}^{n\times m},\quad \alpha\begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{pmatrix} := \begin{pmatrix} \alpha a_{1,1} & \cdots & \alpha a_{1,m} \\ \vdots & \ddots & \vdots \\ \alpha a_{n,1} & \cdots & \alpha a_{n,m} \end{pmatrix}$$

und die Addition gelten die Gesetze $\alpha(A+B)=\alpha A+\alpha B$, $(\alpha+\beta)A=\alpha A+\beta A$, $(\alpha\beta)A=\alpha(\beta A)$, $1A=A$, und $(\alpha A)C=\alpha(AC)$, jeweils für alle $\alpha,\beta\in\mathbb{K}$, $A,B\in\mathbb{K}^{n\times m}$, $C\in\mathbb{K}^{m\times k}$.

Beweis. Übung. ∎

Definition 21. Die *Transposition* von Matrizen ist definiert durch

$$\cdot^\top\colon \mathbb{K}^{n\times m}\to\mathbb{K}^{m\times n},\quad \begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{pmatrix}^\top = \begin{pmatrix} a_{1,1} & \cdots & a_{n,1} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{n,m} \end{pmatrix}.$$

Beispiel. $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}^\top = \begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{pmatrix}$.

Satz 18.

1. Für alle $A\in\mathbb{K}^{n\times m}$ und $B\in\mathbb{K}^{m\times k}$ gilt $(AB)^\top=B^\top A^\top$.
2. Für alle $A\in\mathrm{GL}(n,\mathbb{K})$ gilt $(A^\top)^{-1}=(A^{-1})^\top$.

Beweis.

1. Es seien $a_{i,j}$ und $b_{i,j}$ die Einträge von A bzw. B in der i-ten Zeile und j-ten Spalte. Der (i,j)-te Eintrag von $(AB)^\top$ ist nach Definition der Transposition gleich dem (j,i)-ten Eintrag von AB, und dieser ist nach Definition der Matrixmultiplikation gleich

$$\sum_{\ell=1}^{m} a_{j,\ell}b_{\ell,i}.$$

Der (i,j)-te Eintrag von $B^\top A^\top$ ist

$$\sum_{\ell=1}^{m} \underbrace{b_{\ell,i}}_{\substack{\uparrow \\ (i,\ell)\text{-Eintrag von } B^\top}} \underbrace{a_{j,\ell}}_{\substack{\uparrow \\ (\ell,j)\text{-Eintrag von } A^\top}} = \sum_{\ell=1}^{m} a_{j,\ell} b_{\ell,i}.$$

Die Einträge sind also gleich.

2. Es gilt $AA^{-1} = I_n$. Mit Teil 1 des Satzes folgt

$$\underbrace{(AA^{-1})^\top}_{=(A^{-1})^\top A^\top} = I_n^\top = I_n,$$

also $(A^{-1})^\top A^\top = I_n$. ∎

Definition 22. Sei $\pi \in S_n$ eine Permutation. Dann heißt die Matrix $A = ((a_{i,j}))_{i,j=1}^n \in \mathbb{K}^{n\times n}$ mit

$$a_{i,j} = \begin{cases} 1 & \text{falls } \pi(i) = j \\ 0 & \text{sonst} \end{cases}$$

die zu π gehörige *Permutationsmatrix.*

Beispiel. Die zu $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} \in S_4$ gehörige Permutationsmatrix lautet

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Zum Beispiel steht in Zeile 2 eine Eins in der vierten Spalte, weil $\pi(2) = 4$ ist.

Multiplikation einer Permutationsmatrix mit einem Vektor permutiert die Einträge des Vektors:

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} 0a+1b+0c+0d \\ 0a+0b+0c+1d \\ 0a+0b+1c+0d \\ 1a+0b+0c+0d \end{pmatrix} = \begin{pmatrix} b \\ d \\ c \\ a \end{pmatrix}.$$

A ist genau dann eine Permutationsmatrix, wenn in jeder Zeile und in jeder Spalte genau eine Eins und sonst nur Nullen stehen.

Satz 19. Es sei P_π die Permutationsmatrix zu einer Permutation $\pi \in S_n$. Dann gilt:

1. $\forall\ \pi, \sigma \in S_n : P_{\sigma\pi} = P_\pi P_\sigma$,
2. $\forall\ \pi \in S_n : P_{\pi^{-1}} = P_\pi^{-1} = P_\pi^\top$.
3. Für jede Matrix $A = ((a_{i,j}))_{i,j=1}^n$ und jede Permutation $\pi \in S_n$ gilt

$$((a_{\pi(i),\pi(j)}))_{i,j=1}^n = P_\pi A P_\pi^{-1}.$$

Beweis.

1. Seien $\pi, \sigma \in S_n$ beliebig. Nach Definition ist

$$P_\pi = ((a_{i,j}))_{i,j=1}^n \quad \text{mit } a_{i,j} = \begin{cases} 1 & \text{falls } \pi(i) = j \\ 0 & \text{sonst} \end{cases}$$
$$P_\sigma = ((b_{i,j}))_{i,j=1}^n \quad \text{mit } b_{i,j} = \begin{cases} 1 & \text{falls } \sigma(i) = j \\ 0 & \text{sonst} \end{cases}$$

   Sei $P_\pi P_\sigma = ((c_{i,j}))_{i,j=1}^n$. Dann gilt:

$$\begin{aligned} c_{i,j} &= \sum_{k=1}^{n} \underbrace{a_{i,k} b_{k,j}}_{= \begin{cases} 1 & \text{falls } \pi(i) = k \text{ und } \sigma(k) = j \\ 0 & \text{sonst} \end{cases}} \\ &= \begin{cases} 1 & \text{falls } \sigma(\pi(i)) = j \\ 0 & \text{sonst} \end{cases} \\ &= \begin{cases} 1 & \text{falls } (\sigma\pi)(i) = j \\ 0 & \text{sonst} \end{cases} \end{aligned}$$

2. Aus der Definition folgt unmittelbar $P_{\mathrm{id}} = I_n$. Unter Verwendung von Teil 1 erhält man daraus

$$I_n = P_{\mathrm{id}} = P_{\pi\pi^{-1}} = P_{\pi^{-1}} P_\pi,$$

   und damit $P_\pi^{-1} = P_{\pi^{-1}}$.

   Die Behauptung $P_{\pi^{-1}} = P_\pi^\top$ folgt aus $\pi(i) = j \iff \pi^{-1}(j) = i$.

3. Wir verwenden die Notation

$$\delta_{u,v} := \begin{cases} 1 & \text{falls } u = v \\ 0 & \text{sonst} \end{cases}$$

   für $u, v \in \mathbb{N}$. Für den Eintrag an Position (i, j) von $P_\pi^{-1} A P_\pi$ ergibt sich unter Verwendung von Teil 2

$$\underbrace{\sum_{k=1}^{n} \delta_{\pi(i),k} \underbrace{\sum_{l=1}^{n} a_{k,l} \delta_{l,\pi(j)}}_{a_{k,\pi(j)}}}_{= a_{\pi(i),\pi(j)}},$$

   wie behauptet. ∎

Die Abbildung $h\colon S_n \to \mathrm{GL}(n, \mathbb{K})$, $\pi \mapsto P_{\pi^{-1}}$ ist ein injektiver Gruppenhomomorphismus.

9 Gleichungssysteme

Viele Probleme in der linearen Algebra lassen sich zurückführen auf ein Problem von folgendem Typ:

> Gegeben $A \in \mathbb{K}^{n\times m}$, finde alle $x \in \mathbb{K}^m$, so dass $Ax = 0 \in \mathbb{K}^n$.

Man nennt dieses Problem ein *lineares Gleichungssystem* und $L = \{\, x \in \mathbb{K}^m : Ax = 0 \,\}$ dessen Lösungsmenge. Jedes Element $x \in L$ heißt *Lösung* des Gleichungssystems. Man sagt auch, L ist der *Kern* der Matrix A, Notation: $\ker A := L$.

- Wie findet man Lösungen eines linearen Gleichungssystems?
- Was lässt sich über die Struktur der Lösungsmenge sagen?

Schreibe

$$A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{pmatrix}$$

für die bekannten Daten und

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}$$

für die unbekannten Daten. Dann lautet das Problem also, alle $x_1, \ldots, x_m \in \mathbb{K}$ zu finden mit

$$\begin{aligned} & a_{1,1}x_1 + \cdots + a_{1,m}x_m = 0 \\ \wedge \quad & a_{2,1}x_1 + \cdots + a_{2,m}x_m = 0 \\ \wedge \quad & \cdots \\ \wedge \quad & a_{n,1}x_1 + \cdots + a_{n,m}x_m = 0. \end{aligned}$$

Das System besteht aus n Gleichungen und m Variablen.
Beispiel:

$$\begin{aligned} 2x_1 + 7x_2 &= 0 \\ 3x_1 - 2x_2 &= 0. \end{aligned}$$

Beobachtung: Die Lösungsmenge ändert sich nicht, wenn man

- Gleichungen mit einer von 0 verschiedenen Konstanten multipliziert,
- Das c-fache einer Gleichung zu einer anderen Gleichung dazuaddiert, für ein beliebiges $c \in \mathbb{K}$,
- Gleichungen vertauscht.

All diese Operationen lassen sich durch eine Operation vom gleichen Typ wieder rückgängig machen.

Idee: Verwende diese Operationen, um ein gegebenes Gleichungssystem systematisch in eine Form zu bringen, aus der sich die Lösungen leicht ablesen lassen.

Beispiel.

1.

$$\begin{array}{rl} & \begin{array}{r|l} \text{I} & 2x_1 + 7x_2 = 0 \\ \text{II} & 3x_1 - 2x_2 = 0 \end{array} \\ \overset{\text{II}\to\text{II}-\frac{3}{2}\text{I}}{\iff} & \begin{array}{r|l} \text{I} & 2x_1 + 7x_2 = 0 \\ \text{II} & 0x_1 - \frac{25}{2}x_2 = 0 \end{array} \\ \overset{\text{II}\to-\frac{2}{25}\text{II}}{\iff} & \begin{array}{r|l} \text{I} & 2x_1 + 7x_2 = 0 \\ \text{II} & 0x_1 + 1x_2 = 0 \end{array} \\ \overset{\text{I}\to\text{I}-7\text{II}}{\iff} & \begin{array}{r|l} \text{I} & 2x_1 + 0x_2 = 0 \\ \text{II} & 0x_1 + 1x_2 = 0 \end{array} \\ \overset{\text{I}\to\frac{1}{2}\text{I}}{\iff} & \begin{array}{r|l} \text{I} & 1x_1 + 0x_2 = 0 \\ \text{II} & 0x_1 + 1x_2 = 0 \end{array} \\ \iff & (x_1, x_2) = (0, 0) \end{array}$$

Also ist in diesem Fall $L = \{\binom{0}{0}\}$ die Lösungsmenge des Gleichungssystems.

Handlichere Schreibweise für die gleiche Rechnung:

$$\begin{pmatrix} 2 & 7 \\ 3 & -2 \end{pmatrix} \begin{matrix} \\ \leftarrow\!\!\rfloor{\scriptstyle -3/2} \\ \leftarrow\!\!\rfloor{\scriptstyle +} \end{matrix} \leftrightarrow \begin{pmatrix} 2 & 7 \\ 0 & -\frac{25}{2} \end{pmatrix} \mid \cdot -\frac{2}{25} \leftrightarrow$$
$$\begin{pmatrix} 2 & 7 \\ 0 & 1 \end{pmatrix} \begin{matrix} \leftarrow\!\!\rfloor{\scriptstyle +} \\ \leftarrow\!\!\rfloor{\scriptstyle -7} \end{matrix} \leftrightarrow \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \mid \cdot \frac{1}{2} \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

2.

$$\begin{array}{rl} & \begin{array}{r|l} \text{I} & 2x_1 - 3x_2 = 0 \\ \text{II} & -4x_1 + 6x_2 = 0 \end{array} \\ \overset{\text{II}\to\text{II}+2\text{I}}{\iff} & \begin{array}{r|l} \text{I} & 2x_1 - 3x_2 = 0 \\ \text{II} & 0x_1 + 0x_2 = 0 \end{array} \\ \iff & 2x_1 - 3x_2 = 0 \end{array}$$

In diesem Fall kann x_2 beliebig gewählt werden, z. B. $x_2 = \alpha \in \mathbb{Q}$, und für jede Wahl gibt es genau eine passende Wahl von x_1, nämlich $x_1 = \frac{3}{2}\alpha$. Die Lösungsmenge hat also die Gestalt

$$L = \{\, \alpha \begin{pmatrix} 3/2 \\ 1 \end{pmatrix} : \alpha \in \mathbb{Q} \,\}.$$

3. Ein Beispiel mit drei Gleichungen und drei Variablen:

$$\begin{array}{r|l} \text{I} & 0x_1 + 4x_2 - x_3 = 0 \\ \text{II} & 1x_1 + 2x_2 + 0x_3 = 0 \\ \text{III} & 1x_1 - x_2 + 2x_3 = 0 \end{array}$$

Wir verwenden gleich die handlichere Schreibweise:

$$\begin{pmatrix} 0 & 4 & -1 \\ 1 & 2 & 0 \\ 1 & -1 & 2 \end{pmatrix} \overset{\leftarrow}{\leftarrow} \leftrightarrow \begin{pmatrix} 1 & 2 & 0 \\ 0 & 4 & -1 \\ 1 & -1 & 2 \end{pmatrix} \overset{-1}{\underset{+}{\leftarrow}} \leftrightarrow$$

$$\begin{pmatrix} 1 & 2 & 0 \\ 0 & 4 & -1 \\ 0 & -3 & 2 \end{pmatrix} \overset{\frac{3}{4}}{\underset{+}{\leftarrow}} \leftrightarrow \begin{pmatrix} 1 & 2 & 0 \\ 0 & 4 & -1 \\ 0 & 0 & \frac{5}{4} \end{pmatrix} \mid \cdot \tfrac{4}{5} \leftrightarrow \begin{pmatrix} 1 & 2 & 0 \\ 0 & 4 & -1 \\ 0 & 0 & 1 \end{pmatrix} \overset{+}{\leftarrow} \leftrightarrow$$

$$\begin{pmatrix} 1 & 2 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 1 \end{pmatrix} \overset{+}{\underset{-2}{\leftarrow}} \mid \cdot \tfrac{1}{4} \leftrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Die Lösungsmenge ist also offensichtlich $L = \{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \}$.

Definition 23.

1. Eine Matrix A heißt in *Treppenform* (TF) (engl. *echelon form*), falls gilt:

   (a) $A = (1, *, *, \ldots, *) \in \mathbb{K}^{1 \times m}$, oder

   (b) $A = 0$, oder

   (c) $A = \begin{pmatrix} 1 & * & \cdots & * \\ 0 & & & \\ \vdots & & B & \\ 0 & & & \end{pmatrix}$ für eine Matrix $B \in \mathbb{K}^{(n-1)\times(m-1)}$ in Treppenform, oder

   (d) $A = \begin{pmatrix} 0 & & & \\ \vdots & & B & \\ 0 & & & \end{pmatrix}$ für eine Matrix $B \in \mathbb{K}^{n\times(m-1)}$ in Treppenform.

   Dabei stehen die Symbole $*$ für beliebige (nicht notwendigerweise identische) Elemente von $\mathbb{K}$.

2. Ist A in Treppenform, so heißen die Stellen (i, j) mit $a_{i,1} = a_{i,2} = \cdots = a_{i,j-1} = 0$ und $a_{i,j} = 1$ die *Treppenstufen* von A.

3. A heißt *Treppennormalform* (TNF) (engl. *reduced echelon form*), falls A in Treppenform ist und zusätzlich für alle ihre Treppenstufen (i, j) gilt $a_{1,j} = a_{2,j} = \cdots = a_{i-1,j} = 0$.

Beispiel. Eine Matrix in Treppenform:

$$\begin{pmatrix} 1 & * & * & * & * & * & * & * & * & * & * & * & * & * & * \\ 0 & 0 & 1 & * & * & * & * & * & * & * & * & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & * & * & * & * & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & * & * & * & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & * & * & * & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Eine Matrix in Treppennormalform:

$$\begin{pmatrix} 1 & * & 0 & * & * & * & 0 & 0 & 0 & * & * & 0 & * & * & * \\ 0 & 0 & 1 & * & * & * & 0 & 0 & 0 & * & * & 0 & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & * & * & 0 & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & * & * & 0 & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & * & * & 0 & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & * & * & * \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

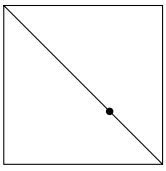
Definition 24. Zwei Matrizen $A, B \in \mathbb{K}^{n\times m}$ heißen *äquivalent,* geschrieben $A \leftrightarrow B$, falls es Matrizen $E_1, \ldots, E_k \in \mathbb{K}^{n\times n}$ gibt, so dass $A = E_k E_{k-1} \cdots E_1 B$, wobei jedes E_i eine der folgenden drei möglichen Formen hat:

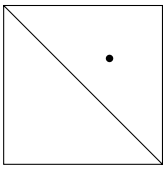
1. Alle Einträge jenseits der Diagonalen sind 0, die Einträge auf der Diagonale sind nicht 0, und mindestens $n-1$ dieser Einträge sind 1.

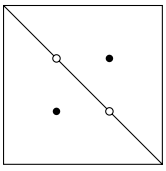
2. Alle Einträge auf der Diagonalen sind 1, die Einträge jenseits der Diagonale sind bis auf höchstens eine Ausnahme 0.

3. Eine Permutationsmatrix für eine Permutation, die $n-2$ Punkte fest lässt und die beiden anderen miteinander vertauscht.

Matrizen dieser Form heißen *Elementarmatrizen.*

1. 

2. 

3. 

Beachte: Die Multiplikation einer Matrix von links mit einer dieser Matrizen entspricht genau der Anwendung der vorher genannten Zeilenoperationen. Multiplikation dieser Matrizen von rechts bewirkt die entsprechende Operation auf den Spalten der Matrix.

Satz 20.

1. $\leftrightarrow$ ist eine Äquivalenzrelation auf $\mathbb{K}^{n\times m}$.
2. Jede Äquivalenzklasse enthält genau eine Matrix in Treppenormalform.
3. Zwei Matrizen haben genau dann den gleichen Kern, wenn sie äquivalent sind.

Beweis. (Skizze)

1. Übung.
2. Dass es mindestens eine TNF gibt, ergibt sich aus dem im folgenden beschriebenen Gauß-Algorithmus, der eine solche Form berechnet.

   Für die Eindeutigkeit argumentiert man per Induktion über die Anzahl der Spalten der Matrix und verwendet die rekursive Struktur der Definition.
3. Man konstruiert eine bijektive Abbildung zwischen den Matrizen in Treppennormalform und den Mengen, die als Lösungsmenge eines Gleichungssystems auftreten können. ∎

Diese Argumente sind zugegebenermaßen nicht das, was wir normalerweise unter einem Beweis verstehen. Das ist unbefriedigend, zumal der Satz durchaus eine zentrale Bedeutung für den Aufbau der linearen Algebra hat und man tunlichts vermeiden sollte, Folgerungen aus Behauptungen zu ziehen, die nicht lückenlos bewiesen wurden. Selbstverständlich kann man den Beweis des Satzes auch nach allen Regeln der Kunst formal sauber aufschreiben. Nur wird er dann recht technisch und länglich, und man sieht nicht wirklich, was vor sich geht. Wir wollen deshalb ausnahmsweise darauf verzichten, und uns bloß anhand von Beispielen von der Richtigkeit der Aussagen überzeugen. Wer dem nicht traut, sollte keine Schwierigkeiten haben, in der einschlägigen Literatur einen ausformulierten formalen Beweis zu finden.

Um die Lösungsmenge eines Gleichungssystems zu bestimmen, bringt man die Matrix zuerst in Treppennormalform. Daraus kann man dann eine explizite Darstellung der Lösungsmenge ablesen. Wir formulieren dieses Vorgehen als drei separate Algorithmen. Der erste bringt eine gegebene Matrix in Treppenform, der zweite eine gegebene Treppenform in Treppennormalform, und der dritte bestimmt aus einer gegebenen Treppennormalform eine Beschreibung des Kerns. Alle drei Algorithmen bezeichnet man als *Gauß-Algorithmus* oder *Gauß-Elimination.*

Algorithmus 1. Eingabe: $A = ((a_{i,j}))_{i=1,j=1}^{n,m} \in \mathbb{K}^{n\times m}$
Ausgabe: Eine zu A äquivalente Treppenform.

```
1   r := 1
2   für c = 1, ..., m:
3     wenn ∃ p ∈ {r, ..., n} : A[p, c] ≠ 0, dann:
4       wähle so ein p
5       wenn p ≠ r, dann vertausche die Zeilen p und r
6       multipliziere die Zeile r mit 1/A[r, c]
7       für i = r + 1, ..., n:
8         addiere das (−A[i, c])-fache der Zeile r zur Zeile i
9       r := r + 1
```

10 gib A als Ergebnis zurück

Der Algorithmus ist so beschrieben, dass er die Einträge der Matrix A im Laufe der Rechnung verändert. Mit der Notation $A[i,j]$ sind die Körperelemente gemeint, die zum aktuellen Zeitpunkt gerade an Position (i,j) in der Matrix stehen. Insbesondere gilt also $A[r,c] \neq 0$ in Schritt 6, denn durch die Vertauschung in Schritt 5 steht jetzt in Schritt r, was vorher in Zeile p stand, und diese Zeile war in Schritt 4 gerade so gewählt, dass $A[p,c] \neq 0$ ist.

Algorithmus 2. Eingabe: $A \in \mathbb{K}^{n\times m}$ in Treppenform
Ausgabe: Eine zu A äquivalente Treppennormalform.

1 für $r = n, \ldots, 1$:

2 wenn $\exists\, j \in \{1,\ldots,m\} : A[r,j] \neq 0$, dann:

3 wähle das kleinste solche j

4 für $i = 1, \ldots, r-1$:

5 addiere das $(-A[i,j])$-fache von Zeile r zur Zeile i

6 gib A als Ergebnis zurück

Beispiel. Wie kommt man von einer TNF zur entsprechenden Lösungsmenge? Betrachte

$$\begin{pmatrix} 1 & 0 & 3 & 0 & 6 & 0 \\ & 1 & 2 & 0 & 5 & 0 \\ & & & 1 & 4 & 0 \\ & & & & & 1 \end{pmatrix}.$$

Als Gleichungssystem geschrieben:

$$\begin{array}{c|cccccccc} \text{I} & x_1 & & +3x_3 & & +6x_5 & & = 0 \\ \text{II} & & x_2 & +2x_3 & & +5x_5 & & = 0 \\ \text{III} & & & & x_4 & +4x_5 & & = 0 \\ \text{IV} & & & & & & x_6 & = 0 \end{array}$$

Wir stellen jede Gleichung nach der ersten vorkommenden Variablen frei und ergänzen zur Verdeutlichung der Situation triviale Gleichungen für die Variablen, die keine eigene Gleichung haben:

$$\begin{aligned} x_1 &= -3x_3 - 6x_5 \\ x_2 &= -2x_3 - 5x_5 \\ x_3 &= x_3 \\ x_4 &= -4x_5 \\ x_5 &= x_5 \\ x_6 &= 0 \end{aligned}$$

In dieser Darstellung sieht man, dass die Lösungsmenge von zwei frei wählbaren Parametern abhängt, die x_3 und x_5 entsprechen. Für jede (beliebige) Wahl von x_3 und x_5 sind die Werte aller anderen Variablen dann eindeutig bestimmt. Die Lösungsmenge lässt sich also schreiben

als

$$L = \Big\{ \alpha \begin{pmatrix} -3 \\ -2 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} -6 \\ -5 \\ 0 \\ -4 \\ 1 \\ 0 \end{pmatrix} : \alpha, \beta \in \mathbb{Q} \Big\}.$$

Trick: Die Vektoren, die in der Beschreibung der Lösungsmenge stehen, kann man wie folgt bekommen. Ergänze die TNF mit zusätzlichen Zeilen der Form $(0, \ldots, 0, -1, 0, \ldots, 0)$, und zwar so, dass eine Matrix entsteht, die unterhalb der Diagonalen lauter Nullen hat, und auf deren Diagonalen nur $+1$ und -1 stehen. Die Lösungsmenge L besteht dann genau aus den Linearkombinationen aller Spalten, bei denen -1 auf der Diagonalen steht.

Im vorliegenden Beispiel ist in der TNF eine solche Zeile zwischen der dritten und der vierten sowie zwischen der vorletzten und der letzten Zeile einzufügen. Man erhält dann

$$\begin{array}{rl} & \begin{pmatrix} 1 & 0 & \boxed{3} & 0 & \boxed{6} & 0 \\ 0 & 1 & 2 & 0 & 5 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 4 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \\ \text{neu} \rightarrow & \\ \text{neu} \rightarrow & \\ & \qquad\qquad \downarrow b_1 \qquad \downarrow b_2 \end{array}$$

Algorithmus 3. Eingabe: $A \in \mathbb{K}^{n \times m}$ in TNF
Ausgabe: Eine Menge $\{b_1, \ldots, b_k\}$, so dass

$$L = \{ \alpha_1 b_1 + \cdots + \alpha_k b_k : \alpha_1, \ldots, \alpha_k \in \mathbb{K} \}$$

die Lösungsmenge des Gleichungssystems $Ax = 0$ ist.

1 für $r = 1, \ldots, m$:

2 wenn $A[r, r] = 0$, dann:

3 füge $-e_r = (0, \ldots, 0, -1, 0 \ldots, 0) \in \mathbb{K}^m$ als zusätzliche Zeile zwischen der $r$ten und der $(r-1)$ten ein.

4 $B = \emptyset$

5 für $c = 1, \ldots, m$:

6 wenn $A[c, c] = -1$, dann:

7 $$B = B \cup \{ \begin{pmatrix} A[1, c] \\ \vdots \\ A[n, c] \end{pmatrix} \}$$

8 gib B als Ergebnis zurück

Algorithmus 4. (Gauß-Algorithmus)
Eingabe: $A \in \mathbb{K}^{n \times m}$
Ausgabe: Eine Menge $\{b_1, \ldots, b_k\}$, so dass

$$L = \{\, \alpha_1 b_1 + \cdots + \alpha_k b_k : \alpha_1, \ldots, \alpha_k \in \mathbb{K} \,\}$$

die Lösungsmenge des Gleichungssystems $Ax = 0$ ist.

1 Berechne eine Treppenform B von A mit Algorithmus 1

2 Berechne eine Treppennormalform C von B mit Algorithmus 2

3 Berechne $\{b_1, \ldots, b_k\}$ aus C mit Algorithmus 3

4 gib $\{b_1, \ldots, b_k\}$ als Ergebnis zurück.

Beispiel. Es sei die Matrix

$$A = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 2 & 2 & 1 & 0 \\ 0 & 1 & 1 & 2 & 1 \\ 2 & 2 & 2 & 1 & 1 \end{pmatrix}$$

gegeben. Die Einträge seien als Elemente von $\mathbb{Z}_3$ zu verstehen, d.h. es gilt z.B. $2 \cdot 2 = 1$ und $1 + 2 = 0$. Gesucht ist der Kern von A.

Schritt 1: Berechnung einer Treppenform von A. Der Algorithmus arbeitet sich dazu von links nach rechts durch die Spalten der Matrix. In jedem Schritt ist nur die jeweils eingerahmte Teilmatrix relevant. Dieser eingerahmte Teil wird in jedem Schritt um eine Spalte kürzer.

$$\begin{pmatrix} \boxed{1} & 0 & 1 & 0 & 1 \\ \boxed{1} & 2 & 2 & 1 & 0 \\ \boxed{0} & 1 & 1 & 2 & 1 \\ \boxed{2} & 2 & 2 & 1 & 1 \end{pmatrix} \begin{matrix} \\ \leftarrow 2+ \\ \\ \leftarrow + \end{matrix} \longleftrightarrow \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & \boxed{2} & 1 & 1 & 2 \\ 0 & \boxed{1} & 1 & 2 & 1 \\ 0 & \boxed{2} & 0 & 1 & 2 \end{pmatrix} \mid \cdot 2$$

$$\longleftrightarrow \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & \boxed{1} & 2 & 2 & 1 \\ 0 & \boxed{1} & 1 & 2 & 1 \\ 0 & \boxed{2} & 0 & 1 & 2 \end{pmatrix} \begin{matrix} \\ \leftarrow 2+ \\ \\ \leftarrow + \end{matrix} \longleftrightarrow \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 2 & 2 & 1 \\ 0 & 0 & \boxed{2} & 0 & 0 \\ 0 & 0 & \boxed{2} & 0 & 0 \end{pmatrix} \mid \cdot 2$$

$$\longleftrightarrow \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 2 & 2 & 1 \\ 0 & 0 & \boxed{1} & 0 & 0 \\ 0 & 0 & \boxed{2} & 0 & 0 \end{pmatrix} \begin{matrix} \\ \\ \\ \leftarrow + \end{matrix} \longleftrightarrow \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 2 & 2 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \boxed{0} & 0 \end{pmatrix}$$

Schritt 2: Transformation der Treppenform in eine Treppennormalform. Hier geht man von rechts nach links durch die Matrix. Von links nach rechts vorzugehen würde auch zum richtigen Ergebnis führen, ist aber meist mit etwas mehr Rechenaufwand verbunden. Im vorliegenden Beispiel ist es egal, weil es nur eine Treppenstufe gibt (nämlich die in der dritten Zeile), über der Einträge stehen, die von Null verschieden sind. Dieser Rechenschritt könnte theoretisch die Einträge in der eingerahmten Teilmatrix ändern. Im vorliegenden Fall ändern sich nur

die Einträge oberhalb der dritten Treppenstufe, weil die Einträge rechts dieser Treppenstufe zufällig Null sind.

$$\begin{pmatrix} 1 & 0 & \boxed{1} & 0 & 1 \\ 0 & 1 & \boxed{2} & 2 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{matrix} \longleftarrow + \\ \longleftarrow + \\ \longleftarrow 2 \end{matrix} \quad \longleftrightarrow \quad \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Schritt 3: Bestimmung der Lösungsvektoren aus der Treppennormalform. Wir müssen die TNF durch hinzufügen geeigneter negativer Einheitsvektoren zu einer Matrix ergänzen, und zwar so, dass

- die Diagonale am Ende so viele Einträge hat wie die Matrix Spalten hat (also hier fünf),
- auf der Diagonalen keine Nullen mehr stehen,
- unterhalb der Diagonalen nur Nullen stehen.

Nullzeilen kann man, wenn man will, streichen. Im vorliegenden Beispiel erhält man also, da wir in $\mathbb{Z}_3$ rechnen und dort $-1 = 2$ gilt, die Matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 2 \end{pmatrix}.$$

Diese Matrix ist **nicht** äquivalent zur TNF, sondern nur eine Hilfsmatrix, die es erleichtert, die Lösungsvektoren abzulesen. Dieses sind nämlich genau jene Spalten, bei denen auf der Diagonale -1 steht. Die Lösungsmenge lautet also

$$\ker A = \{\alpha \begin{pmatrix} 0 \\ 2 \\ 0 \\ 2 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 2 \end{pmatrix} : \alpha, \beta \in \mathbb{Z}_3\}.$$

Satz 21. Die Menge $\{b_1, \ldots, b_k\}$, die von Algorithmus 4 berechnet wird, ist linear unabhängig.

Beweis. Wir dürfen annehmen, dass die b_i in der Reihenfolge indiziert sind, in der der Algorithmus sie findet.

Zu zeigen: für alle $\alpha_1, \ldots, \alpha_k \in \mathbb{K}$ gilt:

$$\alpha_1 b_1 + \cdots + \alpha_k b_k = \underset{\substack{\uparrow \\ \in \mathbb{K}^m}}{0} \quad \Rightarrow \quad \alpha_1 = \cdots = \alpha_k = \underset{\substack{\uparrow \\ \in \mathbb{K}}}{0}.$$

Seien also $\alpha_1, \ldots, \alpha_k \in \mathbb{K}$ so dass $\alpha_1 b_1 + \cdots + \alpha_k b_k = 0$. Angenommen, nicht alle α_i sind Null. Dann gibt es ein $i \in \{1, \ldots, k\}$, so dass $\alpha_i \neq 0$ und $\alpha_{i+1} = \cdots = \alpha_k = 0$. Wenn $j \in$

$\{1, \ldots, m\}$ der maximale Index ist, so dass die j-te Komponente von b_i von Null verschieden ist, dann ist diese Komponente -1 und die j-te Komponente der Vektoren $b_1, \ldots, b_{i-1}$ ist Null. Das folgt aus Zeile 3 von Algorithmus 3. Die j-te Komponente der Linearkombination $\alpha_1 b_1 + \cdots + \alpha_k b_k$ ist dann $\alpha_1 0 + \cdots + \alpha_{i-1} 0 - \alpha_i + 0(b_{i+1})_j + \cdots + 0(b_k)_j = -\alpha_i \neq 0$. Damit kann die Linearkombination nicht der Nullvektor sein. ∎

Später werden wir sagen, $\{b_1, \ldots, b_k\}$ ist eine „Basis“ des Lösungsraums, und $k = |\{b_1, \ldots, b_k\}|$ ist dessen „Dimension“.

Algorithmus 4 berechnet also nicht die komplette Lösungsmenge, sondern nur eine endliche Menge von Vektoren, durch die sich alle (evtl. unendlich vielen) Lösungen darstellen lassen. Wozu dann der ganze Aufwand? Die Matrix A selbst ist schließlich auch eine endliche Menge von Vektoren, durch die sich alle Lösungen darstellen lassen: $L = \{\, x \in \mathbb{K}^m : Ax = 0 \,\}$. Warum ist eine Basis besser?

In der Tat kann man nicht pauschal sagen, dass eine Darstellung besser ist als die andere. Es kommt darauf an, was man machen will. Wenn man z. B. einen Vektor $x \in \mathbb{K}^m$ gegeben hat und wissen will, ob er in L liegt, dann ist eine Basis zunächst nicht sehr hilfreich. Einfacher ist es, Ax auszurechnen und zu schauen, ob 0 rauskommt. Umgekehrt, wenn man einen konkreten Lösungsvektor sucht, dann ist A nicht sehr hilfreich, aber eine Basis schon (jedes Basiselement ist ja insbesondere eine Lösung; wähle $\alpha_i = 1$ und alle $\alpha_j = 0$ für $j \neq i$).

Man sagt, „$L = \{\, x \in \mathbb{K}^m : Ax = 0 \,\}$“ ist eine *implizite* Darstellung von L, und man nennt „$L = \{\alpha_1 b_1 + \cdots + \alpha_k b_k : \alpha_1, \ldots, \alpha_k \in \mathbb{K}\} = \{\, (b_1, \ldots, b_k)x : x \in \mathbb{K}^k \,\}$“ eine *explizite* Darstellung.

Algorithmus 4 ist also ein Algorithmus, der eine implizite Darstellung in eine explizite Darstellung umwandelt. Geht es auch umgekehrt? Klar!

Algorithmus 5. Eingabe: $\{b_1, \ldots, b_k\} \subseteq \mathbb{K}^m$
Ausgabe: Eine Matrix $A \in \mathbb{K}^{n \times m}$, so dass $\ker A = \{\, \alpha_1 b_1 + \cdots + \alpha_k b_k : \alpha_1, \ldots, \alpha_k \in \mathbb{K} \,\}$.

1 Sei $B = \begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix} \in \mathbb{K}^{k \times m}$.

2 Berechne $a_1, \ldots, a_n \in \mathbb{K}^m$, so dass

$$\{\, x \in \mathbb{K}^m : Bx = 0 \,\} = \{\, \alpha_1 a_1 + \cdots + \alpha_n a_n : \alpha_1, \ldots, \alpha_n \in \mathbb{K} \,\}.$$

3 gib $A = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in \mathbb{K}^{n \times m}$ als Ergebnis zurück.

Um die Korrektheit dieses Algorithmus zu zeigen, muss man beweisen

$$\begin{aligned} & \{\, x \in \mathbb{K}^m : Bx = 0 \,\} = \{\, \alpha_1 a_1 + \cdots + \alpha_n a_n : \alpha_1, \ldots, \alpha_n \in \mathbb{K} \,\} \\ \Rightarrow\quad & \{\, x \in \mathbb{K}^m : Ax = 0 \,\} = \{\, \alpha_1 b_1 + \cdots + \alpha_k b_k : \alpha_1, \ldots, \alpha_n \in \mathbb{K} \,\}. \end{aligned}$$

„$\supseteq$“ Nach Annahme gilt

$$\underbrace{\begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix}}_{\in \mathbb{K}^{k \times m}} \underbrace{(a_1, \ldots, a_n)}_{\in \mathbb{K}^{m \times n}} = 0 \in \mathbb{K}^{k \times n} \quad \Rightarrow \quad \underbrace{\left(\begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix} (a_1, \ldots, a_n) \right)^\top}_{= \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} (b_1, \ldots, b_k)} = 0 \in \mathbb{K}^{n \times k},$$

$$= A$$

also gilt $Ab_i = 0$ für alle i, und damit auch

$$\begin{aligned} &A \cdot (\alpha_1 b_1 + \cdots + \alpha_k b_k) \\ &= \alpha_1 A b_1 + \cdots + \alpha_k A b_k \\ &= \alpha_1 0 + \cdots + \alpha_k 0 = 0 \end{aligned}$$

für jede Wahl von $\alpha_1, \ldots, \alpha_k \in \mathbb{K}$.

„$\subseteq$“ Diese Richtung ist nicht ganz so offensichtlich. Wir werden in Abschnitt 16 darauf zurückkommen.

10 Lineare Unabhängigkeit und Rang

Satz 22. Seien $b_1, \ldots, b_m \in \mathbb{K}^n$ und sei $T := \begin{pmatrix} t_1 \\ \vdots \\ t_m \end{pmatrix} \in \mathbb{K}^{m \times n}$ eine Treppenform von $B := \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in \mathbb{K}^{m \times n}$. Dann gilt: $b_1, \ldots, b_m$ sind genau dann linear abhängig, wenn $t_m = (0, \ldots, 0)$ ist.

Beweis. „$\Leftarrow$“ $t_m = (0, \ldots, 0)$. Es gibt Elementarmatrizen $E_1, \ldots, E_k$, so dass

$$T = E_k \cdots E_1 B.$$

Wenn $U = E_k \cdots E_1$ ist und $(u_{m,1}, \ldots, u_{m,m})$ der m-te Zeilenvektor von U, dann gilt also $0 = t_m = u_{m,1} b_1 + \cdots + u_{m,m} b_m$.

Da die E_i invertierbare Matrizen sind, ist auch U eine invertierbare Matrix. Als solche kann U keine Nullzeile enthalten, denn es muss ja $U^{-1}U = I_m$ gelten, und wäre z.B. die m-te Zeile von U komplett Null, so wäre auch die m-te Zeile von I_m komplett Null, was nicht der Fall ist.

Es gilt also, dass $(u_{m,1}, \ldots, u_{m,m})$ nicht der Nullvektor ist, und also $b_1, \ldots, b_m$ linear abhängig sind.

„$\Rightarrow$“ $b_1, \ldots, b_m$ sind linear abhängig, etwa

$$\alpha_1 b_1 + \cdots + \alpha_m b_m = 0$$

für gewisse $\alpha_1, \ldots, \alpha_m \in \mathbb{K}$, von denen nicht alle Null sind.

Es gilt also

$$\begin{aligned} (\alpha_1, \ldots, \alpha_m) \underbrace{\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}} &= (0, \ldots, 0) \\ = U \begin{pmatrix} t_1 \\ \vdots \\ t_m \end{pmatrix} & \end{aligned}$$

für ein invertierbares $U \in \mathbb{K}^{m\times m}$. Mit $(\beta_1, \dots, \beta_m) := (\alpha_1, \dots, \alpha_m)U$ gilt deshalb

$$\beta_1 t_1 + \cdots + \beta_m t_m = (0, \dots, 0).$$

Da U invertierbar ist und nicht alle α_i Null sind, sind auch nicht alle β_i Null, denn wären alle β_i Null, dann wären wegen $(\alpha_1, \dots, \alpha_m) = (\beta_1, \dots, \beta_m)U^{-1}$ auch alle α_i Null.

Also sind $t_1, \dots, t_m$ linear abhängig.

Sei i minimal, so dass $\beta_i \neq 0$. Wir können dann o.B.d.A. annehmen, dass $\beta_i = -1$ ist. Dann gilt

$$t_i = \beta_{i+1} t_{i+1} + \cdots + \beta_m t_m. \qquad (*)$$

Wir zeigen, dass $t_i = 0$ ist. Wegen der Treppenform folgt dann $t_{i+1} = \cdots = t_m = 0$.

Wäre $t_i \neq 0$, dann wäre es wegen der Treppenform von der Form $(0, \dots, 0, \underset{\uparrow}{1}, *, \dots, *)$ mit der k

1 an einem bestimmten Index k, und $t_{i+1}, \dots, t_m$ wären von der Form $(0, \dots, 0, 0, \underset{\uparrow}{*}, \dots, *)$,
$k+1$

mit einer 0 am Index k. Für die k-te Komponente der Gleichung $(*)$ würde dann gelten

$$1 = \beta_{i+1} 0 + \cdots + \beta_m 0 = 0.$$

Widerspruch. ∎

Der Beweis zeigt übrigens auch, dass die Menge aller Zeilen einer Treppenform, die von 0 verschieden sind, stets linear unabhängig ist. Wenn also $b_1, \dots, b_m \in \mathbb{K}^n$ linear abhängig sind, dann übersetzen sich die Linearkombinationen $b_1, \dots, b_m$, die 0 ergeben, in Linearkombinationen von der Form

$$0t_1 + \cdots + 0t_k + \alpha_{k+1} 0 + \cdots + \alpha_m 0 = 0$$

für beliebige $\alpha_{k+1}, \dots, \alpha_m \in \mathbb{K}$.

Man kann also sagen, dass eine Treppenform den linear unabhängigen und den linear abhängigen Anteil von $b_1, \dots, b_m$ voneinander trennt. Es ist deshalb von Interesse, wie viele Nullzeilen eine Treppenfrom enthält.

Definition 25. Sei $A \in \mathbb{K}^{n\times m} \setminus \{0\}$. Sei $T = \begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix}$ eine Treppenform von A und $k \in \{1, \dots, n\}$ maximal mit $t_k \neq 0$. Dann heißt $\operatorname{Rang} A := k$ der *Rang* (engl. *rank*) von A.

Für die Nullmatrix definiert man $\operatorname{Rang} 0 := 0$.

Der vorherige Satz sagt also, dass die Zeilen von $A \in \mathbb{K}^{n\times m}$ genau dann linear abhängig sind, wenn $\operatorname{Rang} A < n$ ist.

Wenn T und T' zwei verschiedene Treppenformen von A sind, so müssen doch beide den gleichen Rang haben. Die Definition hängt also nicht von der Wahl der Treppenform ab und ist deshalb zulässig.

Allgemein gilt $\operatorname{Rang} A \leq n$. Übrigens gilt auch $\operatorname{Rang} A \leq m$. Es folgt also aus $m < n$ direkt, dass die Zeilen von A linear abhängig sind.

Beachte außerdem: Wenn E eine Elementarmatrix ist, dann gilt $\operatorname{Rang} A = \operatorname{Rang} EA$.

Beispiel.

1. Rang $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = 3$, da $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \leftrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ und diese TF drei Stufen hat.
2. Rang $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} = 2$, da $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \leftrightarrow \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}$ und diese TF zwei Stufen hat.
3. Rang $\begin{pmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 3 & 3 & 3 \end{pmatrix} = 1$, da $\begin{pmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 3 & 3 & 3 \end{pmatrix} \leftrightarrow \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ und diese TF eine Stufe hat.

Satz 23. Sei $A \in \mathbb{K}^{n \times m}$. Dann gilt:

1. Ist irgendeine Wahl von k Zeilen von A linear unabhängig, so ist $\operatorname{Rang} A \geq k$.
2. Ist jede Wahl von k Zeilen von A linear abhängig, so ist $\operatorname{Rang} A < k$.

Mit anderen Worten: $\operatorname{Rang} A = k$ genau dann, wenn k die maximale Anzahl von linear unabhängigen Zeilen von A ist.

Beweis. Seien $a_1, \ldots, a_n \in \mathbb{K}^m$ die Zeilenvektoren von A.

1. Wir zeigen: wenn $\operatorname{Rang} A < k$, dann sind $a_1, \ldots, a_k$ linear abhängig. Nehmen wir also an, es gilt $\operatorname{Rang} A < k$. Dann hat jede Treppenform von A die Form

$$T = \begin{pmatrix} t_1 \\ \vdots \\ t_{k-1} \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

   Es gibt eine invertierbare Matrix $U \in \mathbb{K}^{m \times m}$ mit $A = UT$. Damit lässt sich jedes a_i als Linearkombination von $t_1, \ldots, t_n$ darstellen, und damit auch als Linearkombination von $t_1, \ldots, t_{k-1}$, etwa

$$\begin{aligned} a_1 &= c_{1,1}t_1 + \cdots + c_{1,k-1}t_{k-1} + 0 + \cdots + 0 \\ a_2 &= c_{2,1}t_1 + \cdots + c_{2,k-1}t_{k-1} \\ &\vdots \\ a_k &= c_{k,1}t_1 + \cdots + c_{k,k-1}t_{k-1}. \end{aligned}$$

   Die Matrix

$$C = \begin{pmatrix} c_{1,1} & \cdots & c_{1,k-1} \\ \vdots & \ddots & \vdots \\ c_{k,1} & \cdots & c_{k,k-1} \end{pmatrix}$$

hat mehr Zeilen als Spalten, deshalb müssen wegen $\operatorname{Rang} C \leq k-1$ nach Satz 22 ihre Zeilen linear abhängig sein, etwa

$$\begin{aligned}&\alpha_1(c_{1,1},\ldots,c_{1,k-1})\\&+\alpha_2(c_{2,1},\ldots,c_{2,k-1})\\&+\cdots\\&+\alpha_k(c_{k,1},\ldots,c_{k,k-1})=0\end{aligned}$$

für gewisse $\alpha_1,\ldots,\alpha_k \in \mathbb{K}$, von denen nicht alle Null sind.

Dann gilt auch

$$\begin{aligned}0 &= \underbrace{\sum_{i=1}^{k} \alpha_i(c_{i,1},\ldots,c_{i,k-1})}_{=0} \begin{pmatrix} t_1 \\ \vdots \\ t_{k-1} \end{pmatrix} \\ &= \alpha_1 a_1 + \cdots + \alpha_k a_k,\end{aligned}$$

d. h. $\{a_1,\ldots,a_k\}$ ist linear abhängig.

2. Wir zeigen: wenn $\operatorname{Rang} A \geq k$ ist, dann gibt es eine Wahl von k Zeilen von A, die linear unabhängig sind. Sei $M = \{a_{i_1},\ldots,a_{i_\ell}\}$ eine Menge von Zeilen von A, die linear unabhängig ist und in dem Sinn maximal, dass $M \cup \{a\}$ linear abhängig ist für jede Zeile a von A, die nicht schon in M ist. Dann gilt

$$A \leftrightarrow \begin{pmatrix} a_{i_1} \\ \vdots \\ a_{i_\ell} \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \qquad (*)$$

denn für jede Zeile $a \in \{a_1,\ldots,a_n\} \setminus M$ gibt es nach Wahl von M eine lineare Abhängigkeit $\alpha_0 a + \alpha_{i_1} a_{i_1} + \cdots + \alpha_{i_\ell} a_{i_\ell} = 0$, und in dieser muss $\alpha_0 \neq 0$ sein, weil sonst schon $a_{i_1},\ldots,a_{i_\ell}$ linear abhängig wären. Wenn aber $\alpha_0 \neq 0$ ist, kann man O.B.d.A. annehmen, dass $\alpha_0 = -1$ ist, dass es also eine Darstellung $a = \alpha_{i_1} a_{i_1} + \cdots + \alpha_{i_\ell} a_{i_\ell}$ gibt. Daher lässt sich die Zeile a durch geeignete Zeilenoperationen mithilfe der Zeilen in M in eine Nullzeile überführen.

Aus der Form $(*)$ folgt $\operatorname{Rang} A \leq \ell$. Zusammen mit der Annahme $\operatorname{Rang} A \geq k$ folgt $\ell \geq k$. ∎

Satz 24. Für alle $A \in \mathbb{K}^{n\times m}$ gilt $\operatorname{Rang} A = \operatorname{Rang} A^\top$.

Beweis. Wegen $(A^\top)^\top = A$ genügt es zu zeigen, dass $\operatorname{Rang} A \geq \operatorname{Rang} A^\top$.

Ist $\operatorname{Rang} A = k$, so ist $A = UT$ für eine Matrix U, die das Produkt von Elementarmatrizen ist, und eine Treppenform T, bei der die ersten k Zeilen von 0 verschieden sind, und die letzten $n-k$ Zeilen Null sind. Dann ist $A^\top = T^\top U^\top$. Die Matrix $T^\top$ hat die Form

$$\underbrace{\begin{pmatrix} * & \cdots & * & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ * & \cdots & * & 0 & \cdots & 0 \end{pmatrix}}_{k \qquad\qquad n-k}.$$

Für die Treppenformen dieser Matrix sind nur die ersten k Spalten relevant. Der Rang der Matrix $T^\top$ ist daher höchstens k.

Nach Satz 23 sind deshalb je $k+1$ Zeilen von $T^\top$ linear abhängig. Sei $\tilde{T} \in \mathbb{K}^{n\times(k+1)}$ eine beliebige Wahl von $k+1$ Spalten von T, so dass $\tilde{T}^\top \in \mathbb{K}^{(k+1)\times n}$ eine beliebige Wahl von $k+1$ Zeilen von $T^\top$ ist. Dann gibt es also $(\alpha_1, \ldots, \alpha_{k+1}) \neq 0$ mit

$$(\alpha_1, \ldots, \alpha_{k+1})\tilde{T}^\top = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \in \mathbb{K}^n.$$

Und dann gilt auch

$$(\alpha_1, \ldots, \alpha_{k+1})\tilde{T}^\top U^\top = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Damit ist gezeigt, dass jede Wahl von $k+1$ Zeilen von $A^\top = T^\top U^\top$ linear abhängig ist. Nach Satz 23 folgt $\operatorname{Rang} A^\top < k+1$, d. h. $\operatorname{Rang} A^\top \leq k$, wie behauptet. ∎

Wegen Satz 24 gilt Satz 23 auch für die Spalten von A. Für die Berechnung des Rangs einer Matrix bedeutet das, dass man sowohl Zeilen- als auch Spaltenoperationen anwenden darf, um A in eine Form zu bringen, aus der man den Rang ablesen kann. Spaltenoperationen sind ja Zeilenoperationen auf der Transponierten, und solche Operationen ändern den Rang nicht.

Durch Zeilen- und Spaltenoperationen lässt sich jede Matrix $A \in \mathbb{K}^{n\times m}$ mit $\operatorname{Rang} A = k$ auf die Form

$$\underbrace{\begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}}_{k \qquad\qquad m-k} \left.\begin{matrix} \\ \\ \\ \\ \\ \\ \end{matrix}\right\} \begin{matrix} k \\ \\ \\ \\ n-k \\ \\ \end{matrix}$$

bringen.

Beispiel.

$$\overset{\overset{-2}{\frown}\ \overset{+}{\downarrow}}{\begin{pmatrix}1&2&0\\0&3&1\\2&1&3\end{pmatrix}} \rightsquigarrow \begin{pmatrix}1&0&0\\0&3&1\\2&-3&3\end{pmatrix} \overset{-2}{\underset{+}{\leftarrow}} \rightsquigarrow \begin{pmatrix}1&0&0\\0&3&-1\\0&-3&3\end{pmatrix} \overset{}{\underset{+}{\leftarrow}}$$

$$\overset{:3}{\rightsquigarrow} \begin{pmatrix}1&0&0\\0&3&-1\\0&0&2\end{pmatrix} \rightsquigarrow \begin{pmatrix}1&0&0\\0&1&-1\\0&0&2\end{pmatrix} \mid :2 \rightsquigarrow \overset{\overset{+}{\frown}\ \overset{}{\downarrow}}{\begin{pmatrix}1&0&0\\0&1&-1\\0&0&1\end{pmatrix}}$$

$$\rightsquigarrow \begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix} .$$

Also ist Rang $\begin{pmatrix}1&2&0\\0&3&1\\2&1&3\end{pmatrix} = 3$.

Man braucht sich aber gar nicht die Mühe zu machen, eine Matrix bis zu dieser Form zu bringen. Es genügt schon, durch Zeilen- und Spaltenoperationen alle Einträge unterhalb der Diagonale zu Null zu machen. Danach ist der Rang genau die Anzahl der Elemente auf der Diagonale, die von Null verschieden sind. Im vorliegenden Beispiel hätte man also schon bei der ersten Matrix in der zweiten Zeile aufhören können.

11 Inhomogene Systeme

Gegeben seien $A \in \mathbb{K}^{n\times m}$, $b \in \mathbb{K}^n$, und gesucht seien alle $x \in \mathbb{K}^m$ mit $Ax = b$.
Mit $A = ((a_{i,j}))_{i=1,j=1}^{n,m}$, $b = (b_1, \ldots, b_n)$ und $x = (x_1, \ldots, x_m)$ ist also folgendes System von Gleichungen zu lösen:

$$\begin{aligned} a_{1,1}x_1 + \cdots + a_{1,m}x_m &= b_1 \\ &\vdots \\ a_{n,1}x_1 + \cdots + a_{n,m}x_m &= b_n. \end{aligned}$$

Der Fall $b = (0, \ldots, 0)$ wurde schon in Abschnitt 9 behandelt. In diesem Fall spricht man von einem *homogenen* Gleichungssystem. Den Fall $b \neq 0$ bezeichnet man als *inhomogenes* Gleichungssystem. (engl. *homogeneous*/*inhomogeneous*)

Wie sieht die Lösungsmenge eines inhomogenen Gleichungssystems aus, und wie bestimmt man sie?

Beachte:

- x ist genau dann eine Lösung von $Ax = b$ wenn für jedes x_h mit $Ax_h = 0$ auch $x + x_h$ eine Lösung ist.

  Es genügt also, eine einzige Lösung x des Gleichungssystems $Ax = b$ zu finden. Alle weiteren unterscheiden sich von dieser dann nur noch um Lösungen des homogenen Systems $Ax = 0$.

- $x = (x_1, \dots, x_n) \in \mathbb{K}^m$ ist genau dann eine Lösung von $Ax = b$, wenn $\tilde{x} = (x_1, \dots, x_n, -1) \in \mathbb{K}^{m+1}$ eine Lösung von $(A|b)\tilde{x} = 0$ ist.

  Dabei ist $(A|b) \in \mathbb{K}^{n\times(m+1)}$ die Matrix, die aus A entsteht, wenn man b als zusätzliche Spalte rechts anfügt.

Idee: Berechne zunächst die Lösungsmenge des homogenen Systems $(A|b)\tilde{x} = 0$ und bestimme dann die Vektoren der Lösungsmenge, für die die $(m+1)$-te Koordinate -1 ist.

Betrachten wir dazu eine Treppenform $T = \begin{pmatrix} t_1 \\ \vdots \\ t_n \end{pmatrix} \in \mathbb{K}^{n\times(m+1)}$ von $(A|b)$. Es gibt zwei Fälle zu unterscheiden:

1. Die letzte von 0 verschiedene Zeile hat mehr als einen Eintrag:

$$T = \begin{pmatrix} * & \cdots & \cdots & \cdots & \cdots & * \\ \vdots & & & & & \vdots \\ * & \cdots & \cdots & \cdots & \cdots & * \\ & & 1 & * & \cdots & * \\ & & & & & \end{pmatrix}.$$

   In diesem Fall können wir die $(m+1)$te Koordinate des Lösungsvektors (des homogenen Systems) frei wählen. Insbesondere ist -1 eine mögliche Wahl. Die weiteren Koordinaten $x_1, \dots, x_m$ ergeben sich dann wie üblich. Im allgemeinen werden manche von ihnen durch Gleichungen bestimmt sein und andere frei wählbar.

2. Die letzte von 0 verschiedene Zeile hat genau einen Eintrag:

$$T = \begin{pmatrix} * & \cdots & \cdots & \cdots & \cdots & * \\ \vdots & & & & & \vdots \\ * & \cdots & \cdots & \cdots & \cdots & * \\ & & & & & 1 \\ & & & & & \end{pmatrix}.$$

   In diesem Fall entspricht die letzte Zeile der Treppenform der Gleichung $1 \cdot x_{m+1} = 0$, d. h. alle Lösungen $(x_1, \dots, x_{m+1})$ des homogenen Systems haben 0 als letzte Koordinate. Insbesondere gibt es keine Lösung mit -1 als letzter Koordinate. Das inhomogene System hat in diesem Fall also *keine Lösung.*

Beispiel.

1. $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$, $b = \begin{pmatrix} 5 \\ 6 \end{pmatrix}$

$$\left(\begin{array}{cc|c} 1 & 2 & 5 \\ 3 & 4 & 6 \end{array}\right) \begin{array}{l} \rceil^{-3} \\ \leftarrow\rfloor_{+} \end{array} \leftrightarrow \left(\begin{array}{cc|c} 1 & 2 & 5 \\ 0 & -2 & -9 \end{array}\right) \quad | :(-2)$$

$$\leftrightarrow \left(\begin{array}{cc|c} 1 & 2 & 5 \\ 0 & 1 & 9/2 \end{array}\right) \begin{array}{l} \leftarrow\rceil^{+} \\ \rfloor_{-2} \end{array}$$

$$\leftrightarrow \left(\begin{array}{cc|c} 1 & 0 & -4 \\ 0 & 1 & 9/2 \end{array}\right)$$

   Die Lösungsmenge lautet $L = \{\begin{pmatrix} -4 \\ 9/2 \end{pmatrix}\}$.

2. $A = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$, $b = \begin{pmatrix} 3 \\ 1 \end{pmatrix}$

$$\left(\begin{array}{cc|c} 1 & 2 & 3 \\ 2 & 4 & 1 \end{array}\right) \begin{array}{l} \\ \leftarrow + \end{array} \begin{array}{l} \\ -2 \end{array} \leftrightarrow \left(\begin{array}{cc|c} 1 & 2 & 3 \\ 0 & 0 & -5 \end{array}\right)$$

Die Lösungsmenge lautet $L = \emptyset$.

3. $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$, $b = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$.

$$\left(\begin{array}{ccc|c} 1 & 2 & 3 & 1 \\ 4 & 5 & 6 & 2 \\ 7 & 8 & 9 & 3 \end{array}\right) \begin{array}{l} \\ \leftarrow + \\ \leftarrow + \end{array} \begin{array}{l} \\ -4 \\ -7 \end{array} \leftrightarrow \left(\begin{array}{ccc|c} 1 & 2 & 3 & 1 \\ 0 & -3 & -6 & -2 \\ 0 & -6 & -12 & -4 \end{array}\right) \begin{array}{l} \\ \leftarrow + \\ \end{array} \begin{array}{l} \\ -2 \\ \end{array} \mid :(-3)$$

$$\leftrightarrow \left(\begin{array}{ccc|c} 1 & 2 & 3 & 1 \\ 0 & 1 & 2 & 2/3 \\ 0 & 0 & 0 & 0 \end{array}\right) \begin{array}{l} \leftarrow + \\ \\ \end{array} \begin{array}{l} \\ -2 \\ \end{array}$$

$$\leftrightarrow \left(\begin{array}{ccc|c} 1 & 0 & -1 & -1/3 \\ 0 & 1 & 2 & 2/3 \\ 0 & 0 & 0 & 0 \end{array}\right)$$

Die Lösungsmenge lautet

$$L = \left\{ \begin{pmatrix} -1/3 \\ 2/3 \\ 0 \end{pmatrix} + \alpha \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix} : \alpha \in \mathbb{R} \right\}.$$

Beachte: das homogene Gleichungssystem $Ax = 0$ hat die Lösungsmenge

$$L_h = \left\{ \alpha \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix} : \alpha \in \mathbb{R} \right\}.$$

Die Ergebnisse der vorangegangenen Diskussion lassen sich wie folgt als Satz zusammenfassen:

Satz 25. Sei $A \in \mathbb{K}^{n \times m}$, $b \in \mathbb{K}^n$ und sei $L = \{ x \in \mathbb{K}^m : Ax = b \}$. Dann gilt: $L = \emptyset$ oder es gibt ein $x_0 \in \mathbb{K}^m$ so dass

$$L = \{ x_0 + x_h : x_h \in \ker A \} \subseteq \mathbb{K}^m.$$

(Zur Erinnerung: $\ker A = \{ x \in \mathbb{K}^m : Ax = 0 \}$.)
Insbesondere gilt: wenn $\ker A = \{0\}$ und $n = m$, dann ist $|L| = 1$. Wenn $\ker A \neq \{0\}$, dann ist $|L| = 0$ oder $|L| > 1$. Im Fall $|L| > 1$ hat L mindestens so viele Elemente wie der Körper $\mathbb{K}$.

Bei der Berechnung der Lösungsmenge entfällt der größte Teil der Rechenarbeit auf A und nur ein vergleichsweise kleiner Teil auf b. Wenn man also mehrere inhomogene Gleichungssysteme mit dem selben A zu lösen hat, sollte man die Rechenschritte, die A betreffen, nicht mehrmals durchführen. Stattdessen bietet es sich an, alle Systeme gleichzeitig zu lösen.

Beispiel. $A = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & -1 \\ 1 & -1 & 0 \end{pmatrix}$, $b_1 = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$, $b_2 = \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix}$.

$$
\begin{aligned}
(A \mid b_1\, b_2) &= \left(\begin{array}{ccc|cc} 1 & 0 & 2 & 1 & 3 \\ 0 & 1 & -1 & 2 & 2 \\ 1 & -1 & 0 & 3 & 1 \end{array}\right) \begin{array}{l} \\ \\ \leftarrow + \end{array} \begin{array}{l} \\ \\ -1 \end{array} \\
&\leftrightarrow \left(\begin{array}{ccc|cc} 1 & 0 & 2 & 1 & 3 \\ 0 & 1 & -1 & 2 & 2 \\ 0 & -1 & -2 & 2 & -2 \end{array}\right) \begin{array}{l} \\ \\ \leftarrow + \end{array} \\
&\leftrightarrow \left(\begin{array}{ccc|cc} 1 & 0 & 2 & 1 & 3 \\ 0 & 1 & -1 & 2 & 2 \\ 0 & 0 & -3 & 4 & 0 \end{array}\right) \begin{array}{l} \\ \leftarrow + \\ \mid : (-3) \end{array} \begin{array}{l} + \\ + \\ -2 \end{array} \\
&\leftrightarrow \left(\begin{array}{ccc|cc} 1 & 0 & 0 & 11/3 & 3 \\ 0 & 1 & 0 & 2/3 & 2 \\ 0 & 0 & 1 & -4/3 & 0 \end{array}\right)
\end{aligned}
$$

Daraus folgt: Die Lösungsmenge von $Ax = b_1$ ist $\{\begin{pmatrix} 11/3 \\ 2/3 \\ -4/3 \end{pmatrix}\}$ und die Lösungsmenge von $Ax = b_2$ ist $\{\begin{pmatrix} 3 \\ 2 \\ 0 \end{pmatrix}\}$.

Und was, wenn uns jetzt noch jemand nach der Lösung x von $Ax = 3b_1 - 7b_2$ fragt? Antwort: Wir können entweder noch einmal von vorne losrechnen. Oder wir kombinieren die Lösung einfach aus den schon bekannten Lösungen. Tatsächlich lautet die Lösung

$$x = 3\begin{pmatrix} 11/3 \\ 2/3 \\ -4/3 \end{pmatrix} - 7\begin{pmatrix} 3 \\ 2 \\ 0 \end{pmatrix} \quad [= \begin{pmatrix} -20 \\ -12 \\ -4 \end{pmatrix}].$$

Begründung: Wenn $Ax_1 = b_1$ und $Ax_2 = b_2$, dann ist $A(\alpha_1 x_1 + \alpha_2 x_2) = \alpha_1 A x_1 + \alpha_2 A x_2 = \alpha_1 b_1 + \alpha_2 b_2$ für alle $\alpha_1, \alpha_2 \in \mathbb{K}$.

Das gleichzeitige Lösen mehrerer inhomogener Gleichungssysteme lässt sich auch auffassen als das Lösen von Matrixgleichungen. Gegeben: $A \in \mathbb{K}^{n\times m}$, $B \in \mathbb{K}^{n\times k}$, gesucht: alle $X \in \mathbb{K}^{m\times k}$ mit $AX = B$. Um so eine Gleichung zu lösen, bringt man einfach die erweiterte Matrix $(A|B) \in \mathbb{K}^{n\times(m+k)}$ in Treppen(normal)form und liest daraus die Lösungsmenge $L \subseteq \mathbb{K}^{m\times k}$ ab.

Der wichtigste Spezialfall ist, wenn $A = \mathbb{K}^{n\times n}$ und $B = I_n \in \mathbb{K}^{n\times n}$. Die Gleichung $AX = I_n$ ist genau dann lösbar, wenn A eine invertierbare Matrix ist. Die Lösung ist dann $X = A^{-1}$.

Beispiel.

1. $A = \begin{pmatrix} 1 & 0 & 3 \\ 3 & 1 & 0 \\ 0 & 1 & 2 \end{pmatrix}$

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 3 & 1 & 0 & 0 \\ 3 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 2 & 0 & 0 & 1 \end{array}\right) \begin{array}{l} \urcorner^{-3} \\ \hookleftarrow^{+} \\ \end{array} \leftrightarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 3 & 1 & 0 & 0 \\ 0 & 1 & -9 & -3 & 1 & 0 \\ 0 & 1 & 2 & 0 & 0 & 1 \end{array}\right) \begin{array}{l} \\ \urcorner^{-1} \\ \hookleftarrow^{+} \end{array}$$

$$\leftrightarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 3 & 1 & 0 & 0 \\ 0 & 1 & -9 & -3 & 1 & 0 \\ 0 & 0 & 11 & 3 & -1 & 1 \end{array}\right) \begin{array}{l} \longleftarrow^{+} \\ \longleftarrow^{+} \\ \mid :11 \ \lrcorner_{9} \ \lrcorner_{-3} \end{array}$$

$$\leftrightarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 2/11 & 3/11 & -3/11 \\ 0 & 1 & 0 & -6/11 & 2/11 & 9/11 \\ 0 & 0 & 1 & 3/11 & -1/11 & 1/11 \end{array}\right)$$

Also ist $A^{-1} = \frac{1}{11} \begin{pmatrix} 2 & 3 & -3 \\ -6 & 2 & 9 \\ 3 & -1 & 1 \end{pmatrix}$.

2. $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 4 & 5 & 6 & 0 & 1 & 0 \\ 7 & 8 & 9 & 0 & 0 & 1 \end{array}\right) \begin{array}{l} \urcorner^{-4} \ \urcorner^{-7} \\ \hookleftarrow^{+} \\ \longleftarrow^{+} \end{array} \leftrightarrow \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -3 & -6 & -4 & 1 & 0 \\ 0 & -6 & -12 & -7 & 0 & 1 \end{array}\right) \begin{array}{l} \\ \urcorner^{-2} \\ \hookleftarrow^{+} \end{array}$$

$$\leftrightarrow \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -3 & -6 & -4 & 1 & 0 \\ 0 & 0 & 0 & 1 & -2 & 1 \end{array}\right).$$

Daraus folgt, dass A nicht invertierbar ist.

Satz 26. Sei $A \in \mathbb{K}^{n \times n}$. Dann sind folgende Aussagen äquivalent:

1. A ist invertierbar
2. $\ker A = \{0\}$
3. $\operatorname{Rang} A = n$
4. Die Zeilen von A sind linear unabhängig
5. Die Spalten von A sind linear unabhängig
6. A lässt sich als endliches Produkt von Elementarmatrizen schreiben

Beweis. Die Äquivalenzen (3)⇔(4)⇔(5) folgen aus den Sätzen 23 und 24.

(1)⇒(2). Sei $x \in \mathbb{K}^n$ so, dass $Ax = 0$ ist. Dann ist $x = A^{-1}Ax = A^{-1}0 = 0$.

(2)⇒(5). Wären die Spalten von $A = (a_1, \ldots, a_n) \in \mathbb{K}^{n\times n}$ linear abhängig, dann gäbe es ein $(\alpha_1, \ldots, \alpha_n) \in \mathbb{K}^n \setminus \{0\}$ mit

$$\alpha_1 a_1 + \cdots + \alpha_n a_n = 0,$$

also $A \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = 0$, also $(\alpha_1, \ldots, \alpha_n) \in \ker A$, also $\ker A \neq \{0\}$.

(3)⇒(6). Wenn $\operatorname{Rang} A = n$ ist, ist die TNF von A die Einheitsmatrix I_n. Es gibt also Elementarmatrizen $E_1, \ldots, E_m \in \mathbb{K}^{n\times n}$ mit $I_n = E_m \cdots E_1 A$. Da jede Elementarmatrix invertierbar ist und ihr Inverses wieder eine Elementarmatrix ist, ist $A = E_1^{-1} \cdots E_m^{-1}$ die gewünschte Darstellung.

(6)⇒(1). Jede Elementarmatrix ist invertierbar und das Produkt invertierbarer Matrizen ist invertierbar. ∎

Das Verfahren zum Invertieren von Matrizen kann man allgemein auch dazu verwenden, zu gegebenem $A \in \mathbb{K}^{n\times m}$ eine invertierbare Matrix $U \in \mathbb{K}^{n\times n}$ zu finden, so dass UA in Treppen(normal)form ist: die Treppen(normal)form von $(A|I_n)$ ist $(T|U)$, wobei T die Treppen(normal)form von A ist und U die gesuchte Transformationsmatrix.

Beispiel.

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 4 & 5 & 6 & 0 & 1 & 0 \\ 7 & 8 & 9 & 0 & 0 & 1 \end{array}\right) \leftrightarrow \cdots \leftrightarrow \left(\begin{array}{ccc|ccc} 1 & 0 & -1 & -5/3 & 2/3 & 0 \\ 0 & 1 & 2 & 4/3 & -1/3 & 0 \\ 0 & 0 & 0 & 1 & -2 & 1 \end{array}\right).$$

Für $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$ ist also $U = \frac{1}{3}\begin{pmatrix} -5 & 2 & 0 \\ 4 & -1 & 0 \\ 3 & -6 & 3 \end{pmatrix}$ eine Matrix, so dass

$$UA = \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}$$

die Treppennormalform von A ist.

Noch allgemeiner: Wenn wir sowohl Zeilen- als auch Spaltenoperationen anwenden wollen, zum Beispiel um den Rang einer Matrix A zu bestimmen, dann können wir Matrizen $U \in \mathbb{K}^{n\times n}$ und $V \in \mathbb{K}^{m\times m}$ finden, so dass

$$UAV = D := \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}.$$

Dazu betrachtet man die Matrix $\begin{pmatrix} A & I_n \\ I_m & 0 \end{pmatrix}$ und wendet darauf nur Zeilen- und Spaltenoperationen an, die die oberen n Zeilen oder die linken m Spalten betreffen. Das Ergebnis ist eine Matrix $\begin{pmatrix} D & U \\ V & 0 \end{pmatrix}$.

Beispiel. $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$

$$\left(\begin{array}{ccc|cc} 1 & 2 & 3 & 1 & 0 \\ 4 & 5 & 6 & 0 & 1 \\ \hline 1 & 0 & 0 & & \\ 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \end{array}\right) \begin{array}{l} \urcorner -4 \\ \leftarrow + \end{array} \quad \rightsquigarrow \quad \begin{array}{c} \text{Spalte 1} \cdot (-2) \to \text{Spalte 2} \; (+), \quad \text{Spalte 1} \cdot (-3) \to \text{Spalte 3} \; (+) \\ \left(\begin{array}{ccc|cc} 1 & 2 & 3 & 1 & 0 \\ 0 & -3 & -6 & -4 & 1 \\ \hline 1 & 0 & 0 & & \\ 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \end{array}\right) \end{array}$$

$$\rightsquigarrow \left(\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 0 \\ 0 & -3 & -6 & -4 & 1 \\ \hline 1 & -2 & -3 & & \\ 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \end{array}\right) \begin{array}{l} \\ \mid :(-3) \\ \\ \\ \\ \end{array}$$

$$\rightsquigarrow \begin{array}{c} \text{Spalte 2} \cdot (-2) \to \text{Spalte 3} \; (+) \\ \left(\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 2 & 4/3 & -1/3 \\ \hline 1 & -2 & -3 & & \\ 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \end{array}\right) \end{array}$$

$$\rightsquigarrow \left(\begin{array}{ccc|cc} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 4/3 & -1/3 \\ \hline 1 & -2 & 1 & & \\ 0 & 1 & -2 & & \\ 0 & 0 & 1 & & \end{array}\right).$$

In der Tat gilt

$$\begin{pmatrix} 1 & 0 \\ 4/3 & -1/3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \begin{pmatrix} 1 & -2 & 1 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

12 Determinanten

In diesem Abschnitt sind alle Matrizen quadratisch, d. h. wir betrachten hier nur Matrizen, die gleich viele Zeilen wie Spalten haben.

Das Ziel ist, eine Funktion $\det\colon \mathbb{K}^{n\times n} \to \mathbb{K}$ zu konstruieren, so dass der Wert $\det(A) \in \mathbb{K}$ etwas darüber aussagt, ob $A \in \mathbb{K}^{n\times n}$ einen nichtleeren Kern hat.

Dazu ist etwas Vorbereitung nötig. Man erinnere sich, dass S_n die Gruppe der bijektiven Funktionen $\{1,\dots,n\} \to \{1,\dots,n\}$ ist, und dass ihre Elemente auch als Permutationen bezeichnet werden.

Definition 26.

1. Eine Permutation $\pi \in S_n$ heißt *Zyklus* (engl. *cycle*), falls es paarweise verschiedene $k_1,\dots,k_m \in \{1,\dots,n\}$ gibt, so dass

$$\pi(k_1) = k_2, \quad \pi(k_2) = k_3, \quad \dots, \quad \pi(k_{m-1}) = k_m, \quad \pi(k_m) = k_1$$

   sowie $\pi(k) = k$ für alle $k \in \{1,\dots,n\} \setminus \{k_1,\dots,k_m\}$ gilt.

   Schreibweise: $\pi = (k_1\ k_2\ \dots\ k_m)$.

   Man nennt m die *Länge* des Zyklus.

2. Zwei Permutationen π_1, π_2 heißen (zueinander) *disjunkt,* falls gilt

$$\forall\ k \in \{1,\dots,n\} : \pi_1(k) = k \vee \pi_2(k) = k.$$

3. Ein Zyklus der Länge zwei heißt *Transposition.*

4. Ein $k \in \{1,\dots,n\}$ mit $\pi(k) = k$ heißt *Fixpunkt* von $\pi \in S_n$.

Beispiel.

1. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} = (1\ 2\ 4\ 3) = (3\ 1\ 2\ 4)$ ist ein Zyklus. Beachte: Ein Zyklus lässt sich auf verschiedene Weise schreiben.

2. $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ 3)$ ist eine Transposition.

3. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ ist kein Zyklus, lässt sich aber als Produkt (Komposition) der beiden disjunkten Zyklen (1 3) und (2 4) schreiben.

Satz 27.

1. Sind $\pi_1, \pi_2 \in S_n$ disjunkt, so gilt $\pi_1\pi_2 = \pi_2\pi_1$. (Zur Erinnerung: Im allgemeinen ist die Verknüpfung von Permutationen nicht kommutativ.)

2. Jedes $\pi \in S_n$ lässt sich als endliches Produkt von disjunkten und von id verschiedenen Zyklen schreiben. Diese Darstellung ist bis auf die Reihenfolge der Faktoren eindeutig.

3. Sind $k_1, \ldots, k_m \in \{1, \ldots, m\}$ paarweise verschieden, so gilt

$$(k_1\ k_2\ \ldots\ k_m) = (k_1\ k_2)(k_2\ k_3)\cdots(k_{m-1}\ k_m),$$
$$(k_1\ k_2\ \ldots\ k_m)^{-1} = (k_m\ k_{m-1}\ \ldots\ k_1).$$

4. Sind $\tau_1, \ldots, \tau_m \in S_n$ Transpositionen mit $\tau_1 \cdots \tau_m = \mathrm{id}$, so ist m gerade.

5. $|S_n| = n! := 1 \cdot 2 \cdots (n-1) \cdot n$.

Beweis.

1. Sei $k \in \{1, \ldots, n\}$ beliebig. Falls $\pi_1(k) = \pi_2(k) = k$ ist, gilt $(\pi_1\pi_2)(k) = (\pi_2\pi_1)(k) = k$.

   Wenn $\pi_1(k) \neq k$ ist, dann ist $\pi_2(k) = k$, weil π_1, π_2 disjunkt sind. Da π_1 bijektiv ist, gilt dann auch $\pi_1(\pi_2(k)) = \pi_1(k)$.

   Aus $\pi_1(k) \neq k$ und der Bijektivität von π_1 folgt auch, dass $\pi_1(\pi_1(k)) \neq \pi_1(k)$. Aus der Disjunktheit von π_1, π_2 folgt deshalb $\pi_2(\pi_1(k)) = \pi_1(k)$.

   Damit ist gezeigt $\pi_1(\pi_2(k)) = \pi_2(\pi_1(k))$.

   Der Fall $\pi_2(k) \neq k$ geht genauso. Insgesamt ist also gezeigt, dass für alle $k \in \{1, \ldots, n\}$ gilt $(\pi_1\pi_2)(k) = (\pi_2\pi_1)(k)$, wie behauptet.

2. Die *Existenz* folgt aus folgendem konstruktiven Argument.

   1 Setze $B := \{1, \ldots, n\}$.
   2 Solange $B \neq \emptyset$
   3 Wähle ein beliebiges $k \in B$.
   4 Falls $\pi(k) = k$, dann
   5 Setze $B := B \setminus \{k\}$
   6 ansonsten
   7 Bestimme $m \in \{1, \ldots, n\}$ mit $\pi^m(k) = k$ und $\pi^i(k) \neq k$ für $i = 1, \ldots, m-1$. So ein m existiert.
   8 Notiere den Zyklus $(k\ \pi(k)\ \ldots\ \pi^{m-1}(k))$.
   9 Setze $B := B \setminus \{k, \ldots, \pi^{m-1}(k)\}$.

   Da in jeder Iteration die Menge B um wenigstens ein Element kleiner wird, wird dieses Verfahren nach endlich vielen Schritten fertig. Offensichtlich ist π das Produkt aller notierten Zyklen und diese sind $\neq \mathrm{id}$ und paarweise zueinander disjunkt.

Eindeutigkeit: Hätte $\pi \in S_n$ zwei verschiedene Darstellungen als Produkt disjunkter Zyklen, etwa

$$\pi = \sigma_1 \cdots \sigma_m = \tilde{\sigma}_1 \cdots \tilde{\sigma}_{\tilde{m}},$$

dann müsste $\sigma_i \notin \{\tilde{\sigma}_1, \ldots, \tilde{\sigma}_{\tilde{m}}\}$ für mindestens ein $i \in \{1, \ldots, m\}$ gelten. (O.B.d.A. können wir annehmen $m \geq \tilde{m}$.) Wähle so ein σ_i.

Da $\sigma_i \neq \mathrm{id}$ ist, gibt es ein $k \in \{1, \ldots, n\}$ mit $\sigma_i(k) \neq k$. Wegen Disjunktheit ist dann auch $\pi(k) = \sigma_i(k) \neq k$. Damit muss es ein $\tilde{\imath} \in \{1, \ldots, \tilde{m}\}$ geben mit $\pi(k) = \tilde{\sigma}_{\tilde{\imath}}(k) \neq k$. Induktiv zeigt man $\forall\ \ell \in \mathbb{N} : \pi^\ell(k) = \sigma_i^\ell(k) = \tilde{\sigma}_{\tilde{\imath}}^\ell(k)$. Aber dann ist $\sigma_i = \tilde{\sigma}_{\tilde{\imath}}$, im Widerspruch zur Wahl von σ_i.

3. Übung.

4. Betrachte die Funktion

$$F\colon S_n \to \mathbb{N}, \quad \pi \mapsto |\{\, (i,j) \in \{1, \ldots, n\}^2 : i < j \wedge \pi(i) > \pi(j) \,\}|.$$

(Beispiel: $F(\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix}) = |\{(1,3),(2,3),(2,5),(4,5)\}| = 4.$)

Sei $\pi \in S_n$ beliebig und $\tau = (i\ j)$ mit $i < j$ eine Transposition.

1. Fall: $\pi(i) > \pi(j)$. Dann gilt $(\pi\tau)(i) < (\pi\tau)(j)$ und $(\pi\tau)(k) = \pi(k)$ für alle $k \in \{1, \ldots, n\} \setminus \{i, j\}$. Es gilt also $F(\pi\tau) = F(\pi) - 1$.
2. Fall: $\pi(i) < \pi(j)$. Dann ist $(\pi\tau)(i) > (\pi\tau)(j)$ und $(\pi\tau)(k) = \pi(k)$ für alle $k \in \{1, \ldots, n\} \setminus \{i, j\}$. Es gilt also $F(\pi\tau) = F(\pi) + 1$.
3. Fall: $\pi(i) = \pi(j)$. Dieser Fall kann nicht auftreten, weil $i < j$, also $i \neq j$ und π bijektiv, also injektiv.

Damit ist gezeigt, dass für jede Permutation $\pi \in S_n$, die ein Produkt einer ungeraden Anzahl von Transpositionen ist, auch $F(\pi)$ ungerade ist. Da $F(\mathrm{id}) = 0$ gerade ist, folgt die Behauptung.

5. Induktion nach n. Für $n = 1$ gilt $S_1 = \{\mathrm{id}\}$, also $|S_1| = 1$. Sei nun $n \in \mathbb{N}$ so, dass $|S_n| = n!$ gilt. Wir zeigen $|S_{n+1}| = (n+1)!$.

Zunächst ist klar, dass die Permutationen von $\{1, \ldots, n\}$ genauso zahlreich sind wie die Permutationen von $\{1, \ldots, n+1\}$, die $n+1$ als Fixpunkt haben. Nach Induktionsannahme gibt es $n!$ viele Permutationen von $\{1, \ldots, n\}$. Für jede solche Permutation π und jede Wahl von $k \in \{1, \ldots, n+1\}$ ist $(n+1\ k) \circ \pi$ eine Permutation von $\{1, \ldots, n+1\}$. Da all diese Permutationen paarweise verschieden sind, folgt $|S_{n+1}| \geq (n+1)|S_n|$.

Umgekehrt gilt: ist $\sigma \in S_{n+1}$ beliebig, so ist $\pi := (n+1\ \sigma(n+1)) \circ \sigma$ eine Permutation, die $n+1$ als Fixpunkt hat. Da Transpositionen selbstinvers sind, gilt auch $\sigma = (n+1\ \pi(n+1)) \circ \pi$, so dass sich also jedes Element von S_{n+1} als Produkt einer Permutation mit Fixpunkt $n+1$ und einer Transposition $(n+1\ k)$ schreiben lässt. Daher werden mit der vorher beschriebenen Konstruktion alle Elemente von S_{n+1} erreicht und es folgt $|S_{n+1}| = (n+1)|S_n|$. ∎

Wegen Teil 2 und 3 lässt sich jedes $\pi \in S_n$ als Produkt von (nicht notwendigerweise disjunkten) Transpositionen schreiben. Diese Darstellung ist zwar nicht eindeutig, aber wegen Teil 4 gilt: Entweder haben alle Darstellungen von $\pi \in S_n$ eine gerade Anzahl von Transpositionen, oder alle Darstellungen haben eine ungerade Anzahl. Deshalb ist folgende Definition erlaubt:

Definition 27. Sei $\pi \in S_n$. Dann heißt

$$\operatorname{sgn}(\pi) := \begin{cases} 1 & \text{falls } \pi \text{ Produkt einer geraden Anzahl von Transpositionen ist} \\ -1 & \text{falls } \pi \text{ Produkt einer ungeraden Anzahl von Transpositionen ist} \end{cases}$$

das *Vorzeichen* (engl. *sign*) von π.

Ist F wie im Beweis von Satz 27, so gilt $\operatorname{sgn}(\pi) = (-1)^{F(\pi)}$.
Außerdem ist $\operatorname{sgn}\colon S_n \to \{-1, 1\}$ ein Gruppenhomomorphismus, d. h. es gilt $\operatorname{sgn}(\pi\sigma) = \operatorname{sgn}(\pi)\operatorname{sgn}(\sigma)$.

Beispiel.

$$\operatorname{sgn}\left(\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\right) = 1, \qquad \operatorname{sgn}\left(\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}\right) = -1$$

Definition 28. Sei $A = ((a_{i,j}))_{i,j=1}^n \in \mathbb{K}^{n\times n}$. Dann heißt

$$\det(A) := \sum_{\pi\in S_n} \operatorname{sgn}(\pi) \prod_{i=1}^{n} a_{i,\pi(i)} \in \mathbb{K}$$

die *Determinante* von A. Statt $\det(A)$ schreibt man auch

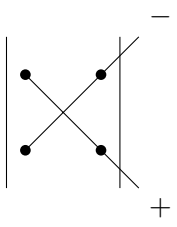
$$\begin{vmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{vmatrix}.$$

Beispiel.

1. $n = 2$, $A = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$.

$$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\} = \{ \underset{\substack{\uparrow \\ \text{sgn} = 1}}{\text{id}}, \overset{\substack{\text{sgn} = -1 \\ \downarrow}}{(1\ 2)} \}.$$

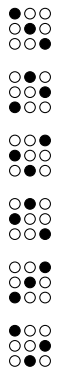
$\det A = 1 \cdot a_{1,1}a_{2,2} + (-1)a_{1,2}a_{2,1} = a_{1,1}a_{2,2} - a_{1,2}a_{2,1}$.



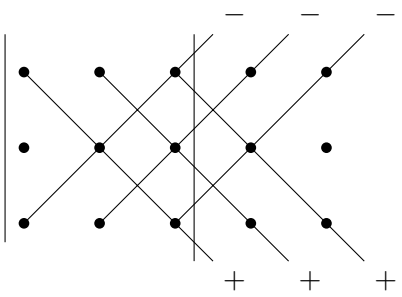
2. $n = 3$, $A = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}$.

$$S_3 = \{ \underset{+}{\text{id}}, \underset{-}{(1\ 2)}, \underset{-}{(1\ 3)}, \underset{-}{(2\ 3)}, \underset{+}{(1\ 3\ 2)}, \underset{+}{(1\ 2\ 3)} \}.$$

$$\begin{aligned}
\det(A) &= a_{1,1}a_{2,2}a_{3,3} \\
&+ a_{1,3}a_{2,1}a_{3,2} \\
&+ a_{1,2}a_{2,3}a_{3,1} \\
&- a_{1,2}a_{2,1}a_{3,3} \\
&- a_{1,3}a_{2,2}a_{3,1} \\
&- a_{1,1}a_{2,3}a_{3,2}
\end{aligned}$$



Für die Handrechnung ist es nützlich, die 3×5-Matrix zu betrachten, die man aus A erhält, wenn man die erste Spalte in die vierte und die zweite in die fünfte kopiert. Dann lässt sich die Determinante berechnen, indem man für die drei absteigenden und die drei aufsteigenden Diagonalen jeweils das Produkt der Elemente berechnet, bei den aufsteigenden Diagonalen das Vorzeichen ändert, und die Ergebnisse aufaddiert.



Ab $n = 4$ wird die Berechnung von $\det(A)$ mit der Definition unangenehm. (Beachte: $|S_4| = 24$, $|S_5| = 120$.) Wir werden aber in Kürze sehen, dass die Berechnung von $\det(A)$ mit dem gleichen Aufwand möglich ist wie die Lösung eines Gleichungssystems.

Satz 28. Für alle $A \in \mathbb{K}^{n\times n}$ gilt $\det(A) = \det(A^\top)$.

Beweis. Zunächst gilt

$$\prod_{i=1}^{n} a_{i,\pi(i)} = \prod_{i=1}^{n} a_{\sigma(i),\pi(\sigma(i))}$$

für jedes beliebige $\sigma \in S_n$, weil $(\mathbb{K} \setminus \{0\}, \cdot)$ kommutativ ist (σ vertauscht bloß die Reihenfolge der Faktoren im Produkt).

Für $\sigma = \pi^{-1}$ folgt daraus insbesondere

$$\prod_{i=1}^{n} a_{i,\pi(i)} = \prod_{i=1}^{n} a_{\pi^{-1}(i),i}.$$

Zweitens gilt $\operatorname{sgn}(\pi) = \operatorname{sgn}(\pi^{-1})$ wegen der Teile 3 und 4 von Satz 27.

Drittens gilt $\{\, \pi : \pi \in S_n \,\} = \{\, \pi^{-1} : \pi \in S_n \,\}$, weil S_n eine Gruppe ist. Deshalb gilt $\sum_{\pi\in S_n} f(\pi) = \sum_{\pi\in S_n} f(\pi^{-1})$ für jede Funktion $f\colon S_n \to \mathbb{K}$ (es ändert sich nur die Reihenfolge der Summanden, aber nicht der Wert der Summe).

Aus allem zusammen folgt

$$\begin{aligned}\det(A) &= \sum_{\pi\in S_n} \operatorname{sgn}(\pi) \prod_{i=1}^{n} a_{i,\pi(i)} \\ &= \sum_{\pi\in S_n} \operatorname{sgn}(\pi^{-1}) \prod_{i=1}^{n} a_{\pi^{-1}(i),i} \\ &= \sum_{\pi\in S_n} \operatorname{sgn}(\pi) \prod_{i=1}^{n} a_{\pi(i),i} = \det(A^\top).\end{aligned}$$

■

Satz 29. Sei $A \in \mathbb{K}^{n\times n}$.

1. Entsteht $B \in \mathbb{K}^{n\times n}$ aus A durch Multiplikation einer Zeile mit $\lambda \in \mathbb{K}$, so gilt $\det(B) = \lambda \det(A)$.
2. Entsteht $B \in \mathbb{K}^{n\times n}$ aus A durch Vertauschen zweier Zeilen, so gilt $\det(B) = -\det(A)$.
3. Entsteht $B \in \mathbb{K}^{n\times n}$ aus A dadurch, dass man das λ-fache einer Zeile von A zu einer anderen Zeile dazuaddiert, so gilt $\det(B) = \det(A)$.

Beweis. Schreibe jeweils $A = ((a_{i,j}))_{i,j=1}^n$, $B = ((b_{i,j}))_{i,j=1}^n$.

1. $\det(B) = \sum_{\pi\in S_n} \operatorname{sgn}(\pi) \underbrace{\prod_{i=1}^{n} b_{i,\pi(i)}}_{= \lambda \prod_{i=1}^n a_{i,\pi(i)}} = \lambda \det(A)$.
2. Sei $\tau \in S_n$ die entsprechende Transposition. gilt:

$$\begin{aligned}\det(B) &= \sum_{\pi\in S_n} \operatorname{sgn}(\pi) \prod_{i=1}^{n} a_{\tau(i),\pi(i)} \\ &= \sum_{\pi\in S_n} \operatorname{sgn}(\pi) \prod_{i=1}^{n} a_{i,(\pi\tau)(i)} \qquad (\text{weil } \tau^2 = \mathrm{id}) \\ &= \operatorname{sgn}(\tau) \sum_{\pi\in S_n} \operatorname{sgn}(\pi\tau) \prod_{i=1}^{n} a_{i,(\pi\tau)(i)} \\ &= -\sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)} \\ &= -\det(A).\end{aligned}$$

3. Wegen Teil 2 können wir o.B.d.A. annehmen, dass das λ-fache der zweiten Zeile zur ersten addiert wird, also

$$b_{1,j} = a_{1,j} + \lambda a_{2,j}$$

$$b_{i,j} = a_{i,j} \qquad (i > 1).$$

Dann gilt:

$$\begin{aligned}\det(B) &= \sum_{\pi\in S_n} \operatorname{sgn}(\pi) \underbrace{\prod_{i=1}^{n} b_{i,\pi(i)}}_{= (a_{1,\pi(1)} + \lambda a_{2,\pi(1)}) \prod_{i=2}^{n} a_{i,\pi(i)}} \\ &= \det(A) + \lambda \underbrace{\sum_{\pi\in S_n} \operatorname{sgn}(\pi) a_{2,\pi(1)} \prod_{i=2}^{n} a_{i,\pi(i)}}_{= \begin{vmatrix} a_{2,1} & \cdots & a_{2,n} \\ a_{2,1} & \cdots & a_{2,n} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{vmatrix} =: \Delta}.\end{aligned}$$

Wir sind fertig, wenn wir zeigen können, dass $\Delta = 0$ ist.

Dazu nutzen wir aus, dass Δ die Determinante einer Matrix mit zwei identischen Zeilen ist. Vertauscht man diese beiden Zeilen, so bleibt Δ gleich, und aus Teil 2 folgt deshalb $\Delta = -\Delta$, also $2\Delta = 0$. Daraus folgt $\Delta = 0$, jedoch nur, wenn $\mathbb{K}$ ein Körper ist, in dem $2 \neq 0$ gilt! Das dürfen wir nicht ohne weiteres annehmen.

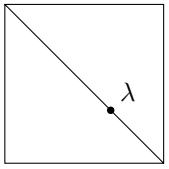
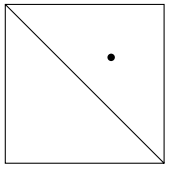
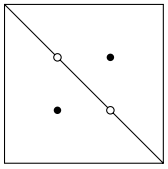
Es geht auch ohne diese Annahme: Durch $\sigma \sim \tau \iff \sigma = \tau \vee \sigma = \tau \circ (1\ 2)$ wird auf S_n eine Äquivalenzrelation erklärt. Jede Äquivalenzklasse hat genau zwei Elemente, und für beide Elemente π einer Äquivalenzklasse hat $a_{2,\pi(1)} a_{1,\pi(2)} \prod_{i=3}^{n} a_{i,\pi(i)}$ denselben Wert und $\operatorname{sgn}(\pi)$ unterschiedliches Vorzeichen. Daher gilt

$$\Delta = \sum_{[\pi]\in S_n/\sim} \underbrace{(1 + (-1))}_{=0} a_{2,\pi(1)} a_{2,\pi(2)} \prod_{i=3}^{n} a_{i,\pi(i)} = 0.$$

■

Wegen Satz 28 gilt Satz 29 auch für Spaltenoperationen statt Zeilenoperationen.

Für die Identitätsmatrix I_n folgt leicht aus der Definition, dass $\det(I_n) = 1$. Mit Satz 29 folgt daraus für die Determinate von Elementarmatrizen:

$\det\Big($  $\Big) = \lambda,$ $\det\Big($  $\Big) = 1,$ $\det\Big($  $\Big) = -1.$

Damit lassen sich Determinanten durch Zeilen- und Spaltenoperationen ausrechnen, indem man sie auf eine Form bringt, aus der man den Wert direkt ablesen kann. Insbesondere kann man den Wert einer Determinante direkt ablesen bei Matrizen, bei denen auf einer Seite der Diagonalen lauter Nullen stehen:

$$\begin{vmatrix} \lambda_1 & * & \cdots & * \\ 0 & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & * \\ 0 & \cdots & 0 & \lambda_n \end{vmatrix} = \lambda_1 \cdots \lambda_n.$$

Beispiel.

$$\begin{vmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \end{vmatrix} \overset{\substack{-1 \\ -1}}{=} \begin{vmatrix} 1 & 1 & 1 \\ 0 & 1 & 3 \\ 0 & 2 & 8 \end{vmatrix} \overset{|:8}{=} 8 \overset{+\ -1/4}{\begin{vmatrix} 1 & 1 & 1 \\ 0 & 1 & 3 \\ 0 & \frac{1}{4} & 1 \end{vmatrix}} = 8 \begin{vmatrix} 1 & \frac{3}{4} & 1 \\ 0 & \frac{1}{4} & 3 \\ 0 & 0 & 1 \end{vmatrix} = 2.$$

Satz 30. (Ergänzung zum Satz 26) $A \in \mathbb{K}^{n\times n}$ ist genau dann invertierbar, wenn $\det(A) \neq 0$ gilt.

Beweis. „⇒“ Ist A invertierbar, so lässt sich A durch Zeilenumformungen auf die Treppennormalform I_n bringen. Nach Satz 29 ändert sich bei jeder Zeilenumformung der Wert der Determinante höchstes durch Multiplikation mit einem $\lambda \in \mathbb{K} \setminus \{0\}$. Daraus folgt $\det(A) \neq 0$.

„⇐“ Ist A nicht invertierbar, so gilt $\operatorname{Rang} A < n$ und jede Treppenform T von A enthält eine Nullzeile. Für solche Treppenformen muss gelten $\det(T) = 0$. Da sich A durch Zeilenumformungen in T überführen lässt und jede Zeilenumformung den Wert der Determinaten höchstes mit einer Konstanten multipliziert, folgt $\det(A) = 0$. ∎

Satz 31. Für alle $A, B \in \mathbb{K}^{n\times n}$ gilt: $\det(AB) = \det(A)\det(B)$.

Beweis. Falls $\operatorname{Rang} A < n$ ist, ist auch $\operatorname{Rang} AB < n$, und es gilt sowohl $\det(AB) = 0$ als auch $\det(A)\det(B) = 0$.

Falls $\operatorname{Rang} A = n$ ist, ist A nach Satz 26 ein Produkt endlich vieler Elementarmatrizen, etwa $A = E_1 \cdots E_m$. Nach Satz 29 bewirkt die Multiplikation einer Matrix mit einer Elementarmatrix E die Multiplikation ihrer Determinante mit $\det(E)$. Also gilt

$$\det(AB) = \underbrace{\det(E_1)\cdots\det(E_m)}_{= \det(\underbrace{E_1\cdots E_m I_n}_{= A})} \det(B).$$

∎

Aus Satz 31 und $\det(I_n) = 1$ folgt direkt $\det(A^{-1}) = \frac{1}{\det(A)}$ für invertierbare Matrizen $A \in \mathbb{K}^{n\times n}$. Darüber hinaus folgt, dass

$$\det\colon \mathrm{GL}(n,\mathbb{K}) \to (\mathbb{K}\setminus\{0\}, \cdot)$$

ein Gruppenhomomorphismus ist. Sein Kern

$$\ker\det := \{\, A \in \mathrm{GL}(n,\mathbb{K}) : \det(A) = 1 \,\}$$

heißt die *spezielle lineare Gruppe* und wird $\mathrm{SL}(n,\mathbb{K})$ geschrieben. (Beachte: der Kern eines Gruppenhomomorphismus ist nach Teil 2 von Satz 2 eine Gruppe.)

Determinanten sind nützlich, um Vektoren auf lineare Unabhängigkeit zu untersuchen. Vor allem dann, wenn es nicht um konkrete Vektoren geht, so dass das Gauß-Verfahren sich nicht ohne weiteres anwenden lässt.

Beispiel.

1. Seien $\phi_1, \dots, \phi_n \in \mathbb{K}$ paarweise verschieden und $v_1, \dots, v_n \in \mathbb{K}^n$ definiert durch

$$v_i = (1, \phi_i, \phi_i^2, \dots, \phi_i^{n-1}) \in \mathbb{K}^n$$

für $i = 1, \dots, n$. Dann ist $\{v_1, \dots, v_n\}$ linear unabhängig. Zum Beweis zeigt man, dass

$$\begin{vmatrix} 1 & \cdots & 1 \\ \phi_1 & \cdots & \phi_n \\ \vdots & & \vdots \\ \phi_1^{n-1} & \cdots & \phi_n^{n-1} \end{vmatrix} = \underbrace{\prod_{i=2}^{n} \prod_{j=1}^{i-1} \underbrace{(\phi_i - \phi_j)}_{\neq 0}}_{\neq 0}.$$

2. Für welche Werte von $\alpha \in \mathbb{R}$ sind die Vektoren

$$\begin{pmatrix} 1 \\ \alpha \\ 2 \end{pmatrix}, \quad \begin{pmatrix} 1-\alpha \\ 0 \\ 4 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ 1 \\ -2\alpha \end{pmatrix}$$

linear abhängig? Um das zu beantworten, berechnen wir die Determinante

$$\begin{vmatrix} 1 & 1-\alpha & 1 \\ \alpha & 0 & 1 \\ 2 & 4 & -2\alpha \end{vmatrix} = -2\alpha^3 + 2\alpha^2 + 2\alpha - 2 = -2(\alpha - 1)^2(\alpha + 1).$$

Die gesuchten Werte für α sind genau jene, für die die Determinante Null wird. Das ist offensichtlich genau dann der Fall, wenn $\alpha = 1$ oder $\alpha = -1$ ist.

Satz 32. Sind $v, w, v_2, \dots, v_n \in \mathbb{K}^n$, so gilt

$$\det\big(v, v_2, \cdots, v_n\big) + \det\big(w, v_2, \cdots, v_n\big) = \det\big(v + w, v_2, \cdots, v_n\big).$$

Beweis. Übung. ∎

Satz 33. (Laplace-Entwicklung) Sei $A = ((a_{i,j}))_{i,j=1}^n \in \mathbb{K}^{n \times n}$. Es sei $A^{(i,j)} \in \mathbb{K}^{(n-1)\times(n-1)}$ die Matrix, die aus A entsteht, wenn man die i-te Zeile und die j-te Spalte löscht. Dann gilt:

$$\det(A) = a_{1,1} \det(A^{(1,1)}) - a_{1,2} \det(A^{(1,2)}) + a_{1,3} \det(A^{(1,3)}) \pm \cdots + (-1)^n a_{1,n} \det(A^{(1,n)}).$$

Beweis. Wegen Satz 29 und Satz 32 gilt zunächst

$$\det(A) = a_{1,1} \begin{vmatrix} 1 & 0 & \cdots & 0 \\ a_{2,1} & \cdots & \cdots & a_{2,n} \\ \vdots & & & \vdots \\ a_{n,1} & \cdots & \cdots & a_{n,n} \end{vmatrix}$$

$$+ a_{1,2} \begin{vmatrix} 0 & 1 & 0 & \cdots & 0 \\ a_{2,1} & \cdots & \cdots & \cdots & a_{2,n} \\ \vdots & & & & \vdots \\ a_{n,1} & \cdots & \cdots & \cdots & a_{n,n} \end{vmatrix}$$

$$+\cdots$$
$$+ a_{1,n} \begin{vmatrix} 0 & \cdots & 0 & 1 \\ a_{2,1} & \cdots & \cdots & a_{2,n} \\ \vdots & & & \vdots \\ a_{n,1} & \cdots & \cdots & a_{n,n} \end{vmatrix}.$$

Daher, und wegen Teil 2 von Satz 29, genügt es, die Behauptung für den Fall

$$A = \begin{vmatrix} 1 & 0 & \cdots & 0 \\ a_{2,1} & \cdots & \cdots & a_{2,n} \\ \vdots & & & \vdots \\ a_{n,1} & \cdots & \cdots & a_{n,n} \end{vmatrix}$$

zu zeigen. Nach Definition gilt für diesen Fall

$$\begin{aligned} \det(A) &= \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \underbrace{\prod_{i=1}^{n} a_{i,\pi(i)}}_{= 0, \text{ außer wenn } \pi(1) = 1} \\ &= \sum_{\pi \in S_n : \pi(1) = 1} \operatorname{sgn}(\pi) a_{1,1} \prod_{i=2}^{n} a_{i,\pi(i)} \\ &= \begin{vmatrix} a_{2,2} & \cdots & a_{2,n} \\ \vdots & & \vdots \\ a_{n,2} & \cdots & a_{n,n} \end{vmatrix}, \end{aligned}$$

denn die Permutationen von $\{1, \ldots, n\}$, die 1 fest lassen, sind offenbar genau die Permutationen von $\{2, \ldots, n\}$. ∎

Beispiel.

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} = 1 \begin{vmatrix} 6 & 7 & 8 \\ 10 & 11 & 12 \\ 14 & 15 & 16 \end{vmatrix} - 2 \begin{vmatrix} 5 & 7 & 8 \\ 9 & 11 & 12 \\ 13 & 15 & 16 \end{vmatrix} + 3 \begin{vmatrix} 5 & 6 & 8 \\ 9 & 10 & 12 \\ 13 & 14 & 16 \end{vmatrix} - 4 \begin{vmatrix} 5 & 6 & 7 \\ 9 & 10 & 11 \\ 13 & 14 & 15 \end{vmatrix}.$$

Sprechweise: „Die Determinante wird nach der ersten Zeile entwickelt.“ Wegen der Sätze 28 und 29 gilt Satz 33 natürlich analog für andere Zeilen oder Spalten, zum Beispiel können wir auch nach der zweiten Spalte entwickeln:

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} = -2 \begin{vmatrix} 5 & 7 & 8 \\ 9 & 11 & 12 \\ 13 & 15 & 16 \end{vmatrix} + 6 \begin{vmatrix} 1 & 3 & 4 \\ 9 & 11 & 12 \\ 13 & 15 & 16 \end{vmatrix} - 10 \begin{vmatrix} 1 & 3 & 4 \\ 5 & 7 & 8 \\ 13 & 15 & 16 \end{vmatrix} + 14 \begin{vmatrix} 1 & 3 & 4 \\ 5 & 7 & 8 \\ 9 & 11 & 12 \end{vmatrix}.$$

Zweckmäßig ist es, für die Entwicklung eine Zeile oder Spalte auszuwählen, in der viele Nullen stehen.

Man beachte bei der Entwicklung das Vorzeichenmuster für die Koeffizienten:

$$\begin{matrix} + & - & + & \cdots \\ - & + & - & \cdots \\ + & - & + & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{matrix}$$

Satz 34. (Cramersche Regel) Sei $A \in \mathbb{K}^{n\times n}$ invertierbar, $b \in \mathbb{K}^n$ und $x \in \mathbb{K}^n$ so, dass $Ax = b$ gilt. Dann ist

$$x = \Big(\frac{\det A^{(1)}}{\det A}, \ldots, \frac{\det A^{(n)}}{\det A}\Big),$$

wobei $A^{(i)}$ die Matrix ist, die aus A entsteht, wenn man die i-te Spalte durch b ersetzt.

Beweis. Schreibe $A = (a_1, \ldots, a_n)$ mit $a_1, \ldots, a_n \in \mathbb{K}^n$ und $x = (x_1, \ldots, x_n)$ mit $x_1, \ldots, x_n \in \mathbb{K}$. Dann gilt

$$\begin{aligned} x_i \det(A) &= \det(a_1, \ldots, a_{i-1}, x_i a_i, a_{i+1}, \ldots, a_n) \\ &= \det(a_1, \ldots, a_{i-1}, \underbrace{\sum_{j=1}^{n} x_j a_j}_{=b}, a_{i+1}, \ldots, a_n) = \det A^{(i)} \end{aligned}$$

für jedes $i = 1, \ldots, n$. ∎

Teil III

Vektorräume und Lineare Abbildungen

13 Vektorräume

Definition 29. Sei $(V, +)$ eine abelsche Gruppe und $\cdot\colon \mathbb{K} \times V \to V$ so, dass

1. $(\alpha + \beta) \cdot v = \alpha \cdot v + \beta \cdot v$
2. $(\alpha\beta) \cdot v = \alpha \cdot (\beta \cdot v)$
3. $\alpha \cdot (v + w) = \alpha \cdot v + \alpha \cdot w$
4. $1 \cdot v = v$

für alle $\alpha, \beta \in \mathbb{K}$ und alle $v, w \in V$. Dann heißt $(V, +, \cdot)$ ein *Vektorraum* (engl. *vector space*) über $\mathbb{K}$, oder einfach: ein $\mathbb{K}$-Vektorraum. Die Elemente von V heißen *Vektoren* (im weiteren Sinn; vgl. Def. 17). Das Neutralelement von V heißt *Nullvektor* und wird mit dem Symbol 0 bezeichnet. Die Operation $\cdot$ heißt *Skalarmultiplikation.* Statt $\alpha \cdot v$ schreibt man auch αv.

Beispiel.

1. $\mathbb{K}$ ist ein Vektorraum über sich selbst.
2. $\mathbb{K}^n$ ist ein Vektorraum über $\mathbb{K}$.
3. $\mathbb{K}^{n\times m}$ ist ein Vektorraum über $\mathbb{K}$.
4. Seien $v_1, \ldots, v_k \in \mathbb{K}^n$ und

   $$V = \{\, \alpha_1 v_1 + \cdots + \alpha_k v_k : \alpha_1, \ldots, \alpha_k \in \mathbb{K} \,\} \subseteq \mathbb{K}^n$$

   die Menge aller Linearkombinationen von $v_1, \ldots, v_k$. Dann ist V ein Vektorraum. (Beachte: $v, w \in V, \alpha, \beta \in \mathbb{K} \Rightarrow \alpha v + \beta w \in V$.) Man sagt, V „wird von $v_1, \ldots, v_k$ aufgespannt“ oder „erzeugt“.

   Insbesondere lassen sich jeder Matrix $A \in \mathbb{K}^{n\times m}$ in natürlicher Weise vier Vektorräume zuordnen:

   - der *Spaltenraum* $\operatorname{im} A$ (engl. *column space*) – das ist die Teilmenge von $\mathbb{K}^n$, die von den Spaltenvektoren von A aufgespannt wird
   - der *Zeilenraum* $\operatorname{coim} A$ (engl. *row space*) – das ist die Teilmenge von $\mathbb{K}^m$, die von den Zeilenvektoren von A aufgespannt wird
   - der *Kern* $\ker A$ – das ist die Menge aller $x \in \mathbb{K}^m$ mit $Ax = 0$
   - der *Co-Kern* $\operatorname{coker} A$ – das ist die Menge aller $x \in \mathbb{K}^n$ mit $xA = 0$.

   Dass Spaltenraum und Zeilenraum Vektorräume sind, ist klar. Dass der Kern ein Vektorraum ist, ergibt sich aus den Ergebnissen des Abschnitts über Gleichungssysteme. Dass auch der Co-Kern ein Vektorraum ist, folgt dann unmittelbar aus $\operatorname{coker} A = \ker A^\top$.
5. $\mathbb{Q}(\sqrt{2})$ ist ein Vektorraum über $\mathbb{Q}$ (vgl. Bsp. 3 nach Def. 16).
6. $\mathbb{C}$ ist ein Vektorraum über $\mathbb{R}$ (vgl. Bsp. 4 nach Def. 16).

7. $\mathbb{R}$ ist ein Vektorraum über $\mathbb{Q}$, und auch über $\mathbb{Q}(\sqrt{2})$.

8. $\mathbb{K}[X]$ ist ein Vektorraum über $\mathbb{K}$. Ebenso die Obermenge $\mathbb{K}[[X]]$ und die Untermenge

$$\mathbb{K}[X]_{\leq 3} := \{\, \alpha_0 + \alpha_1 X + \alpha_2 X^2 + \alpha_3 X^3 : \alpha_0, \ldots, \alpha_3 \in \mathbb{K} \,\} \subseteq \mathbb{K}[X]$$

   aller Polynome vom Grad höchstens drei.

9. Die Menge $\mathbb{K}^{\mathbb{N}}$ aller Folgen in $\mathbb{K}$ bildet einen Vektorraum über $\mathbb{K}$, wenn man definiert

$$\begin{aligned}(a_0, a_1, \ldots) + (b_0, b_1, \ldots) &:= (a_0 + b_0, a_1 + b_1, \ldots)\\ \alpha(a_0, a_1, \ldots) &:= (\alpha a_0, \alpha a_1, \ldots).\end{aligned}$$

   Allgemeiner: Die Menge $\mathbb{K}^A$ aller Funktionen $f\colon A \to \mathbb{K}$ bildet in natürlicher Weise einen Vektorraum über $\mathbb{K}$.

10. Im Fall $\mathbb{K} = \mathbb{R}$ bildet die Menge aller konvergenten Folgen einen Vektorraum, denn es gilt ja: sind $(a_n)_{n=0}^{\infty}$, $(b_n)_{n=0}^{\infty}$ konvergent, so ist auch $(\alpha a_n + \beta b_n)_{n=0}^{\infty}$ konvergent, für jede Wahl von Konstanten $\alpha, \beta \in \mathbb{R}$.

    Auch die Menge $N \subseteq \mathbb{R}^{\mathbb{N}}$ aller Nullfolgen bildet einen Vektorraum über $\mathbb{R}$, denn mit $\lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n = 0$ gilt auch $\lim_{n\to\infty}(\alpha a_n + \beta b_n) = 0$ für jede Wahl von Konstanten $\alpha, \beta \in \mathbb{R}$.

11. Die Menge $C(\mathbb{R}, \mathbb{R})$ aller stetigen Funktionen $f\colon \mathbb{R} \to \mathbb{R}$ ist ein Vektorraum über $\mathbb{R}$, denn wenn f, g stetig sind, so ist auch $\alpha f + \beta g$ stetig, für jede Wahl von Konstanten $\alpha, \beta \in \mathbb{R}$.

    Ebenso die Menge $C^1(\mathbb{R}, \mathbb{R})$ aller differenzierbaren Funktionen $f\colon \mathbb{R} \to \mathbb{R}$, deren Ableitung f' stetig ist, sowie die Menge $C^\infty(\mathbb{R}, \mathbb{R})$ aller beliebig oft differenzierbaren Funktionen.

12. Seien $a, b, c\colon [0,1] \to \mathbb{R}$ stetige Funktionen und sei V die Menge aller Funktionen $f\colon [0,1] \to \mathbb{R}$, die mindestens zwei mal differenzierbar sind und für die gilt

$$a(x)f(x) + b(x)f'(x) + c(x)f''(x) = 0$$

    für alle $x \in [0,1]$. Eine solche Gleichung nennt man eine (lineare) *Differentialgleichung* (zweiter Ordnung), und die Funktionen f heißen *Lösungen* (engl. *solution*) der Differentialgleichung.

    Die Menge $V \subseteq C^2([0,1], \mathbb{R})$ bildet einen Vektorraum über $\mathbb{R}$, denn wenn f, g Lösungen sind und $\alpha, \beta \in \mathbb{R}$ Konstanten, dann folgt aus

$$\begin{aligned} a\,f + b\,f' + c\,f'' &= 0 \qquad \mid \cdot\,\alpha\\ a\,g + b\,g' + c\,g'' &= 0 \qquad \mid \cdot\,\beta\end{aligned}$$

    durch Addition, dass

$$a\,(\alpha f + \beta g) + b\,(\alpha f + \beta g)' + c\,(\alpha f + \beta g)'' = 0,$$

    also $\alpha f + \beta g \in V$.

13. Seien $a, b, c\colon \mathbb{Z} \to \mathbb{K}$ Funktionen und sei V die Menge aller Funktionen $f\colon \mathbb{Z} \to \mathbb{K}$, für die gilt
$$a(n)f(n) + b(n)f(n+1) + c(n)f(n+2) = 0$$
für alle $n \in \mathbb{Z}$. Eine solche Gleichung heißt (lineare) *Rekurrenz* (zweiter Ordnung), und die Funktionen f heißen *Lösungen* der Rekurrenz.

    Die Menge $V \subseteq \mathbb{K}^{\mathbb{Z}}$ bildet einen Vektorraum über $\mathbb{K}$, denn wenn f, g Lösungen sind und $\alpha, \beta \in \mathbb{K}$ Konstanten, dann folgt aus
$$\begin{aligned} a(n)f(n) + b(n)f(n+1) + c(n)f(n+2) &= 0 \qquad &&| \cdot \alpha \\ a(n)g(n) + b(n)g(n+1) + c(n)g(n+2) &= 0 \qquad &&| \cdot \beta \end{aligned}$$
durch Addition, dass auch die Funktion $h\colon \mathbb{Z} \to \mathbb{K}$, $h(n) := \alpha f(n) + \beta g(n)$ die Rekurrenz erfüllt.

Sie werden im Verlauf Ihres Studiums noch viele weitere Vektorräume kennenlernen. Es lohnt sich deshalb, im folgenden beim Begriff „Vektor“ nicht nur an Pfeile zu denken, mit denen eine bestimmte geometrische Anschauung verbunden ist, sondern eine allgemeinere Vorstellung des Begriffs zu entwickeln, die die Beispiele oben miteinschließt. Ein Vektor ist ab jetzt einfach ein Element eines Vektorraums, und ein Vektorraum ist alles, was die Bedingungen aus Definition 29 erfüllt, egal ob man sich darunter räumlich etwas vorstellen kann oder nicht.

Satz 35. Sei V ein Vektorraum über $\mathbb{K}$. Dann gilt:

1. $\forall\, v \in V : 0 \cdot v = 0$
2. $\forall\, v \in V : (-1) \cdot v = -v$
3. $\forall\, \alpha \in \mathbb{K} : \alpha \cdot 0 = 0$
4. $\forall\, \alpha \in \mathbb{K}\ \forall\, v \in V : \alpha v = 0 \Rightarrow \alpha = 0 \vee v = 0$

Beweis. Übung ∎

Definition 30. Sei V ein $\mathbb{K}$-Vektorraum. Eine Teilmenge $\emptyset \neq U \subseteq V$ heißt *Untervektorraum* (oder einfach: *Unterraum*, engl: *subspace*) von V, falls gilt:
$$\forall\, u, v \in U\ \forall\, \alpha, \beta \in \mathbb{K} : \alpha u + \beta v \in U.$$

Beispiel.

1. Sind $u_1, \ldots, u_k \in \mathbb{K}^n$, so ist die Menge U aller Linearkombinationen von $u_1, \ldots, u_k$ ein Unterraum von $\mathbb{K}^n$. Man sagt dann, U ist die *lineare Hülle* (engl. *span*) von $u_1, \ldots, u_k$ in $\mathbb{K}^n$. Schreibweise: $V = \langle u_1, \ldots, u_k \rangle$ oder $V = \operatorname{span}(u_1, \ldots, u_k)$.

    Allgemeiner kann man statt $\mathbb{K}^n$ irgendeinen Vektorraum V betrachten: für jede Wahl von $u_1, \ldots, u_k \in V$ ist die Menge $\langle u_1, \ldots, u_k \rangle$ aller Linearkombinationen von $u_1, \ldots, u_k$ ein Unterraum von V.
2. $\mathbb{Q}(\sqrt{2})$ ist als $\mathbb{Q}$-Vektorraum ein Unterraum von $\mathbb{R}$.

3. $\mathbb{K}[X]_{\leq 3}$ ist ein Unterraum von $\mathbb{K}[X]$, und $\mathbb{K}[X]$ ist ein Unterraum von $\mathbb{K}[[X]]$.

4. Die Nullfolgen in $\mathbb{R}$ bilden einen Unterraum des Raums der konvergenten Folgen, und diese bilden einen Unterraum des Raums aller Folgen in $\mathbb{R}$.

5. Die differenzierbaren Funktionen bilden einen Unterraum des Raums aller stetigen Funktionen, und diese einen Unterraum des Raums aller reellen Funktionen.

6. Die Menge aller Lösungen $f\colon [0,1] \to \mathbb{R}$ der linearen Differentialgleichung

$$a(x)f(x) + b(x)f'(x) + c(x)f''(x) = 0$$

bildet einen Unterraum des Vektorraums $C^2([0,1],\mathbb{R})$ aller zweimal stetig differenzierbaren Funktionen.

Satz 36. Sei V ein $\mathbb{K}$-Vektorraum und $U \subseteq V$ ein Unterraum von V. Dann ist U auch ein $\mathbb{K}$-Vektorraum.

Beweis. Es ist zu zeigen, dass $(U,+)$ eine abelsche Gruppe ist und dass die Skalarmultiplikation die Gesetze aus Definition 29 erfüllt. Dass die Gesetze an sich erfüllt sind, folgt schon daraus, dass sie für V erfüllt sind und $U \subseteq V$ ist. Es könnte höchstens sein, dass U nicht unter allen Operationen abgeschlossen ist. Dass das nicht so ist, garantiert die Bedingung aus Definition 30, z. B. mit $\alpha = \beta = 1$ gilt $\forall\ u,v \in U : u+v \in U$ und mit $\alpha = -1, \beta = 0$ gilt $\forall\ u \in U : -u \in U$. Damit ist $(U,+)$ eine Untergruppe von $(V,+)$, und also eine Gruppe. Ähnlich argumentiert man für die Skalarmultiplikation. ∎

Satz 37. Sei V ein $\mathbb{K}$-Vektorraum und $U_1, U_2 \subseteq V$ seien Unterräume von V. Dann gilt:

1. $U_1 \cap U_2$ ist ein Unterraum von V.
2. $U_1 + U_2 := \{\, u_1 + u_2 : u_1 \in U_1, u_2 \in U_2 \,\}$ ist ein Unterraum von V.

Beweis.

1. Zu zeigen: $\forall\ u,v \in U_1 \cap U_2\ \forall\ \alpha,\beta \in \mathbb{K} : \alpha u + \beta v \in U_1 \cap U_2$.

   Seien $u,v \in U_1 \cap U_2$ und $\alpha,\beta \in \mathbb{K}$ beliebig. Dann gilt $u,v \in U_1$, und weil U_1 Unterraum ist, folgt $\alpha u + \beta v \in U_1$. Ebenso gilt $\alpha u + \beta v \in U_2$, weil $u,v \in U_2$ und U_2 Unterraum ist.

   Also ist $\alpha u + \beta v \in U_1 \cap U_2$, was zu zeigen war.

2. Zu zeigen: $\forall\ u,v \in U_1 + U_2\ \forall\ \alpha,\beta \in \mathbb{K} : \alpha u + \beta v \in U_1 + U_2$.

   Seien $u,v \in U_1 + U_2$ und $\alpha,\beta \in \mathbb{K}$ beliebig. Dann gibt es $u_1, v_1 \in U_1$ und $u_2, v_2 \in U_2$ mit $u = u_1 + u_2$ und $v = v_1 + v_2$. Da U_1 und U_2 Unterräume sind, gilt

$$\alpha u_1 + \beta v_1 \in U_1 \quad \text{und} \quad \alpha u_2 + \beta v_2 \in U_2,$$

   und folglich

$$\underbrace{(\alpha u_1 + \beta v_1) + (\alpha u_2 + \beta v_2)}_{=\alpha(u_1+u_2)+\beta(v_1+v_2)} \in U_1 + U_2.$$

∎

Beispiel. Sind $v_1, \ldots, v_k \in \mathbb{K}^n$ und schreibt man $\mathbb{K}v_i := \{\, \alpha v_i : \alpha \in \mathbb{K} \,\}$ $(i = 1, \ldots, k)$, so ist $\mathbb{K}v_1 + \cdots + \mathbb{K}v_k = \langle v_1, \ldots, v_k \rangle$ der Unterraum aller Linearkombinationen von $v_1, \ldots, v_k$.

Die Vereinigung $U_1 \cup U_2$ zweier Unterräume ist genau dann wieder ein Unterraum, wenn $U_1 \subseteq U_2$ oder $U_2 \subseteq U_1$ ist. Allgemein gilt: $U_1 + U_2$ ist der kleinste Vektorraum, der $U_1 \cup U_2$ enthält.

14 Basis und Dimension

Definition 31. Sei V ein $\mathbb{K}$-Vektorraum und $B \subseteq V$.

1. B heißt *linear abhängig,* falls es für eine endliche Wahl paarweise verschiedener Vektoren $v_1, \ldots, v_k \in B$ Körperelemente $\alpha_1, \ldots, \alpha_k \in \mathbb{K}$ gibt, von denen mindestens eines nicht Null ist, so dass gilt
$$\alpha_1 v_1 + \cdots + \alpha_k v_k = 0.$$
Anderenfalls heißt B *linear unabhängig.*

2. B heißt *Erzeugendensystem* (engl. *generating set*) von V, falls gilt: für alle $v \in V$ existieren $v_1, \ldots, v_k \in B$ und $\alpha_1, \ldots, \alpha_k \in \mathbb{K}$, so dass
$$v = \alpha_1 v_1 + \cdots + \alpha_k v_k.$$
Schreibweise in diesem Fall: $V = \langle B \rangle$ oder $V = \operatorname{span}(B)$. Sprechweise: „Die Elemente von B spannen V auf“ oder „erzeugen V“.

3. Ein linear unabhängiges Erzeugendensystem von V heißt *Basis* von V.

Beispiel. Sei $V = \mathbb{Q}^4$.

1. $\left\{ \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\0\\1\end{pmatrix} \right\}$ ist eine Basis von V.
Allgemeiner: ist $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ der i-te Einheitsvektor, so ist $\{e_1, \ldots, e_n\}$ eine Basis von $\mathbb{K}^n$, die sogenannte *Standardbasis.*

2. $\left\{ \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \begin{pmatrix}1\\1\\0\\0\end{pmatrix}, \begin{pmatrix}1\\1\\1\\0\end{pmatrix}, \begin{pmatrix}1\\1\\1\\1\end{pmatrix} \right\}$ ist auch eine Basis von V.

3. $\left\{ \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \begin{pmatrix}1\\1\\0\\0\end{pmatrix}, \begin{pmatrix}1\\1\\1\\0\end{pmatrix}, \begin{pmatrix}1\\1\\1\\1\end{pmatrix}, \begin{pmatrix}4\\3\\2\\1\end{pmatrix} \right\}$ ist ein Erzeugendensystem, aber keine Basis von V, da die Menge nicht linear unabhängig ist. Es gilt nämlich:
$$1\begin{pmatrix}1\\0\\0\\0\end{pmatrix} + 1\begin{pmatrix}1\\1\\0\\0\end{pmatrix} + 1\begin{pmatrix}1\\1\\1\\0\end{pmatrix} + 1\begin{pmatrix}1\\1\\1\\1\end{pmatrix} + (-1)\begin{pmatrix}4\\3\\2\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\0\end{pmatrix}.$$

4. $\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \right\}$ ist zwar linear unabhängig, aber kein Erzeugendensystem von V, da z. B. der Vektor $\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$ nicht als Linearkombination von $\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$ dargestellt werden kann.

Für jeden Vektorraum V gilt: V selbst ist ein Erzeugendensystem. Allerdings ist V niemals linear unabhängig, da immer $0 \in V$ gilt und $1 \cdot 0 = 0$ zeigt, dass $\{0\} \subseteq V$ linear abhängig ist.

Satz 38. Sei V ein $\mathbb{K}$-Vektorraum, und seien $B_1, B_2 \subseteq V$ mit $B_1 \subseteq B_2$.

1. Ist B_1 linear abhängig, so ist auch B_2 linear abhängig.
2. Ist B_2 linear unabhängig, so ist auch B_1 linear unabhängig.
3. Ist B_1 ein Erzeugendensystem von V, so ist auch B_2 ein Erzeugendensystem von V.
4. Ist B_2 kein Erzeugendensystem von V, so ist auch B_1 kein Erzeugendensystem von V.

Beweis.

1. Zu zeigen: es gibt $v_1, \ldots, v_k \in B_2$ und $(\alpha_1, \ldots, \alpha_k) \in \mathbb{K}^k \setminus \{0\}$ mit $\alpha_1 v_1 + \cdots + \alpha_k v_k = 0$. Nach Annahme gilt dies für B_1 anstelle von B_2, und damit wegen $B_1 \subseteq B_2$ erstrecht auch für B_2.
2. Folgt direkt aus Teil 1.
3. Zu zeigen: für alle $v \in V$ existieren $v_1, \ldots, v_k \in B_2$ und $\alpha_1, \ldots, \alpha_k \in \mathbb{K}$ so dass $v = \alpha_1 v_1 + \cdots + \alpha_k v_k$. Nach Annahme gilt dies für B_1, und wegen $B_1 \subseteq B_2$ erstrecht auch für B_1.
4. Folgt direkt aus Teil 3. ∎

Satz 39. Sei V ein $\mathbb{K}$-Vektorraum und $B \subseteq V$. Dann sind folgende Aussagen äquivalent:

1. B ist eine Basis von V.
2. B ist ein Erzeugendensystem von V und für jedes $b \in B$ gilt, dass $B \setminus \{b\}$ kein Erzeugendensystem von V ist.
3. B ist linear unabhängig und für jedes $v \in V \setminus B$ gilt, dass $B \cup \{v\}$ linear abhängig ist.
4. Jedes $v \in V$ lässt sich in eindeutiger Weise als Linearkombination von Elementen aus B schreiben.

Beweis.

(1)⇒(2) Gäbe es ein $b \in B$, so dass $B \setminus \{b\}$ auch ein Erzeugendensystem von V ist, dann gäbe es für dieses b eine Darstellung

$$b = \alpha_1 b_1 + \cdots + \alpha_k b_k$$

mit $b_1, \ldots, b_k \in B \setminus \{b\}$ und $\alpha_1, \ldots, \alpha_k \in \mathbb{K}$. Dann ist aber $\alpha_1 b_1 + \cdots + \alpha_k b_k + (-1)b = 0$, d. h. B wäre linear abhängig. Das steht im Widerspruch zur Annahme, dass B eine Basis ist.

(2)⇒(3) zu zeigen: (a) B ist linear unabhängig und (b) $B \cup \{v\}$ ist linear abhängig für jedes $v \in V \setminus B$.

(a) Wäre B linear abhängig, so gäbe es eine Abhängigkeit

$$\alpha_1 b_1 + \cdots + \alpha_k b_k = 0$$

für gewisse $b_1, \ldots, b_k \in B$ und $(\alpha_1, \ldots, \alpha_k) \in \mathbb{K}^k \setminus \{0\}$. O.B.d.A. können wir annehmen, dass $\alpha_1 \neq 0$. Dann aber ist

$$b_1 = (-\frac{\alpha_2}{\alpha_1})b_2 + \cdots + (-\frac{\alpha_k}{\alpha_1})b_k.$$

Damit kann jede Darstellung eines Vektors v, in der b_1 vorkommt, in eine andere übersetzt werden, in der b_1 nicht vorkommt. Also ist auch $B \setminus \{b_1\}$ ein Erzeugendensystem, im Widerspruch zur Annahme.

(b) Sei $v \in V \setminus B$ beliebig. Da B ein Erzeugendensystem ist, gibt es $b_1, \ldots, b_k \in B$ und $\alpha_1, \ldots, \alpha_k \in \mathbb{K}$ mit $v = \alpha_1 b_1 + \cdots + \alpha_k b_k$. Aber dann gilt

$$\alpha_1 b_1 + \cdots + \alpha_k b_k + (-1)v = 0,$$

d. h. $\{b_1, \ldots, b_k, v\}$ ist linear abhängig, und also auch $B \cup \{v\}$.

(3)⇒(4) (a) Existenz: zu zeigen ist, dass sich jedes $v \in V$ als Linearkombination von Elementen aus B schreiben lässt. Für $v \in B$ ist das offensichtlich. Nehmen wir also an, $v \notin B$. Nach Voraussetzung $B \cup \{v\}$ linear abhängig, d. h. es gibt $b_1, \ldots, b_k \in B$ und $(\alpha_1, \ldots, \alpha_k) \in \mathbb{K}^k \setminus \{0\}$ mit

$$\alpha_1 b_1 + \cdots + \alpha_k b_k + \alpha_{k+1} v = 0.$$

Es kann nicht $\alpha_{k+1} = 0$ sein, sonst wäre $\{b_1, \ldots, b_k\}$ linear abhängig, und damit auch B. Wenn aber $\alpha_{k+1} \neq 0$ ist, haben wir

$$v = (-\frac{\alpha_1}{\alpha_{k+1}})b_1 + \cdots + (-\frac{\alpha_k}{\alpha_{k+1}})b_k,$$

d. h. v lässt sich als Linearkombination von Elementen aus B schreiben.

(b) Eindeutigkeit: Sind

$$v = \alpha_1 b_1 + \cdots + \alpha_k b_k$$

und

$$v = \tilde{\alpha}_1 b_1 + \cdots + \tilde{\alpha}_k b_k$$

zwei Darstellungen eines Vektors $v \in V$ durch Elemente von B, so folgt

$$0 = (\alpha_1 - \tilde{\alpha}_1)b_1 + \cdots + (\alpha_k - \tilde{\alpha}_k)b_k,$$

und da B linear unabhängig ist, folgt $\alpha_1 = \tilde{\alpha}_1, \ldots, \alpha_k = \tilde{\alpha}_k$.

(4)⇒(1) Es ist klar, dass B ein Erzeugendensystem ist. Wäre B nicht linear unabhängig, so gäbe es $b_1, \ldots, b_k \in B$ und $(\alpha_1, \ldots, \alpha_k) \in \mathbb{K}^k \setminus \{0\}$ mit

$$\alpha_1 b_1 + \cdots + \alpha_k b_k = 0.$$

Eine andere Darstellung von $0 \in V$ durch Elemente von B ist aber $0b_1 + \cdots + 0b_k = 0$, im Widerspruch zur vorausgesetzten Eindeutigkeit solcher Darstellungen. ∎

Satz 40. Sei V ein $\mathbb{K}$-Vektorraum, $M_1 \subseteq V$ sei ein Erzeugendensystem von V und $M_2 \subseteq V$ sei linear unabhängig. Dann gilt $|M_1| \geq |M_2|$.

Beweis. Angenommen nicht. Dann ist $k := |M_1| < |M_2|$ insbesondere endlich und es gibt paarweise verschiedene Vektoren $v_1, \ldots, v_{k+1} \in M_2$.

Nach Satz 38 ist $\{v_1, \ldots, v_{k+1}\}$ linear unabhängig, weil M_2 linear unabhängig ist. Wir zeigen, dass $\{v_1, \ldots, v_{k+1}\}$ linear abhängig ist und kommen so zu einem Widerspruch zur Annahme $|M_1| < |M_2|$.

Schreibe $M_1 = \{b_1, \ldots, b_k\}$. Da M_1 nach Voraussetzung ein Erzeugendensystem ist, lässt sich jedes $v_i \in M_2 \subseteq V$ als Linearkombination von $b_1, \ldots, b_k$ schreiben, etwa

$$\begin{aligned} v_1 &= \alpha_{1,1}b_1 + \alpha_{1,2}b_2 + \cdots + \alpha_{1,k}b_k \\ &\vdots \\ v_{k+1} &= \alpha_{k+1,1}b_1 + \alpha_{k+1,2}b_2 + \cdots + \alpha_{k+1,k}b_k. \end{aligned}$$

Betrachte die Matrix

$$A = \begin{pmatrix} \alpha_{1,1} & \cdots & \alpha_{1,k} \\ \vdots & \ddots & \vdots \\ \alpha_{k+1,1} & \cdots & \alpha_{k+1,k} \end{pmatrix} \in \mathbb{K}^{(k+1)\times k}.$$

Wegen Satz 23 in Verbindung mit Satz 24 gilt $\operatorname{Rang} A \leq k$. Damit gibt es $\beta_1, \ldots, \beta_{k+1} \in \mathbb{K}$, von denen nicht alle Null sind, so dass

$$\beta_1 \begin{pmatrix} \alpha_{1,1} \\ \vdots \\ \alpha_{1,k} \end{pmatrix} + \cdots + \beta_{k+1} \begin{pmatrix} \alpha_{k+1,1} \\ \vdots \\ \alpha_{k+1,k} \end{pmatrix} = 0,$$

d. h.

$$\begin{aligned} \beta_1\alpha_{1,1} + \cdots + \beta_{k+1}\alpha_{k+1,1} &= 0, \\ &\vdots \\ \beta_1\alpha_{1,k} + \cdots + \beta_{k+1}\alpha_{k+1,k} &= 0, \end{aligned}$$

d.h.

$$\begin{aligned}(\beta_1\alpha_{1,1} + \cdots + \beta_{k+1}\alpha_{k+1,1})b_1 &= 0,\\ &\vdots\\ (\beta_1\alpha_{1,k} + \cdots + \beta_{k+1}\alpha_{k+1,k})b_k &= 0.\end{aligned}$$

Addition dieser k Gleichungen liefert

$$0 = \beta_1 \underbrace{(\alpha_{1,1}b_1 + \cdots + \alpha_{1,k}b_k)}_{=v_1} + \cdots + \beta_{k+1}\underbrace{(\alpha_{k+1,1}b_1 + \cdots + \alpha_{k+1,k}b_k)}_{=v_{k+1}},$$

also ist $\{v_1, \ldots, v_{k+1}\}$ linear abhängig. ∎

Satz 41. Sei V ein $\mathbb{K}$-Vektorraum und B_1, B_2 seien Basen von V. Dann gilt: $|B_1| = |B_2|$.

Beweis. Da B_1 als Basis insbesondere ein Erzeugendensystem von V ist und B_2 als Basis insbesondere linear unabhängig ist, folgt aus dem vorherigen Satz $|B_1| \geq |B_2|$. Umgekehrt ist auch B_2 ein Erzeugendensystem und B_1 ist linear unabhängig, so dass auch $|B_2| \geq |B_1|$ gilt. ∎

Definition 32. Sei V ein $\mathbb{K}$-Vektorraum und B eine Basis von V. Dann heißt

$$\dim V := |B| \in \mathbb{N} \cup \{\infty\}$$

die *Dimension* von V.

Wegen des vorherigen Satzes hängt die Dimension nicht von der Wahl der Basis ab, sondern nur vom Vektorraum. Die Definition ist also in dieser Form zulässig.

Ist M irgendeine linear unabhängige Teilmenge von V, so gilt $|M| \leq \dim V$, und ist M irgendein Erzeugendensystem von V, so ist $|M| \geq \dim V$.

Wenn V sowohl als Vektorraum über $\mathbb{K}$ als auch als Vektorraum über einem anderen Körper $\mathbb{K}'$ aufgefasst werden kann, dann hängt die Dimension im allgemeinen davon ab, welchen Körper man zugrunde legt. Man schreibt deshalb auch $\dim_{\mathbb{K}} V$ statt $\dim V$, wenn der Körper nicht aus dem Zusammenhang klar ist.

Beispiel.

1. $\dim\{0\} = 0$
2. $\dim \mathbb{K} = 1$, wenn man $\mathbb{K}$ als Vektorraum über sich selbst auffasst.
3. $\dim \mathbb{K}^n = n$
4. $\dim \mathbb{K}^{n\times m} = nm$
5. Sei $v_1, \ldots, v_k \in \mathbb{K}^n$ und sei

   $$V = \{\, \alpha_1 v_1 + \cdots + \alpha_k v_k : \alpha_1, \ldots, \alpha_k \in \mathbb{K} \,\}$$

   die Menge aller Linearkombinationen von $v_1, \ldots, v_k$. Klarerweise ist $\{v_1, \ldots, v_k\}$ ein Erzeugendensystem von V, d. h. es gilt $V = \langle v_1, \ldots, v_k\rangle$.

Wegen Satz 38 gilt daher $\dim V \leq k$. Gleichheit gilt genau dann, wenn $\{v_1, \ldots, v_k\}$ linear unabhängig (und damit eine Basis) ist.

Um das zu überprüfen bzw. um eine Basis zu bestimmen, berechnet man eine Trepenform von $\begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} \in \mathbb{K}^{k \times n}$. Die von 0 verschiedenen Zeilen bilden eine Basis von V. (Beweis: Übung.)

Insbesondere gilt: $\dim V = \operatorname{Rang} \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix}$.

6. Eine Basis von $\mathbb{K}[X]$ ist $B = \{1, X, X^2, X^3, \ldots\}$. Es gilt also $\dim \mathbb{K}[X] = \infty$. Eine andere Basis von $\mathbb{K}[X]$ ist $\{1, X, X(X-1), X(X-1)(X-2), X(X-1)(X-2)(X-3), \ldots\}$. Es gilt sogar: Wenn $b\colon \mathbb{N} \to \mathbb{K}[X] \setminus \{0\}$ eine beliebige Folge von Polynomen ist mit der Eigenschaft $\deg b_n = n$ für alle $n \in \mathbb{N}$, dann ist $\{ b_n : n \in \mathbb{N} \}$ eine Basis von $\mathbb{K}[X]$. Dabei bezeichnet $\deg b_n$ den Grad des Polynoms b_n.

7. Eine Basis von $\mathbb{K}[[X]]$ ist nicht bekannt. Aus dem nächsten Satz folgt aber, dass wegen $\mathbb{K}[X] \subseteq \mathbb{K}[[X]]$ und $\dim \mathbb{K}[X] = \infty$ der Vektorraum $\mathbb{K}[[X]]$ allenfalls eine unendliche Basis haben kann. Im darauffolgenden Satz 43 werden wir zeigen, dass jeder Vektorraum eine Basis hat. Es gilt also $\dim \mathbb{K}[[X]] = \infty$.

Satz 42. Sei V ein $\mathbb{K}$-Vektorraum und $U \subseteq V$ ein Unterraum von V. Dann gilt $\dim U \leq \dim V$.

Im Fall $\dim V < \infty$ gilt außerdem $\dim U = \dim V \iff U = V$.

Beweis. Sei B_U eine Basis von U und B_V eine Basis von V. Dann gilt $|B_U| = \dim U$ und $|B_V| = \dim V$ und wegen $U \subseteq V$ auch $B_U \subseteq V$. Als Basis von U ist B_U linear unabhängig, und als Basis von V ist B_V ein Erzeugendensystem von V. Aus Satz 40 folgt deshalb $|B_U| \leq |B_V|$. Damit ist die Ungleichung bewiesen.

Zur Gleichheit ist offensichtlich, dass $U = V \Rightarrow \dim U = \dim V$ gilt. Es bleibt also zu zeigen, dass $U \subseteq V \wedge \dim U = \dim V \Rightarrow U = V$ gilt. Angenommen nicht, d. h. angenommen es gilt $U \subsetneq V$. Dann gibt es also mindestens ein $v \in V$, das nicht in U liegt. Ist B eine Basis von U, so ist dann $B \cup \{v\}$ linear unabhängig, und damit $\dim V \geq \dim U + 1 > \dim U$. ∎

Als nächstes wollen wir beweisen, dass jeder Vektorraum eine Basis hat. Dazu brauchen wir zunächst ein weiteres Axiom aus der Mengenlehre.

Axiom. (Lemma von Zorn) Es sei M eine Menge, $\leq$ eine Halbordnung auf M (d. h. eine Relation, die reflexiv, transitiv und antisymmetrisch ist), und es gelte: Für jede aufsteigende Kette

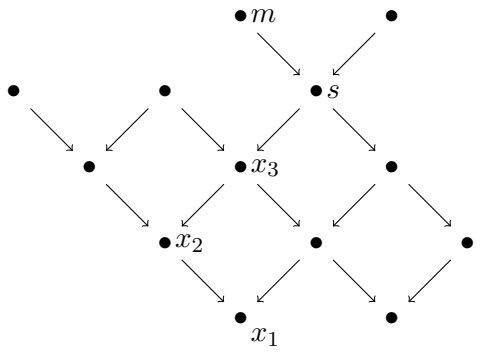
$$x_1 \leq x_2 \leq x_3 \leq \cdots$$

von Elementen von M existiert ein $s \in M$, so dass für jedes Element x_i in der Kette gilt $x_i \leq s$.

Dann gilt: $\exists\, m \in M\ \forall\, x \in M : m \leq x \Rightarrow m = x$.

Beispiel.

1.



2. $M = [0,1] \subseteq \mathbb{R}$. Es gilt: jede monoton steigende Folge $x_1 \leq x_2 \leq \cdots$ in $[0,1]$ hat eine obere Schranke in $[0,1]$, nämlich zum Beispiel $\sup\{x_1, x_2, \dots\}$. (Beachte: $[0,1]$ ist abgeschlossen.) Aus dem Axiom folgt die Existenz von $\max[0,1]$.

3. Sei A eine beliebige Menge. Betrachte $M = \mathcal{P}(A)$ und die Inklusion $\subseteq$ als Halbordnung. Es gilt: Für jede Kette
$$A_1 \subseteq A_2 \subseteq \cdots$$
in M gibt es ein $S \in \mathcal{P}(A)$ mit $A_i \subseteq S$ für alle i, nämlich zum Beispiel $S = \bigcup_i A_i$.

   Aus dem Axiom folgt die Existenz einer Menge $U \in \mathcal{P}(A)$, die nicht in einer noch größeren Menge enthalten ist. (So eine Menge U ist zum Beispiel A selbst.)

Satz 43. (Basisergänzungssatz) Sei V ein $\mathbb{K}$-Vektorraum und $A \subseteq V$ linear unabhängig. Dann gibt es eine Basis B von V mit $A \subseteq B$.

Insbesondere gilt: Jeder Vektorraum hat eine Basis.

Beweis. Betrachte die Menge
$$M = \{\, U : A \subseteq U \subseteq V \text{ und } U \text{ ist linear unabhängig} \,\}$$
zusammen mit der Halbordnung $\subseteq$. Jede Kette
$$A_1 \subseteq A_2 \subseteq \cdots$$
in M hat eine obere Schranke, nämlich zum Beispiel $S = \bigcup_i A_i$. Klarerweise gilt $A_i \subseteq S$ für alle i. Außerdem gilt auch $S \in M$ (d. h. S ist linear unabhängig), denn für jede Wahl $v_1, \dots, v_k \in S$ von endlich vielen Vektoren gibt es ein $i_0 \in \mathbb{N}$, so dass $v_1, \dots, v_k \in \bigcup_{i=1}^{i_0} A_i = A_{i_0} \in M$, d. h. aus $\alpha_1 v_1 + \cdots + \alpha_k v_k = 0$ folgt $\alpha_1 = \cdots = \alpha_k = 0$.

Aus dem Zornschen Lemma folgt daher die Existenz einer Menge $B \in M$, die maximal ist in dem Sinn, dass $B \cup \{v\}$ für jedes $v \in V \setminus B$ linear abhängig ist. Mit Satz 39 folgt, dass B eine Basis von V ist. ∎

Für endlich-dimensionale Vektorräume lässt sich der Satz durch ein weniger abstraktes Argument einsehen. Betrachte dazu folgenden „Algorithmus“:

1 $B := A$

2 solange B kein Erzeugendensystem von V ist:

3 wähle ein $v \in V \setminus \langle B \rangle$

4 setze $B := B \cup \{v\}$

5 return B.

Dabei bezeichnet $\langle B \rangle$ wie üblich den Unterraum von V, der von den Elementen von B erzeugt wird. Man überzeugt sich leicht durch Induktion, dass B während des gesamten Algorithmus linear unabhängig ist, also insbesondere auch am Ende. Ferner ist klar, dass B am Ende auch ein Erzeugendensystem ist, also der Algorithmus tatsächlich eine Basis von V produziert, die A enthält. Da sich in jedem Schleifendurchlauf die Dimension von $\langle B \rangle$ um eins erhöht, ist klar, dass der Algorithmus nach spätestens $\dim V$ ($< \infty$) vielen Schritten terminiert. Im Fall $\dim V = \infty$ funktioniert dieses Argument nicht, weil dann der Algorithmus nicht terminiert.

Beispiel. $V = \mathbb{R}^4$,

$$A = \{ \underbrace{\begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}}_{a_1}, \underbrace{\begin{pmatrix} 5 \\ 6 \\ 7 \\ 8 \end{pmatrix}}_{a_2} \}.$$

Um A zu einer Basis von V zu ergänzen, berechne eine Treppenform von $\binom{a_1}{a_2} \in \mathbb{R}^{2\times 4}$ und fülle diese mit Einheitsvektoren zu einer quadratischen Matrix von maximalem Rang auf. A bildet zusammen mit den hinzugefügten Einheitsvektoren eine Basis von V.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \end{pmatrix} \begin{array}{l} \\ \leftarrow\!\!\lrcorner\, + \end{array} \begin{array}{l} \\ \\ -5 \end{array} \leftrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & -4 & -8 & -12 \end{pmatrix}$$

$$\rightsquigarrow \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & -4 & -8 & -12 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Daraus folgt, dass $A \cup \{ \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \}$ eine Basis von V ist.

Natürlich gibt es andere Möglichkeiten. Zum Beispiel ist auch $A \cup \{ \begin{pmatrix} 1 \\ 2 \\ 4 \\ 4 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \}$ eine Basis von V.

15 Konstruktionen

Wie man mit Vektoren rechnet, ist in Definition 29 festgelegt. Wir wollen jetzt mit ganzen Vektorräumen „rechnen“. Damit ist gemeint, dass wir aus gegebenen Vektorräumen neue Vektorräume konstruieren wollen, und für diese Vektorräume wissen wollen, wie ihre Dimension mit der Dimension

der ursprünglichen Vektorräume zusammenhängt, bzw. wie man aus bekannten Basen der ursprünglichen Räume eine Basis des neuen Raums ausrechnen kann.

Beispiel. Nach Satz 37 gilt: Sind U_1, U_2 Unterräume eines $\mathbb{K}$-Vektorraums V, so sind auch $U_1 \cap U_2$ und $U_1 + U_2$ Unterräume. Wie bekommt man eine Basis für diese Räume, wenn man Basen B_1, B_2 von U_1 und U_2 kennt? Nehmen wir zur Vereinfachung an $V = \mathbb{K}^n$.

1. $U_1 + U_2$: In diesem Fall ist $B_1 \cup B_2$ ein Erzeugendensystem, aber im allgemeinen keine Basis. Wie im Beispiel 5 nach Definition 32 gezeigt, kann man $B_1 \cup B_2$ zu einer Basis machen, indem man eine Treppenform der Matrix der Zeilenvektoren bestimmt und daraus die Nullzeilen streicht. Ist zum Beispiel $U_1 = \langle \begin{pmatrix}1\\1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\0\end{pmatrix} \rangle$, $U_2 = \langle \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \begin{pmatrix}1\\0\\1\\1\end{pmatrix} \rangle$, so gilt

$$\begin{aligned} U_1 + U_2 &= \langle \begin{pmatrix}1\\1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \begin{pmatrix}1\\0\\1\\1\end{pmatrix} \rangle \\ &= \langle \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, \begin{pmatrix}1\\0\\1\\1\end{pmatrix} \rangle. \end{aligned}$$

2. $U_1 \cap U_2$. Für $v \in V$ gilt $v \in U_1 \cap U_2$ genau dann, wenn sich v sowohl als Linearkombination von Elementen einer Basis B_1 von U_1 als auch als Linearkombination von Elementen einer Basis B_2 von U_2 schreiben lässt. Die Menge all dieser v lässt sich bestimmen, indem man ein lineares Gleichungssystem löst.

   Beispiel: $U_1 = \langle \begin{pmatrix}1\\1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\0\end{pmatrix} \rangle$, $U_2 = \langle \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \begin{pmatrix}1\\0\\1\\1\end{pmatrix} \rangle$.

$$\begin{aligned} & \alpha_1 \begin{pmatrix}1\\1\\0\\0\end{pmatrix} + \alpha_2 \begin{pmatrix}0\\1\\0\\0\end{pmatrix} = \beta_1 \begin{pmatrix}1\\0\\0\\0\end{pmatrix} + \beta_2 \begin{pmatrix}1\\0\\1\\1\end{pmatrix} \\ \Leftrightarrow \quad & \begin{pmatrix}1 & 0 & -1 & -1\\ 1 & 1 & 0 & 0\\ 0 & 0 & 0 & -1\\ 0 & 0 & 0 & -1\end{pmatrix} \begin{pmatrix}\alpha_1\\ \alpha_2\\ \beta_1\\ \beta_2\end{pmatrix} = 0. \\ \Leftrightarrow \quad & (\alpha_1, \alpha_2, \beta_1, \beta_2) \in \langle \begin{pmatrix}1\\-1\\1\\0\end{pmatrix} \rangle. \end{aligned}$$

Daraus folgt, dass $\{1 \cdot \begin{pmatrix}1\\1\\0\\0\end{pmatrix} + (-1) \cdot \begin{pmatrix}0\\1\\0\\0\end{pmatrix}\}$ ein Erzeugendensystem von $U_1 \cap U_2$ ist.

Satz 44. Seien U_1, U_2 endlich-dimensionale Unterräume eines $\mathbb{K}$-Vektorraums V. Dann gilt:

$$\dim(U_1 + U_2) = \dim U_1 + \dim U_2 - \dim(U_1 \cap U_2).$$

Beweis. Sei $\{b_1, \ldots, b_k\}$ eine Basis von $U_1 \cap U_2$. Nach Satz 43 gibt es $b_{k+1}, \ldots, b_m \in U_1$ und $\tilde{b}_{k+1}, \ldots, \tilde{b}_\ell \in U_2$, so dass

$$\{b_1, \ldots, b_k, b_{k+1}, \ldots, b_m\}$$

eine Basis von U_1 und

$$\{b_1, \ldots, b_k, \tilde{b}_{k+1}, \ldots, \tilde{b}_\ell\}$$

eine Basis von U_2 ist. Betrachte

$$B := \{b_1, \ldots, b_k, b_{k+1}, \ldots, b_m, \tilde{b}_{k+1}, \ldots, \tilde{b}_\ell\}.$$

B ist ein Erzeugendensystem von $U_1 + U_2$, denn jedes $u \in U_1 + U_2$ lässt sich schreiben als $u = u_1 + u_2$ mit $u_1 \in U_1$ und $u_2 \in U_2$, und jedes $u_1 \in U_1$ ist eine Linearkombination von $\{b_1, \ldots, b_k, b_{k+1}, \ldots, b_m\} \subseteq B$ und jedes $u_2 \in U_2$ ist eine Linearkombination von $\{b_1, \ldots, b_k, \tilde{b}_{k+1}, \ldots, \tilde{b}_\ell\} \subseteq B$, und wenn also jedes $u_1 \in U_1$ und jedes $u_2 \in U_2$ eine Linearkombination von Elementen aus B ist, dann gilt dies auch für $u = u_1 + u_2$.
B ist auch linear unabhängig: Betrachte dazu $\alpha_1, \ldots, \alpha_k, \alpha_{k+1}, \ldots, \alpha_m, \tilde{\alpha}_{k+1}, \ldots, \tilde{\alpha}_\ell \in \mathbb{K}$ mit

$$\alpha_1 b_1 + \cdots + \alpha_m b_m + \tilde{\alpha}_{k+1}\tilde{b}_{k+1} + \cdots + \tilde{\alpha}_\ell \tilde{b}_\ell = 0.$$

Zu zeigen: $\alpha_1 = \cdots = \alpha_m = \tilde{\alpha}_{k+1} = \cdots = \tilde{\alpha}_\ell = 0$. Aus der angenommenen Relation folgt

$$\underbrace{\alpha_1 b_1 + \cdots + \alpha_m b_m}_{\in U_1} = \underbrace{(-\tilde{\alpha}_{k+1})\tilde{b}_{k+1} + \cdots + (-\tilde{\alpha}_\ell)\tilde{b}_\ell}_{\in U_2}.$$

Beide Seiten liegen also in $U_1 \cap U_2$. Der Vektor auf den beiden Seiten der Gleichung hat deshalb auch eine Darstellung $\beta_1 b_1 + \cdots + \beta_k b_k$ für gewisse $\beta_1, \ldots, \beta_k \in \mathbb{K}$. Da $\{b_1, \ldots, b_k, \tilde{b}_{k+1}, \ldots, \tilde{b}_\ell\}$ eine Basis von U_2 und damit linear unabhängig ist, folgt aus

$$\beta_1 b_1 + \cdots + \beta_k b_k = (-\tilde{\alpha}_{k+1})\tilde{b}_{k+1} + \cdots + (-\tilde{\alpha}_\ell)\tilde{b}_\ell$$

zunächst, dass $\beta_1 = \cdots = \beta_k = \tilde{\alpha}_{k+1} = \cdots = \tilde{\alpha}_\ell = 0$ ist. Wir haben es also mit dem Nullvektor zu tun, und deshalb folgt als nächstes aus

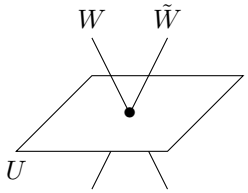
$$\alpha_1 b_1 + \cdots + \alpha_m b_m = 0$$

mit der linearen Unabhängigkeit der Basis $\{b_1, \ldots, b_m\}$ von U_1 auch $\alpha_1 = \cdots = \alpha_m = 0$.
Damit ist gezeigt, dass B eine Basis von $U_1 + U_2$ ist. Es folgt $\dim(U_1 + U_2) = |B| = m + \ell - k = \dim U_1 + \dim U_2 - \dim(U_1 \cap U_2)$. ∎

Gilt $U_1 \cap U_2 = \{0\}$, so schreibt man statt $U_1 + U_2$ auch $U_1 \oplus U_2$ und sagt, die Summe ist *direkt*. Im Fall einer direkten Summe gilt $\dim(U_1 \oplus U_2) = \dim U_1 + \dim U_2$, weil ja $\dim\{0\} = 0$ ist.

Wenn $U = U_1 + U_2$ ist, dann lässt sich jeder Vektor $u \in U$ schreiben als $u = u_1 + u_2$ für ein $u_1 \in U_1$ und ein $u_2 \in U_2$. Bei einer direkten Summe ist diese Darstellung eindeutig.

Aus dem Basisergänzungssatz folgt, dass es für jeden Unterraum U von V ein Unterraum W von V existiert mit $V = U \oplus W$. Einen solchen Raum W nennt man einen *Komplementärraum* von U. Der Komplementärraum von U ist im allgemeinen nicht eindeutig.



Satz 45. Seien U, W zwei $\mathbb{K}$-Vektorräume und B_U, B_W Basen von U bzw. W. Dann ist die Menge $V = U \times W$ zusammen mit

$$\underset{\text{in } V}{(u_1, w_1) + (u_2, w_2)} := \underset{\text{in } U}{(u_1 + u_2}, \underset{\text{in } W}{w_1 + w_2})$$

$$\underset{\text{in } V}{\alpha \cdot (u, w)} = (\underset{\text{in } U}{\alpha \cdot u}, \underset{\text{in } W}{\alpha \cdot w})$$

ein $\mathbb{K}$-Vektorraum, und $B = (B_U \times \{\underset{\in W}{0}\}) \cup (\{\underset{\in U}{0}\} \times B_W)$ ist eine Basis. Insbesondere gilt

$$\dim V = \dim U + \dim W.$$

Beweis. Dass V ein Vektorraum ist, zeigt man durch Nachrechnen der nötigen Gesetze. Die Dimensionsaussage folgt direkt aus der Aussage über die Basis. Wir zeigen: $B = (B_U \times \{0\}) \cup (\{0\} \times B_W)$ ist eine Basis von V.

B ist linear unabhängig: Seien $b_1, \ldots, b_k \in B$ und $\alpha_1, \ldots, \alpha_k \in \mathbb{K}$ mit $\alpha_1 b_1 + \cdots + \alpha_k b_k = 0$. Jedes b_i hat die Form $(b, 0)$ für ein $b \in B_U$ oder $(0, b)$ für ein $b \in B_W$. O.B.d.A. seien $b_1, \ldots, b_i$ von der ersten und $b_{i+1}, \ldots, b_k$ von der zweiten Form. Dann gilt

$$\alpha_1 b_1 + \cdots + \alpha_i b_i = 0 \quad \text{und} \quad \alpha_{i+1} b_{i+1} + \cdots + \alpha_k b_k = 0,$$

und da B_U und B_W linear unabhängig sind, folgt $\alpha_1 = \cdots = \alpha_i = 0$ und $\alpha_{i+1} = \cdots = \alpha_k = 0$.

B ist ein Erzeugendensystem: Sei $v \in V$. Dann ist $v = (u, w)$ für gewisse $u \in U$ und $w \in W$. Daraus folgt, dass es $\alpha_1, \ldots, \alpha_k \in \mathbb{K}$ und $u_1, \ldots, u_k \in B_U$ sowie $\beta_1, \ldots, \beta_\ell \in \mathbb{K}$ und $w_1, \ldots, w_\ell \in B_W$ gibt mit

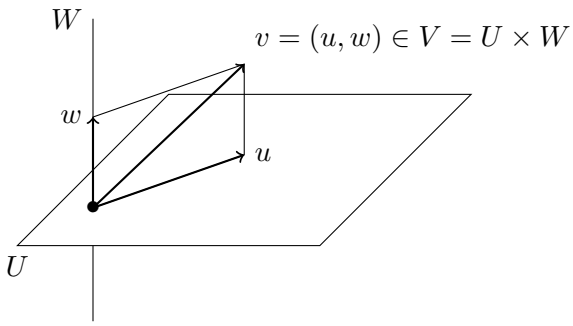
$$u = \alpha_1 u_1 + \cdots + \alpha_k u_k \quad \text{und} \quad w = \beta_1 w_1 + \cdots + \beta_\ell w_\ell.$$

Damit gilt

$$v = \begin{pmatrix} u \\ w \end{pmatrix} = \alpha_1 \begin{pmatrix} u_1 \\ 0 \end{pmatrix} + \cdots + \alpha_k \begin{pmatrix} u_k \\ 0 \end{pmatrix} + \beta_1 \begin{pmatrix} 0 \\ w_1 \end{pmatrix} + \cdots + \beta_\ell \begin{pmatrix} 0 \\ w_\ell \end{pmatrix}.$$

■

Beispiel. $U = \mathbb{R}^2$, $W = \mathbb{R}$



Wenn $\times$ eine Art „Multiplikation“ von Vektorräumen ist, wie müsste dann eine passende „Division“ aussehen? Wenn also ein Vektorraum V und ein Unterraum W von V gegeben ist, wie können wir dann sinnvoll erklären, was $U := V/W$ sein soll, damit diese Operation in gewisser Weise die Produktbildung $V = U \times W$ rückgängig macht?

Die Idee ist, dass man alle Vektoren $v \in V$, die den gleichen U-Anteil haben, als ein und denselben Vektor auffast, d. h. dass man die jeweiligen W-Anteile der Vektoren einfach ignoriert. Formal erreicht man das, indem man auf V die Äquivalenzrelation $\sim$ einführt mit

$$v_1 \sim v_2 \iff v_1 - v_2 \in W.$$

Dann gilt nämlich $v_1 \sim v_2$ genau dann, wenn v_1, v_2 den gleichen U-Anteil haben, denn dieser hebt sich dann bei der Bildung der Differenz heraus und es bleibt nur noch die Differenz der (möglicherweise unterschiedlichen) W-Anteile übrig. Es ist leicht nachzuprüfen, dass $\sim$ tatsächlich eine Äquivalenzrelation ist:

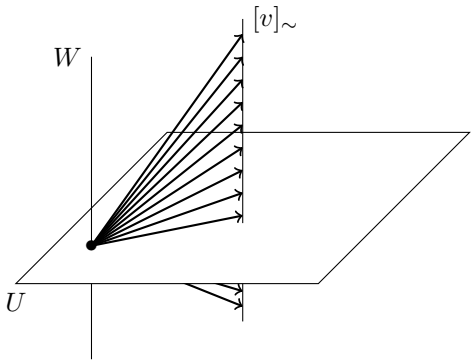
Reflexivität: Da W als Unterraum von V insbesondere ein Vektorraum ist, gilt $0 \in W$. Damit gilt für jedes $v \in V$, dass $v - v = 0 \in W$, also $v \sim v$.

Symmetrie: $v_1 \sim v_2 \Rightarrow v_1 - v_2 \in W \Rightarrow (-1) \cdot (v_1 - v_2) \in W \Rightarrow v_2 - v_1 \in W \Rightarrow v_2 \sim v_1$. Im zweiten Schritt wird wieder verwendet, dass W ein Vektorraum ist, und also abgeschlossen unter Skalarmultiplikation.

Transitivität:

$$\underbrace{\begin{array}{cc} v_1 \sim v_2 & v_2 \sim v_3 \\ \Downarrow & \Downarrow \\ v_1 - v_2 \in W & v_2 - v_3 \in W \end{array}}$$
$$\Downarrow$$
$$(v_1 - v_2) + (v_2 - v_3) = v_1 - v_3 \in W$$
$$\Downarrow$$
$$v_1 \sim v_3$$

Die Vektoren mit dem selben U-Anteil bilden genau die Äquivalenzklassen bezüglich $\sim$.



Wir zeigen als nächstes, dass sich die Menge der Äquivalenzklassen als Vektorraum auffassen lässt. Diesen Vektorraum nennt man dann den Quotientenraum V/W.

Satz 46. Sei V ein $\mathbb{K}$-Vektorraum, $W \subseteq V$ ein Unterraum von V. Für $v_1, v_2 \in V$ sei definiert $v_1 \sim v_2 \iff v_1 - v_2 \in W$. Die Menge $U := V/W := V/\sim$ bildet zusammen mit

$$\begin{aligned} +\colon U \times U \to U, &\quad [v_1]_\sim + [v_2]_\sim := [v_1 + v_2]_\sim \\ \cdot\colon \mathbb{K} \times U \to U, &\quad \alpha[v]_\sim := [\alpha v]_\sim \end{aligned}$$

einen $\mathbb{K}$-Vektorraum.

Beweis. Zu zeigen ist: (a) die Definitionen sind repräsentantenunabhängig, und (b) $(U, +, \cdot)$ ist ein Vektorraum.

(a) Addition:

$$\begin{array}{cc} v_1 \sim v_2 & \tilde{v}_1 \sim \tilde{v}_2 \\ \Downarrow & \Downarrow \\ v_1 - v_2 \in W & \tilde{v}_1 - \tilde{v}_2 \in W \end{array}$$
$$\Downarrow$$
$$(v_1 - v_2) + (\tilde{v}_1 - \tilde{v}_2) \in W$$
$$\Downarrow$$
$$v_1 + \tilde{v}_1 \sim v_2 + \tilde{v}_2$$

Skalarmultiplikation:

$$v_1 \sim v_2 \Rightarrow v_1 - v_2 \in W \Rightarrow \alpha(v_1 - v_2) = \alpha v_1 - \alpha v_2 \in W \Rightarrow \alpha v_1 \sim \alpha v_2.$$

(b) Die nötigen Gesetze sind erfüllt, weil sie nach Voraussetzung in V erfüllt sind und sich von dort übertragen. ∎

Definition 33. Der Vektorraum V/W aus obigem Satz heißt der *Quotientenraum* (engl. *quotient space*) oder *Faktorraum* von V nach W.

Satz 47. Sei V ein $\mathbb{K}$-Vektorraum, $W \subseteq V$ ein Unterraum, $U \subseteq V$ ein Komplementärraum von W (d. h. $V = U \oplus W$, d. h. $V = U + W$ und $U \cap W = \{0\}$). Weiter sei B eine Basis von U. Dann ist $\tilde{B} := \{\, [b]_\sim : b \in B \,\}$ eine Basis von V/W. Wenn U endlich-dimensional ist, gilt insbesondere $\dim V/W = \dim U$. (Wenn auch V und W endlich-dimensional sind, gilt weiters $\dim U = \dim V - \dim W$.)

Beweis. Die Dimensionsaussagen folgen unmittelbar aus der Basiseigenschaft. Daher ist nur zeigen: $\tilde{B}$ ist linear unabhängig und ein Erzeugendensystem.
(a) $\tilde{B}$ ist linear unabhängig: Seien $\alpha_1, \dots, \alpha_k \in \mathbb{K}$ und $[b_1]_\sim, \dots, [b_k]_\sim \in \tilde{B}$ so, dass

$$\alpha_1[b_1]_\sim + \cdots + \alpha_k[b_k]_\sim = [0]_\sim.$$

Dann ist $[\alpha_1 b_1 + \cdots + \alpha_k b_k]_\sim = [0]_\sim$. Dann ist

$$\underbrace{\alpha_1 b_1 + \cdots + \alpha_k b_k}_{\in U} \in W.$$

Dann $\alpha_1 b_1 + \cdots + \alpha_k b_k = 0$, da $U \cap W = \{0\}$. Dann $\alpha_1 = \cdots = \alpha_k = 0$, da B linear unabhängig ist.
(b) $\tilde{B}$ ist ein Erzeugendensystem: Sei $[x]_\sim \in V/W$. Wegen $U + W = V$ lässt sich x schreiben als $x = u + w$ für gewisse $u \in U$ und $w \in W$. Dann lässt sich u schreiben als $u = \alpha_1 b_1 + \cdots + \alpha_k b_k$ für gewisse $\alpha_1, \dots, \alpha_k \in \mathbb{K}$ und $b_1, \dots, b_k \in B$. Dann ist

$$[x]_\sim = [u]_\sim = [\alpha_1 b_1 + \cdots + \alpha_k b_k]_\sim = \alpha_1[b_1]_\sim + \cdots + \alpha_k[b_k]_\sim.$$

■

Beispiel. $V = \mathbb{R}^4$, $W = \langle \begin{pmatrix}1\\2\\3\\4\end{pmatrix}, \begin{pmatrix}5\\6\\7\\8\end{pmatrix} \rangle$. Nach dem Beispiel auf Seite 96 ist $U = \langle \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\0\\1\end{pmatrix} \rangle$ ein Komplementärraum von W, und also ist $\{[\begin{pmatrix}0\\0\\1\\0\end{pmatrix}]_\sim, [\begin{pmatrix}0\\0\\0\\1\end{pmatrix}]_\sim\}$ eine Basis von V/W.

Die nächste Konstruktion ist wieder eine Art „Multiplikation“ von Vektoräumen. Dabei nimmt man nicht das kartesische Produkt $U \times W$ der Räume selbst, sondern betrachtet den Vektorraum, der das kartesische Produkt einer Basis von U mit einer Basis von W als Basis hat.

Dazu beachte man zunächst, dass man jede beliebige Menge M als Basis eines $\mathbb{K}$-Vektorraums auffassen kann, nämlich des Raums $\mathbf{F}_\mathbb{K}(M)$ aller Funktionen $f\colon M \to \mathbb{K}$ mit $|\{x \in \mathbb{K} : f(x) \neq 0\}| < \infty$ zusammen mit der naheliegenden Addition und Skalarmultiplikation. Man nennt $\mathbf{F}_\mathbb{K}(M)$ den *freien Vektorraum* über M.

Die Menge M ist insofern eine Basis von $\mathbf{F}_\mathbb{K}(M)$, als man jedes $m \in M$ identifizieren kann mit der Funktion $\tilde{m}\colon M \to \mathbb{K}$ mit $\tilde{m}(x) = 1$ falls $x = m$ und $\tilde{m}(x) = 0$ falls $x \neq m$. Für ein Element $v \in \mathbf{F}(M)$ mit $v(m_1) = \alpha_1$, $v(m_2) = \alpha_2$ und $v(m) = 0$ für alle $m \in M \setminus \{m_1, m_2\}$ schreibt man $\alpha_1\, m_1 + \alpha_2\, m_2$, usw.

Beispiel.

1. Sei $\mathbb{K} = \mathbb{Q}$ und $M = \{a, b, c\}$. Dann besteht $\mathbf{F}_\mathbb{K}(M)$ aus allen „Linearkombinationen“ $\alpha a + \beta b + \gamma c$ mit $\alpha, \beta, \gamma \in \mathbb{K}$. Streng genommen hat diese Summe keine eigene Bedeutung sondern ist nur eine Kurzschreibweise für die Funktion $f\colon M \to \mathbb{K}$ mit $f(a) = \alpha$, $f(b) = \beta$, $f(c) = \gamma$. Allerdings sind die Addition und Skalarmultiplikation auf $\mathbf{F}_\mathbb{K}(M)$ genau so definiert, wie es die Notation suggeriert. Zum Beispiel gilt $2(5a - 3b + 8c) - (2a + 3b - c) = 8a - 3b + 17c$.

2. Für $n \in \mathbb{N}$ ist $\mathbb{K}^n = \mathbf{F}_{\mathbb{K}}(\{1, 2, \ldots, n\})$, wenn man die gewohnte Vektorschreibweise $a = (\alpha_1, \ldots, \alpha_n)$ für Elemente a von $\mathbb{K}^n$ interpretiert als eine Schreibweise für die Funktion $a\colon \{1, \ldots, n\} \to \mathbb{K}$ mit $a(i) = \alpha_i$ für $i = 1, \ldots, n$. Die Addition und Skalarmultiplikation entsprechen genau den gewohnten Vektor-Rechenregeln. In diesem Fall ist die Kurzschreibeweise $a = \alpha_1 1 + \alpha_2 2 + \cdots + \alpha_n n$ nicht zu empfehlen, weil die Symbole $1, \ldots, n$ sowohl Elemente in M als auch Elemente in $\mathbb{K}$ bezeichnen können. Wenn man aber statt $\{1, \ldots, n\}$ die Menge $\{e_1, \ldots, e_n\}$ nimmt, wobei $e_1, \ldots, e_n$ als neue Symbole verstanden werden, die nicht auch schon für gewisse Elemente von $\mathbb{K}$ stehen, dann ist die Schreibeweise $a = \alpha_1 e_1 + \cdots + \alpha_n e_n$ durchaus suggestiv. Sie passt insbesondere mit der gewohnten Schreibweise zusammen, wenn man die e_i nicht als formale Symbole interpretiert, sondern als Variablen, die für die Einheitsvektoren $(0, \ldots, 0, 1, 0, \ldots, 0)$ stehen.

3. Ähnlich wie im vorherigen Beispiel kann man sagen, dass $\mathbb{K}[X]$ nichts anderes ist als $\mathbf{F}_{\mathbb{K}}(\mathbb{N})$, wobei man für die Basiselemente $0, 1, 2, \ldots$ zur besseren Unterscheidbarkeit von Körperelementen $1, X, X^2, \ldots$ schreibt. Es sei noch einmal daran erinnert, dass auch bei unendlich großen Basen Linearkombinationen immer nur von endlich vielen Vektoren gebildet werden können. Deshalb ist z.B. $1 + X + X^2 + X^3 + \cdots$ kein Element von $\mathbb{K}[X]$.

Wenn nun U und W zwei Vektorräume sind und B_U ist eine Basis von U und B_W eine Basis von W, so kann man definieren $U \otimes W := \mathbf{F}_{\mathbb{K}}(B_U \times B_W)$. Man nennt diesen Vektorraum das *Tensorprodukt* (engl. *tensor product*) von U und W, seine Elemente heißen *Tensoren.*

Ein Tensor ist also eine Linearkombination von Paaren (b_U, b_W), wobei $b_U \in B_U$ und $b_V \in B_V$ ist. Sind $u \in U$, $w \in W$ beliebig, etwa $u = \alpha_1 b_U^{(1)} + \cdots + \alpha_k b_U^{(k)}$ für gewisse $\alpha_1, \ldots, \alpha_k \in \mathbb{K}$ und $b_U^{(1)}, \ldots, b_U^{(k)} \in B_U$, und $w = \beta_1 b_W^{(1)} + \cdots + \beta_m b_W^{(m)}$ für gewisse $\beta_1, \ldots, \beta_m \in \mathbb{K}$ und $b_W^{(1)}, \ldots, b_W^{(m)} \in B_W$, so definiert man

$$u \otimes w := \sum_{i=1}^{k} \sum_{j=1}^{m} \alpha_i \beta_j (b_U^{(i)}, b_V^{(j)}) \in U \otimes W.$$

Insbesondere gilt dann $b_U \otimes b_W = (b_U, b_W)$ für alle $b_U \in B_U$ und $b_W \in B_W$. Ferner gelten die Rechenregeln $\alpha(u \otimes w) = (\alpha u) \otimes w = u \otimes (\alpha w)$ und $(u_1 + u_2) \otimes w = (u_1 \otimes w) + (u_2 \otimes w)$ und $u \otimes (w_1 + w_2) = (u \otimes w_1) + (u \otimes w_2)$ und insbesondere $u \otimes 0 = 0 \otimes w = 0$ für alle $\alpha \in \mathbb{K}$, $u, u_1, u_2 \in U$ und $w, w_1, w_2 \in W$.

Beispiel. Im Fall $U = \mathbb{K}^n$ und $W = \mathbb{K}^m$ kann man sich $V = U \otimes W$ als den Raum $\mathbb{K}^{n \times m}$ der Matrizen vorstellen. Nimmt man für U und W jeweils die Standardbasis $\{e_1, \ldots, e_n\} \subseteq U$ bzw. $\{\tilde{e}_1, \ldots, \tilde{e}_m\} \subseteq W$, so entspricht $e_i \otimes \tilde{e}_j$ der Matrix, die eine 1 an der Stelle (i, j) hat, und überall sonst nur Nullen.

Allgemeiner: Sind $u = (u_1, \ldots, u_n) \in U$, $w = (w_1, \ldots, w_m) \in W$ zwei beliebige Vektoren, so entspricht der Tensor $u \otimes w \in U \otimes W$ der Matrix, die man erhält, wenn man u als Spaltenvektor mit w als Zeilenvektor multipliziert, also

$$\begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} (w_1, w_2, \ldots, w_m) = \begin{pmatrix} u_1 w_1 & u_1 w_2 & \cdots & u_1 w_m \\ u_2 w_1 & u_2 w_2 & \cdots & u_2 w_m \\ \vdots & \vdots & \ddots & \vdots \\ u_n w_1 & u_2 w_n & \cdots & u_n w_m \end{pmatrix}.$$

Dass nicht jede Matrix diese Form hat, verdeutlicht, dass sich nicht jeder Tensor $v \in U \otimes W$

schreiben lässt als $v = u \otimes w$ für gewisse $u \in U, w \in W$. Es gibt zum Beispiel im Fall $n = m = 2$ keine $(u_1, u_2), (w_1, w_2) \in \mathbb{K}^2$, so dass $\begin{pmatrix} u_1 \\ u_2 \end{pmatrix} (w_1, w_2) = \begin{pmatrix} u_1 w_1 & u_1 w_2 \\ u_2 w_1 & u_2 w_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ist.

Die obige Definition von $U \otimes W$ ist etwas unbefriedigend, weil sie auf Basen von U und W zurückgreift. Wählt man statt B_U und B_W zwei andere Basen B'_U, B'_W, so ist $\mathbf{F}_{\mathbb{K}}(B_U \times B_W)$ streng genommen nicht dasselbe wie $\mathbf{F}_{\mathbb{K}}(B'_U \times B'_W)$. Es zeigt sich aber, dass diese Räume „im wesentlichen“ dieselben sind. Um das konkret zu machen, verwendet man den Begriff der Isomorphie von Vektorräumen, um den es im folgenden Abschnitt gehen wird.

16 Lineare Abbildungen und Isomorphie

Definition 34. Seien V, W zwei $\mathbb{K}$-Vektorräume.

1. $h\colon V \to W$ heißt *Homomorphismus* oder *lineare Abbildung,* falls gilt

$$\forall\, x, y \in V\ \forall\, \alpha, \beta \in \mathbb{K} : h(\alpha \cdot x \overset{\text{in } V}{+} \beta \cdot y) = \alpha \cdot h(x) \overset{\text{in } W}{+} \beta \cdot h(y).$$

   Ein Homomorphismus von V nach V heißt auch *Endomorphismus.*

2. Ein bijektiver Homomorphismus heißt *Isomorphismus.* Wenn ein solcher existiert, sagt man, V und W sind (zueinander) *isomorph.* Schreibweise: $V \cong W$.

   Ein Isomorphismus von V nach V heißt auch *Automorphismus.*

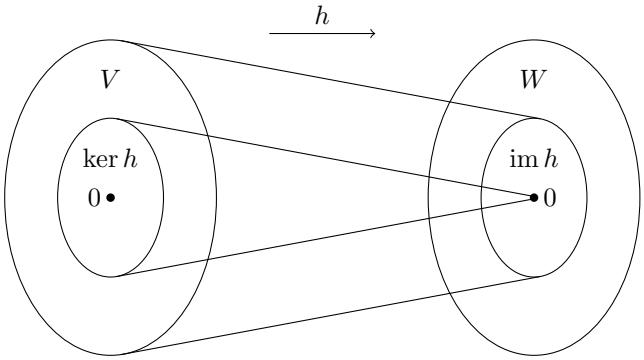
3. Ist $h\colon V \to W$ ein Homomorphismus, so heißt

$$\ker h := \{\, x \in V : h(x) = 0 \,\}$$

   der *Kern* (engl. *kernel*) und

$$\operatorname{im} h := h(V) = \{\, h(x) : x \in V \,\}$$

   das *Bild* (engl. *image*) von h.



Beispiel.

1. $f\colon \mathbb{R} \to \mathbb{R}$, $f(x) = 3x$ ist linear. Die Funktionen $g\colon \mathbb{R} \to \mathbb{R}$, $g(x) = 3x+5$ und $h\colon \mathbb{R} \to \mathbb{R}$, $h(x) = x^2$ sind nicht linear.

2. $V = \mathbb{K}^m$, $W = \mathbb{K}^n$. Für jede beliebige Matrix $A \in \mathbb{K}^{n\times m}$ ist

$$h\colon V \to W, \quad h(x) = Ax$$

eine lineare Abbildung. Es gilt ja

$$h(\alpha x + \beta y) = A(\alpha x + \beta y) = \alpha Ax + \beta Ay = \alpha h(x) + \beta h(y)$$

für alle $\alpha, \beta \in \mathbb{K}$ und alle $x, y \in V$.

3. $V = \mathbb{K}[X]$, $W = \mathbb{K}^{\mathbb{K}}$. Die Funktion

$$h\colon V \to W, \quad h(a_0 + a_1X + \cdots + a_nX^n) := (z \mapsto a_0 + a_1z + \cdots + a_nz^n),$$

die jedem Polynom die entsprechende Polynomfunktion zuordnet, ist linear.

4. Die Abbildung

$$h\colon \mathbb{K}[[X]] \to \mathbb{K}[X], \quad h(\sum_{k=0}^{\infty} a_nX^n) := \sum_{k=0}^{12} a_nX^n$$

ist linear.

5. Die Abbildung $h\colon \mathbb{K}^{n\times m} \to \mathbb{K}^n$, die dadurch definiert ist, dass $h(A)$ die erste Spalte von A ist, ist linear.

6. Sei $V = \mathbb{K}[[X]]$ und $N \in \mathbb{N}$ fix. Dann ist die Abbildung

$$[X^N]\colon V \to \mathbb{K}, \qquad [X^N]\sum_{n=0}^{\infty} a_nX^n := a_N,$$

die aus einer formalen Potenzreihe den N-ten Koeffizient extrahiert, linear.

7. Sei V der $\mathbb{R}$-Vektorraum aller konvergenten Folgen, $W = \mathbb{R}$. Dann ist

$$h\colon V \to W, \quad h(\,(a_n)_{n=0}^{\infty}\,) := \lim_{n\to\infty} a_n$$

eine lineare Abbildung. Ihr Kern ist der Raum aller Nullfolgen.

8. Die Funktion $h\colon \mathbb{Q} \to \mathbb{Q}(\sqrt{2})$ mit $h(x) = x + 0\sqrt{2}$ für alle $x \in \mathbb{Q}$ ist linear.

9. Die Funktionen $\mathrm{Re}, \mathrm{Im}\colon \mathbb{C} \to \mathbb{R}$, die jeder komplexen Zahl ihren Realteil bzw. ihren Imaginärteil zuordnen, sind linear, wenn man $\mathbb{C}$ als Vektorraum über $\mathbb{R}$ auffasst.

10. Sei $V = C^5([-1,1], \mathbb{R})$ die Menge aller fünf mal stetig differenzierbaren Funktionen $f\colon [-1,1] \to \mathbb{R}$. Die Funktion $h\colon V \to \mathbb{R}^6$ mit $h(f) = (f(0), f'(0), \ldots, f^{(5)}(0))$ ist linear.

11. Sei V ein $\mathbb{K}$-Vektorraum, U ein Unterraum von V, $W = V/U$ und $h\colon V \to W$, $h(x) = [x]_{\sim}$. Dann ist h eine lineare Abbildung. Ihr Kern ist U.

12. Sind U, W zwei $\mathbb{K}$-Vektorräume und $V = U \times W$, so ist $\pi\colon V \to U$, $\pi(u, w) = u$ eine lineare Abbildung, die zwar surjektiv aber nicht injektiv ist. Ihr Kern ist $\ker \pi = \{0\} \times W$.

13. Sind U, W zwei $\mathbb{K}$-Vektorräume, so ist $h\colon U \times W \to U \otimes W$, $h(u, w) = u \otimes w$ eine lineare Abbildung, aber kein Isomorphismus, weil h zwar injektiv, aber nicht surjektiv ist.

    Für jedes fest gewählte $w \in W$ ist auch die Abbildung $h\colon U \to U \otimes W$, $h(u) = u \otimes w$ eine lineare Abbildung.

14. Wenn $V = U \oplus W$ gilt, so ist $U \cong V/W$.

15. $\mathbf{F}_{\mathbb{K}}(\{1, \dots, n\}) \cong \mathbb{K}^n$.

16. Ist V irgendein Vektorraum und B eine Basis von V, so gilt $\mathbf{F}_{\mathbb{K}}(B) \cong V$.

17. Für zwei $\mathbb{K}$-Vektorräume U, W gilt $(U \times W) \cong (W \times U)$ und $(U \otimes W) \cong (W \otimes U)$. Echte Gleichheit gilt in beiden Fällen nur, wenn $U = W$ ist.

18. Die Abbildung $\cdot^{\top}\colon \mathbb{K}^{n \times m} \to \mathbb{K}^{m \times n}$, die jeder Matrix $A \in \mathbb{K}^{n \times m}$ ihre Transponierte zuordnet, ist linear.

19. Es gilt $\mathbb{K}^n \otimes \mathbb{K}^m \cong \mathbb{K}^{n \times m}$.

20. Sei $V = C^\infty([0, 1], \mathbb{R})$. Dann ist die Abbildung $\frac{d}{dx}$, die jedem Element des Vektorraums dessen Ableitung zuordnet, linear. Ihr Kern ist die Menge der konstanten Funktionen.

    Für $V = \mathbb{K}[[X]]$ definiert man

    $$\frac{d}{dx}\colon V \to V, \quad \frac{d}{dx} \sum_{n=0}^{\infty} a_n X^n := \sum_{n=0}^{\infty} (n+1) a_{n+1} X^n.$$

    Auch diese (formale) „Ableitung“ ist eine lineare Abbildung.

21. Die Abbildung

    $$I\colon C([0, 1], \mathbb{R}) \to \mathbb{R}, \quad I(f) := \int_0^1 f(t)\, dt$$

    ist linear.

22. Sei $V = \mathbb{R}^{n+1}$ und $W = \mathbb{R}[X]$. Ferner seien $x_0, \dots, x_n \in \mathbb{R}$ fest gewählte paarweise verschiedene reelle Zahlen. Man kann zeigen, dass es dann für jede Wahl von $y_0, \dots, y_n \in \mathbb{R}$ genau ein Polynom $p \in \mathbb{R}[X]$ mit Grad höchstens n gibt, so dass $p(x_i) = y_i$ für alle i gilt. Mit $p(x_i)$ ist dabei die Auswertung der zu p gehörigen Polynomfunktion an der Stelle x_i gemeint. Man nennt p das *Interpolationspolynom* für $(x_0, y_0), \dots, (x_n, y_n)$.

    Die Abbildung, die jedem $(y_0, \dots, y_n) \in V$ dieses Polynom p zuordnet, ist linear.

Satz 48.

1. Die Verkettung linearer Abbildungen ist linear. Die Umkehrfunktion einer bijektiven linearen Abbildung ist linear.

2. Für je drei Vektorräume U, V, W gilt $U \cong U$, $U \cong V \Rightarrow V \cong U$, $U \cong V \wedge V \cong W \Rightarrow U \cong W$.

3. Sind V, W zwei $\mathbb{K}$-Vektorräume und ist $h\colon V \to W$ ein Homomorphismus, so ist $\ker h$ ein Unterraum von V und $\operatorname{im} h$ ein Unterraum von W.

Beweis.

1. Verkettung: Seien U, V, W drei $\mathbb{K}$-Vektorräume, $f\colon U \to V$ und $g\colon V \to W$ Homomorphismen und $h\colon U \to W$, $h(x) := g(f(x))$ deren Verkettung. Für $\alpha, \beta \in \mathbb{K}$ und $x, y \in V$ gilt dann:

   $$h(\alpha x+\beta y) = g(f(\alpha x+\beta y)) = g(\alpha f(x)+\beta f(y)) = \alpha g(f(x))+\beta g(f(y)) = \alpha h(x)+\beta h(y).$$

   Umkehrfunktion: Seien V, W zwei $\mathbb{K}$-Vektorräume, $f\colon V \to W$ ein Isomorphismus und $f^{-1}\colon W \to V$ seine Umkehrfunktion. Für $\alpha, \beta \in \mathbb{K}$ und $x, y \in W$ gilt dann

   $$f(\alpha f^{-1}(x) + \beta f^{-1}(y)) = \alpha f(f^{-1}(x)) + \beta f(f^{-1}(y)) = \alpha x + \beta y.$$

   Anwendung von f^{-1} auf beiden Seiten und Rückwärtslesen der Gleichung liefert

   $$f^{-1}(\alpha x + \beta y) = \alpha f^{-1}(x) + \beta f^{-1}(y).$$

2. Reflexivität: $U \cong U$ gilt, da die Identitätsfunktion id_U linear ist.

   Symmetrie: Folgt auch aus Teil 1 (Linearität der Umkehrfunktion).

   Transitivität: Folgt aus Teil 1 (Linearität der Verkettung).

3. Für beliebige $x, y \in \ker h$ und $\alpha, \beta \in \mathbb{K}$ gilt:

   $$\begin{aligned} h(x) = h(y) = 0 \quad &\Rightarrow \quad h(\alpha x + \beta y) = \alpha h(x) + \beta h(y) = \alpha 0 + \beta 0 = 0 \\ &\Rightarrow \quad \alpha x + \beta y \in \ker h. \end{aligned}$$

   Damit ist $\ker h$ ein Unterraum von V.

   Sind $x, y \in \operatorname{im} h$ beliebig, etwa $x = h(u)$, $y = h(v)$ für bestimmte $u, v \in V$, und sind $\alpha, \beta \in \mathbb{K}$ beliebig, so gilt

   $$\alpha x + \beta y = \alpha h(u) + \beta h(v) = h(\alpha u + \beta v),$$

   also $\alpha x + \beta y \in \operatorname{im} h$. Damit ist $\operatorname{im} h$ ein Unterraum von W. ∎

Beispiel. $V = \mathbb{K}^m$, $W = \mathbb{K}^n$, $h\colon V \to W$, $h(x) = Ax$ für eine bestimmte Matrix $A \in \mathbb{K}^{n\times m}$. Eine Basis für $\ker h = \ker A$ kann man berechnen wie in Abschnitt 9 erklärt.

Ein Erzeugendensystem für $\operatorname{im} h$ ist $\{\, h(b) : b \in B \,\}$, wenn B eine Basis von V ist. Wie man daraus eine Basis gewinnt, haben wir im Beispiel 5 nach Definition 32 gesehen.

Satz 49. Seien V, W zwei $\mathbb{K}$-Vektorräume, $h\colon V \to W$ ein Homomorphismus. Dann gilt: h ist genau dann injektiv, wenn $\ker h = \{0\}$ ist.

Beweis. „⇒“ Sei $x \in \ker h$. Dann gilt $h(x) = 0$. Es gilt aber auch $h(0) = 0$. Da h injektiv ist, folgt $x = 0$.

„⇐“ Seien $x, y \in V$ mit $h(x) = h(y)$. Dann gilt $h(x) - h(y) = 0$, also $h(x - y) = 0$, also $x - y \in \ker h$, also $x - y = 0$, also $x = y$. ∎

Satz 50. Seien V, W zwei $\mathbb{K}$-Vektorräume, B eine Basis von V, und $f\colon B \to W$ eine beliebige Funktion. Dann existiert genau eine lineare Abbildung $h\colon V \to W$ mit $h(b) = f(b)$ für alle $b \in B$.

Beweis. (a) Existenz: Jedes $x \in V$ lässt sich schreiben als $x = \alpha_1 b_1 + \cdots + \alpha_k b_k$ für gewisse $\alpha_1, \ldots, \alpha_k \in \mathbb{K}$ und $b_1, \ldots, b_k \in B$. Definiere $h(x) := \alpha_1 f(b_1) + \cdots + \alpha_k f(b_k)$. Da die Darstellung von x als Linearkombination von Basiselementen eindeutig ist, ist h wohldefiniert. Man überzeugt sich leicht, dass h linear ist und dass $h(b) = f(b)$ für alle $b \in B$ gilt.
(b) Eindeutigkeit: Für jedes $x \in V$ mit $x = \alpha_1 b_1 + \cdots + \alpha_k b_k$ muss gelten

$$\begin{aligned} h(x) &= h(\alpha_1 b_1 + \cdots + \alpha_k b_k) \\ &= \alpha_1 h(b_1) + \cdots + \alpha_k h(b_k) \\ &= \alpha_1 f(b_1) + \cdots + \alpha_k f(b_k). \end{aligned}$$

Eine andere Wahl von h ist also nicht möglich. ∎

Beispiel.

1. $V = \mathbb{Q}^4$, $B = \{e_1, \ldots, e_4\}$, $W = \mathbb{Q}^3$. Betrachte die Funktion $f\colon B \to W$ definiert durch

   $$\begin{aligned} e_1 &\mapsto (1,2,3), \quad & e_2 &\mapsto (4,5,6) \\ e_3 &\mapsto (7,8,9), \quad & e_4 &\mapsto (10,11,12). \end{aligned}$$

   Dann ist $h\colon V \to W$ die Abbildung, die $(x_1, x_2, x_3, x_4) \in V$ auf

   $$x_1 \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + x_2 \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} + x_3 \begin{pmatrix} 7 \\ 8 \\ 9 \end{pmatrix} + x_4 \begin{pmatrix} 10 \\ 11 \\ 12 \end{pmatrix}$$

   abbildet. Mit anderen Worten:

   $$h(x) = \begin{pmatrix} 1 & 4 & 7 & 10 \\ 2 & 5 & 8 & 11 \\ 3 & 6 & 9 & 12 \end{pmatrix} x.$$

2. Seien U, W zwei $\mathbb{K}$-Vektorräume, $B_U, \bar{B}_U$ und $B_W, \bar{B}_W$ je zwei Basen von U bzw. W.

   Die lineare Abbildung $h\colon \mathbf{F}_{\mathbb{K}}(B_U \times B_W) \to \mathbf{F}_{\mathbb{K}}(\bar{B}_U \times \bar{B}_W)$ sei dadurch definiert, dass jeder Basistensor $b_U \otimes b_W$ mit $b_U \in B_U, b_W \in B_W$ auf den entsprechenden Tensor $b_U \otimes b_W \in \mathbf{F}_{\mathbb{K}}(\bar{B}_U \times \bar{B}_W)$ abgebildet wird.

   Ferner sei die lineare Abbildung $\bar{h}\colon \mathbf{F}_{\mathbb{K}}(\bar{B}_U \times \bar{B}_W) \to \mathbf{F}_{\mathbb{K}}(B_U \times B_W)$ dadurch definiert, dass jeder Basistensor $\bar{b}_U \otimes \bar{b}_W$ mit $\bar{b}_U \in \bar{B}_U, \bar{b}_W \in \bar{B}_W$ auf den entsprechenden Tensor $\bar{b}_U \otimes \bar{b}_W \in \mathbf{F}_{\mathbb{K}}(B_U \times B_W)$ abgebildet wird.

   Man kann nachrechnen, dass $h \circ \bar{h}$ die Identität ist, d.h. h und $\bar{h}$ sind bijektiv, d.h. $\mathbf{F}_{\mathbb{K}}(B_U \times B_W) \cong \mathbf{F}_{\mathbb{K}}(\bar{B}_U \times \bar{B}_W)$. Für alle $u \in U$ und $w \in W$ gilt $h(u \otimes w) = u \otimes w$. In diesem Sinn ist die Definition von $U \otimes W$ unabhängig von der Wahl der Basen von U und W.

Satz 51. Seien V, W zwei endlich-dimensionale $\mathbb{K}$-Vektorräume, $h\colon V \to W$ ein Homomorphismus. Dann gilt: $\dim V = \dim \ker h + \dim \operatorname{im} h$.

Beweis. Sei $\{b_1, \ldots, b_n\}$ eine Basis von $\ker h$. Nach Satz 43 gibt es $b_{n+1}, \ldots, b_m \in V$, so dass $\{b_1, \ldots, b_m\}$ eine Basis von V ist. Wir zeigen, dass $B = \{h(b_{n+1}), \ldots, h(b_m)\}$ eine Basis von $\operatorname{im} h$ ist. Daraus folgt die Behauptung.

(a) B ist linear unabhängig: Seien $\alpha_{n+1}, \ldots, \alpha_m \in \mathbb{K}$ so, dass $\alpha_{n+1}h(b_{n+1}) + \cdots + \alpha_m h(b_m) = 0$. Dann ist $h(\alpha_{n+1}b_{n+1} + \cdots + \alpha_m b_m) = 0$, also $\alpha_{n+1}b_{n+1} + \cdots + \alpha_m b_m \in \ker h$. Dann aber gibt es $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ so dass

$$\alpha_1 b_1 + \cdots + \alpha_n b_n = \alpha_{n+1}b_{n+1} + \cdots + \alpha_m b_m.$$

Da $\{b_1, \ldots, b_m\}$ als Basis von V linear unabhängig ist, folgt, dass alle α_i Null sind, insbesondere $\alpha_{n+1}, \ldots, \alpha_m$.

(b) B ist Erzeugendensystem: Sei $y \in \operatorname{im} h$. Dann gibt es ein $x \in V$ mit $y = h(x)$. Dann gibt es $\alpha_1, \ldots, \alpha_m \in \mathbb{K}$ mit $x = \alpha_1 b_1 + \cdots + \alpha_m b_m$. Und dann gilt

$$h(x) = \underbrace{\alpha_1 h(b_1) + \cdots + \alpha_n h(b_n)}_{= 0, \text{ da } \{b_1, \ldots, b_n\} \text{ Basis von } \ker h} + \alpha_{n+1}h(b_{n+1}) + \cdots + \alpha_m h(b_m).$$

■

Mit Satz 51 und einigen früheren Resultaten können wir einiges über die vier Räume aussagen, die einer Matrix zugeordnet sind.

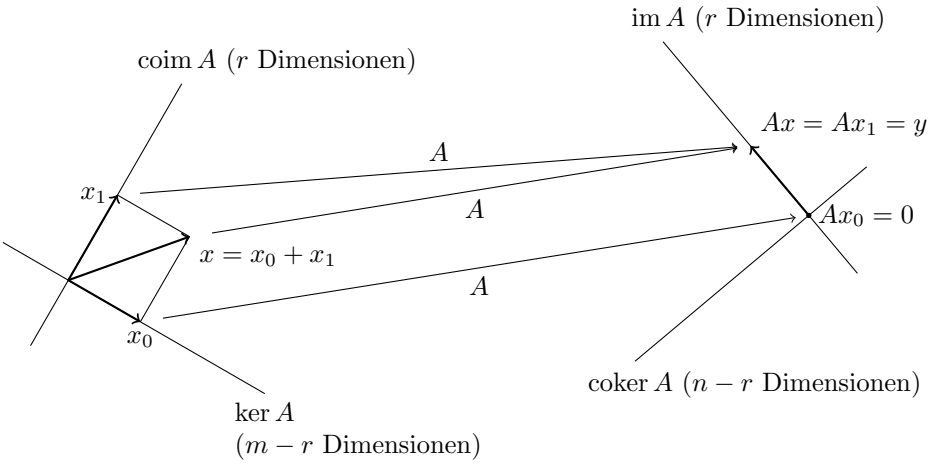
Sei $A \in \mathbb{K}^{n\times m}$ eine Matrix, $r = \operatorname{Rang} A$. Zunächst gilt für die Dimensionen:

- Zeilenraum: $\dim \operatorname{coim} A = r$ (wegen Satz 23)
- Spaltenraum: $\dim \operatorname{im} A = r$ (wegen $\dim \operatorname{coim} A = r$ und Satz 24)
- Kern: $\dim \ker A = m - r$ (wegen $\dim \operatorname{im} A = r$ und Satz 51)
- Co-Kern: $\dim \operatorname{coker} A = n - r$ (wegen $\dim \operatorname{coim} A = r$ und den Sätzen 51 und 24).

Als nächstes gilt $\mathbb{K}^m = \ker A + \operatorname{coim} A$. Das sieht man ein, wenn man sich erinnert, wie man eine Basis von $\ker A$ aus der Treppennormalform bestimmt (vgl. Seite 56). Anhand der Lage der Treppenstufen erkennt man, dass die Zeilen von A die Basis des Lösungsraums zu einer Basis des gesamten Raums $\mathbb{K}^m$ ergänzen. Die Summe ist sogar direkt, wie mit Satz 44 leicht überprüft: $\ker A$ und $\operatorname{coim} A$ sind Unterräume von $\mathbb{K}^m$ und es gilt $m = \dim \mathbb{K}^m = \dim \ker A + \dim \operatorname{coim} A - \dim(\ker A \cap \operatorname{coim} A) = m - r + r - \dim(\ker A \cap \operatorname{coim} A)$, also $\dim(\ker A \cap \operatorname{coim} A) = 0$, also $\ker A \cap \operatorname{coim} A = \{0\}$.

Analog gilt $\mathbb{K}^n = \operatorname{im} A \oplus \operatorname{coker} A$, indem man dasselbe Argument auf $A^\top$ anwendet.

Die Zusammenhänge sind in der folgenden Zeichnung schematisch dargestellt. Man sieht links, dass jedes $x \in \mathbb{K}^m$ sich in einen $\operatorname{coim} A$-Anteil und einen $\ker A$-Anteil zerlegen lässt. Die Matrix A bildet x nach $\operatorname{im} A$ ab. Der $\ker A$-Anteil von x landet bei 0, und das Bild $y = Ax$ von x ist identisch mit dem Bild des $\operatorname{coim} A$-Anteils von x. Es gibt keine Vektoren, die auf $\operatorname{coker} A \setminus \{0\}$ abgebildet werden.



Als Anwendung können wir nun den noch ausstehenden Korrektheitsbeweis von Algorithmus 5 auf Seite 60 zu Ende bringen. Wir hatten dort eine Matrix $B \in \mathbb{K}^{k\times m}$ und eine Basis $\{a_1, \ldots, a_n\} \subseteq \mathbb{K}^m$ von $\ker B$, d. h.

$$\{\, x \in \mathbb{K}^m : Bx = 0 \,\} = \{\, \alpha_1 a_1 + \cdots + \alpha_n a_n : \alpha_1, \ldots, \alpha_n \in \mathbb{K} \,\}.$$

Die Behauptung war, dass dann auch gilt

$$\{\, x \in \mathbb{K}^m : Ax = 0 \,\} = \{\, \alpha_1 b_1 + \cdots + \alpha_k b_k : \alpha_1, \ldots, \alpha_k \in \mathbb{K} \,\},$$

wobei $b_1, \ldots, b_k$ die Zeilenvektoren von B sind und $A = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$. Die Richtung „$\supseteq$“ ist bereits gezeigt worden. Die rechte Seite ist also ein Unterraum des Vektorraums auf der linken Seite.

Die linke Seite ist $\ker A$, die rechte ist $\operatorname{coim} B$. Da $\{a_1, \ldots, a_n\}$ eine Basis und damit linear unabhängig ist, gilt $\operatorname{Rang} A = n$ und daher $\dim \ker A = m - n$. Außerdem folgt $\dim \ker B = n$ und daher $\dim \operatorname{coim} B = m - n$. Damit sind $\ker A$ und $\operatorname{coim} B$ zwei Unterräume von $\mathbb{K}^m$ derselben Dimension. Wegen $\ker A \supseteq \operatorname{coim} B$ folgt aus Satz 42, dass $\ker A = \operatorname{coim} B$ gilt, was zu zeigen war.

Satz 52. Seien V, W zwei endlich-dimensionale $\mathbb{K}$-Vektorräume mit $\dim V = \dim W$, und sei $h\colon V \to W$ ein Homomorphismus. Dann gilt:

$$h \text{ ist injektiv} \iff h \text{ ist surjektiv} \iff h \text{ ist bijektiv.}$$

Beweis. Die zweite Äquivalenz folgt unmittelbar aus der ersten. Wir zeigen die erste.

„$\Rightarrow$“ h ist injektiv. Dann ist $\ker h = \{0\}$ nach Satz 49. Mit Satz 51 folgt dann $\dim V = 0 + \dim \operatorname{im} h$, und wegen $\dim V = \dim W$ also $\dim W = \dim \operatorname{im} h$. Nach Satz 42 folgt $\operatorname{im} h = W$, d.h. h ist surjektiv.

„$\Leftarrow$“ h ist surjektiv. Dann ist $\operatorname{im} h = W$, also $\dim \operatorname{im} h = \dim W$, also $\dim \ker h = \dim V - \dim W = 0$ nach Satz 51 und Voraussetzung $\dim V = \dim W$. Also gilt $\ker h = \{0\}$. Wegen Satz 49 folgt, dass h injektiv ist. ∎

Satz 53. Seien V, W zwei endlich-dimensionale $\mathbb{K}$-Vektorräume. Dann gilt:

1. $\dim V \leq \dim W \iff$ es gibt einen injektiven Homomorphismus $h\colon V \to W$.
2. $\dim V \geq \dim W \iff$ es gibt einen surjektiven Homomorphismus $h\colon V \to W$.
3. $\dim V = \dim W \iff$ es gibt einen bijektiven Homomorphismus $h\colon V \to W$.

Beweis. Wir zeigen den dritten Teil. Der Beweis für die ersten beiden Teile geht ähnlich.
„⇒“ Sei $A = \{a_1, \dots, a_n\}$ eine Basis von V und $B = \{b_1, \dots, b_n\}$ eine Basis von W. Nach Satz 50 existiert eine lineare Abbildung $h\colon V \to W$ mit $h(a_i) = b_i$ für $i = 1, \dots, n$. Diese lineare Abbildung ist injektiv, denn

$$\begin{aligned} 0 &= h(\alpha_1 a_1 + \cdots + \alpha_n a_n) \\ &= \alpha_1 h(a_1) + \cdots + \alpha_n h(a_n) \\ &= \alpha_1 b_1 + \cdots + \alpha_n b_n \\ \Rightarrow \qquad \alpha_1 &= \cdots = \alpha_n = 0, \end{aligned}$$

also $\ker h = \{0\}$.
h ist auch surjektiv, denn ist $y \in W$ beliebig, so ist $y = \beta_1 b_1 + \cdots + \beta_n b_n$ für gewisse $\beta_1, \dots, \beta_n \in W$, also

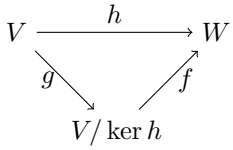
$$y = \beta_1 h(a_1) + \cdots + \beta_n h(a_n) = h(\beta_1 a_1 + \cdots + \beta_n a_n) \in \operatorname{im} h.$$

„⇐“ Ist $h\colon V \to W$ bijektiv und $A = \{a_1, \dots, a_n\}$ eine Basis von V, so ist

$$B = \{h(a_1), \dots, h(a_n)\}$$

eine Basis von W: die lineare Unabhängigkeit folgt aus der Injektivität von h, und dass B ein Erzeugendensystem ist, folgt aus der Surjektivität. ∎

Satz 54. (Homomorphiesatz für Vektorräume) Seien V, W zwei $\mathbb{K}$-Vektorräume, $h\colon V \to W$ ein Homomorphismus. Dann gibt es eine surjektive lineare Abbildung $g\colon V \to V/\ker h$ und eine injektive lineare Abbildung $f\colon V/\ker h \to W$ mit $h = f \circ g$.
Wenn h surjektiv ist, dann auch f. Insbesondere gilt $V/\ker h \cong \operatorname{im} h$.



Beweis. Da Vektorräume insbesondere auch abelsche Gruppen sind, und lineare Abbildungen insbesondere auch Gruppenhomomorphismen, haben wir die meisten Aussagen des Satzes bereits in Satz 10 bewiesen. Es bleibt hier nur noch zu zeigen, dass die dort angegebenen Funktionen

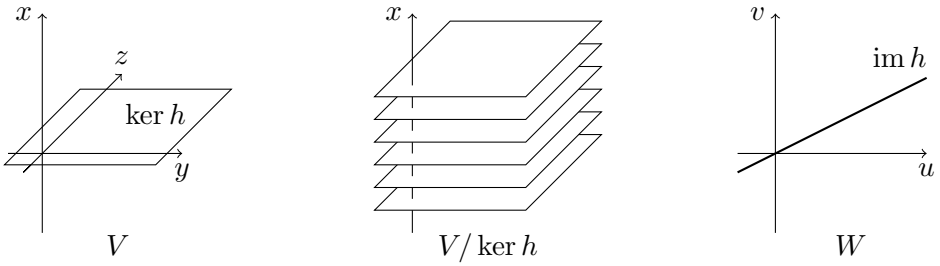
$$\begin{aligned} g\colon V \to V/\ker h, &\qquad g(x) = [x]_\sim \\ f\colon V/\ker h \to W, &\quad f([x]_\sim) = h(x) \end{aligned}$$

auch mit der Skalarmultiplikation verträglich sind. Und in der Tat gilt

$$\begin{aligned} g(\alpha x) = [\alpha x]_\sim = \alpha [x]_\sim = \alpha\, g(x) \\ f(\alpha [x]_\sim) = f([\alpha x]_\sim) = h(\alpha x) = \alpha\, h(x). \end{aligned}$$

∎

Beispiel. $V = \mathbb{R}^3$, $W = \mathbb{R}^2$, $h\colon V \to W$, $h(x,y,z) = (2x, x)$. Dann gilt $\ker h = \langle \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix} \rangle$ und $\operatorname{im} h = \langle \begin{pmatrix}2\\1\end{pmatrix} \rangle$. Geometrisch ist $\ker h$ die (y,z)-Ebene in $\mathbb{R}^3$ und $\operatorname{im} h$ eine Gerade in $\mathbb{R}^2$. Die Elemente von $V/\ker h$ kann man sich vorstellen als die Ebenen, die parallel zu $\ker h$ liegen. Diese bilden einen Vektorraum, der genau wie $\operatorname{im} h$ eindimensional ist. Jedes Ebene in $V/\ker h$ ist eindeutig charakterisiert durch ihren Schnittpunkt mit der x-Achse. Einen Isomorphismus zwischen $V/\ker h$ und $\operatorname{im} h$ erhält man, indem man die Ebene durch $(x,0,0)$ auf $(2x,x)$ abbildet. Beachte, dass zwei Punkte $(x,y,z) \in \mathbb{R}^3$ genau dann dasselbe Bild $h(x,y,z) \in \mathbb{R}^2$ haben, wenn sie zur selben Ebene gehören (vgl. die Beispiele zu Satz 6).



Satz 55. (Isomorphiesätze)

1. Seien U, W zwei Unterräume eines $\mathbb{K}$-Vektorraums V. Dann gilt
$$U/(U \cap W) \cong (U + W)/W.$$
2. Im Fall $U \subseteq W$ gilt außerdem $(V/U)/(W/U) \cong V/W$.

Beweis.

1. Nach Satz 43 gibt es einen Raum $\tilde{W} \subseteq U$ mit $(U \cap W) \oplus \tilde{W} = U$. Wähle so einen Raum $\tilde{W}$. Dann lässt sich jedes $u \in U$ schreiben als $u = u_1 + u_2$ für gewisse eindeutig bestimmte $u_1 \in U \cap W$ und $u_2 \in \tilde{W}$. Betrachte die Abbildung
$$h\colon U \to (U + W)/W, \quad h(u_1 + u_2) = [u_2]_\sim.$$
Diese Funktion ist linear und surjektiv und es gilt $\ker h = U \cap W$. Aus Satz 54 folgt deshalb die Behauptung.

$$\begin{array}{ccc} U & \xrightarrow{\ h\ } & (U+W)/W \\ & \searrow \quad \nearrow & \\ & U/(U \cap W) & \end{array}$$

2. Sei $\tilde{U} \subseteq W$ so, dass $U \oplus \tilde{U} = W$, und sei $\tilde{W} \subseteq V$ so, dass $W \oplus \tilde{W} = V$. Dann ist $V/U \cong \tilde{U} + \tilde{W}$ und $W/U \cong \tilde{U}$, und unter Verwendung von Teil 1 ist
$$(V/U)/(W/U) \cong (\tilde{U} + \tilde{W})/\tilde{U} \cong \tilde{W}/\underbrace{(\tilde{U} \cap \tilde{W})}_{=\{0\}} \cong \tilde{W} \cong V/W.$$

∎

17 Koordinatendarstellungen

Definition 35. Sei V ein endlich-dimensionaler $\mathbb{K}$-Vektorraum.

1. Ein Vektor $B = (b_1, \ldots, b_n) \in V^n$ heißt *geordnete Basis* von V, falls $\{b_1, \ldots, b_n\}$ eine Basis von V ist.

2. Sei $B = (b_1, \ldots, b_n) \in V^n$ eine geordnete Basis von V und $x \in V$. Sind $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ so, dass $x = \alpha_1 b_1 + \cdots + \alpha_n b_k$, dann heißt der Vektor $(\alpha_1, \ldots, \alpha_n) \in \mathbb{K}^n$ die *Koordinatendarstellung* von x bezüglich B. Für $i = 1, \ldots, n$ heißt dann α_i die i-te *Koordinate* von x bezüglich B.

Eine geordnete Basis ist nichts anderes als eine Basis, bei der eine bestimmte Reihenfolge für die Basiselemente festgelegt ist. Man beachte, dass $\{a, b, c\} = \{c, a, b\}$ aber $(a, b, c) \neq (c, a, b)$ ist.

Beim Teil 2 der Definition ist zu beachten, dass es zu jedem $x \in V$ genau eine passende Koordinatendarstellung $(\alpha_1, \ldots, \alpha_n)$ gibt, weil $\{b_1, \ldots, b_n\}$ nach Voraussetzung eine Basis ist.

Beispiel.

1. Vektoren $x = (x_1, \ldots, x_n) \in \mathbb{K}^n$ sind Koordinatendarstellungen von sich selbst bezüglich der Standardbasis $E = (e_1, \ldots, e_n)$.

2. Ist $B = (b_1, b_2, b_3, b_4)$ eine geordnete Basis eines Vektorraums V, so ist $\tilde{B} = (b_3, b_1, b_4, b_2)$ auch eine geordnete Basis von V, und zwar eine von B verschiedene. Ist (x_1, x_2, x_3, x_4) die Koordinatendarstellung eines bestimmten Vektors bezüglich B, so ist (x_3, x_1, x_4, x_2) die Koordinatendarstellung desselben Vektors bezüglich $\tilde{B}$.

3. $B = (1, X, X^2, X^3) \in K[X]^4$ ist eine geordnete Basis für den Unterraum von $K[X]$ bestehend aus allen Polynomen vom Grad höchstes drei. Eine andere geordnete Basis ist $\tilde{B} = (1, X, X(X-1), X(X-1)(X-2))$. Die Koordinatendarstellung von $2 + 3X - 7X^2 + 5X^3$ bezüglich B ist $(2, 3, -7, 5)$. Die Koordinatendarstellung desselben Polynoms bezüglich $\tilde{B}$ ist $(2, 1, 8, 5)$.

4. Im Fall $V = \mathbb{K}^n$ lässt sich eine geordnete Basis als Matrix auffassen. Per Konvention macht man die Basisvektoren zu den Spalten der Matrix. Dann ist zum Beispiel

$$B = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \end{pmatrix}$$

eine geordnete Basis von $\mathbb{Q}^3$. Ist $\begin{pmatrix} 3 \\ 2 \\ 4 \end{pmatrix}$ die Koordinatendarstellung eines Vektors bezüglich dieser Basis B, so erhält man die Koordinatendarstellung desselben Vektors bezüglich der Standardbasis durch die Rechnung

$$3 \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + 2 \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + 4 \begin{pmatrix} 1 \\ 4 \\ 9 \end{pmatrix} = \begin{pmatrix} 9 \\ 23 \\ 45 \end{pmatrix}.$$

Ist umgekehrt $\begin{pmatrix}7\\4\\3\end{pmatrix}$ die Koordiantendarstellung eines Vektors bezüglich der Standardbasis, so bekommt man dessen Darstellung bezüglich der Basis B, indem man das lineare Gleichungssystem

$$\alpha_1 \begin{pmatrix}1\\1\\1\end{pmatrix} + \alpha_2 \begin{pmatrix}1\\2\\3\end{pmatrix} + \alpha_3 \begin{pmatrix}1\\4\\9\end{pmatrix} = \begin{pmatrix}7\\4\\3\end{pmatrix}$$

löst. Das Ergebnis lautet $\begin{pmatrix}12\\-6\\1\end{pmatrix}$.

Bei einem gegebenen Tupel von Körperelementen ist also nicht ohne weiteres klar, welcher Vektor damit beschrieben wird. Man muss immer auch die Basis wissen, bezüglich der die Koordinaten zu verstehen sind. Ist keine Basis angegeben, wird meistens die Standardbasis gemeint sein.

Satz 56. Sei V ein endlich-dimensionaler $\mathbb{K}$-Vektorraum, $B = (b_1, \dots, b_n) \in V^n$ eine geordnete Basis von V. Dann ist die Abbildung $h\colon V \to \mathbb{K}^n$, die jedem $x \in V$ dessen Koordinatendarstellung bezüglich B zuordnet, ein Isomorphismus.

Insbesondere sind alle endlich-dimensionalen $\mathbb{K}$-Vektorräume der gleichen Dimension zueinander isomorph.

Beweis. Übung. ∎

Im vorangegangenen Beispiel haben wir gesehen, wie man zwischen einer Koordinatendarstellung eines Vektors $v \in \mathbb{K}^n$ bezüglich der Standardbasis und der Koordinatendarstellung bezüglich einer anderen geordneten Basis hin und her wechseln kann: ist $v \in \mathbb{K}^n$ ein Vektor (und damit die Koordinatendarstellung von sich selbst bezüglich der Standardbasis), so ist Bv die Koordinatendarstellung desselben Vektors bezüglich B. Und ist $w \in \mathbb{K}^n$ die Koordinatendarstellung eines Vektors bezüglich B, so ist $B^{-1}w$ die Koordinatendarstellung desselben Vektors bezüglich der Standardbasis. (Matrizen, die geordnete Basen enthalten, sind immer invertierbar, weil ihre Spalten linear unabhängig sind.) Die folgende Definition verallgemeinert diesen Sachverhalt.

Definition 36. Seien V, W zwei endlich-dimensionale $\mathbb{K}$-Vektorräume, $A = (a_1, \dots, a_m) \in V^m$ eine geordnete Basis von V, $B = (b_1, \dots, b_n) \in W^n$ eine geordnete Basis von W. Weiter sei $h\colon V \to W$ eine lineare Abbildung. Die Matrix $M \in \mathbb{K}^{n\times m}$, deren (i,j)-ter Eintrag die i-te Koordinate von $h(a_j)$ bezüglich B ist, heißt die *Abbildungsmatrix* oder die *Koordinatendarstellung* von h bezüglich A und B.

Beispiel.

1. Sei $M \in \mathbb{K}^{n\times m}$, $V = \mathbb{K}^m$, $W = \mathbb{K}^n$ und sei $h\colon V \to W$, $h(x) = Mx$. Dann ist M die Abbildungsmatrix von h bezüglich der Standardbasis $\{e_1, \dots, e_m\}$ von V und der Standardbasis $\{e_1, \dots, e_n\}$ von W.

2. Sei $V = \mathbb{Q}[X]_{\le 3} = \{\, a_0 + a_1X + a_2X^2 + a_3X^3 : a_0, a_1, a_2, a_3 \in \mathbb{Q} \,\}$, und sei $W = \mathbb{Q}(\sqrt{2})$. Weiter sei

$$h\colon V \to W, \quad h(a_0 + a_1X + \cdots + a_3X^3) := a_0 + a_1(1+\sqrt{2}) + \cdots + a_3(1+\sqrt{2})^3.$$

Dann ist h eine lineare Abbildung. $A = \{1, X, X^2, X^3\}$ ist eine Basis von V und $B = \{1, \sqrt{2}\}$ ist eine Basis von W. Die Abbildungsmatrix von h bezüglich A und B lautet

$$M = \begin{pmatrix} 1 & 1 & 3 & 7 \\ 0 & 1 & 2 & 5 \end{pmatrix}.$$

Zum Beispiel erklärt sich die letzte Spalte aus $(1 + \sqrt{2})^3 = 7 + 5\sqrt{2}$.

3. $V = W$, $h = \mathrm{id}$, aber zwei nicht notwendigerweise identische Basen $B_1, B_2 \in V^n$. In diesem Fall hat die Abbildungsmatrix M von h bezüglich B_1 und B_2 die Eigenschaft, dass sie Koordinatendarstellungen von $v \in V$ bezüglich B_1 in Koordinatendarstellungen bezüglich B_2 umwandelt. Man nennt M deshalb auch eine *Basiswechselmatrix* und schreibt $T_{B_1 \to B_2} := M$.

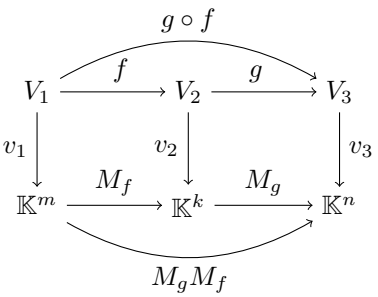
   Im Fall $V = \mathbb{K}^n$, wo sich B_1 und B_2 als invertierbare Matrizen auffassen lassen, und wo die Standardbasis $(e_1, \ldots, e_n)$ der Einheitsmatrix I_n entspricht, gilt $T_{I_n \to B_2} = B_2$, $T_{B_1 \to I_n} = B_1^{-1}$, $T_{B_1 \to B_2} = B_2 B_1^{-1}$, $T_{B_2 \to B_1} = B_1 B_2^{-1} = T_{B_1 \to B_2}^{-1}$. Außerdem gilt: ist B_3 eine dritte geordnete Basis von V, so ist $T_{B_1 \to B_3} = T_{B_2 \to B_3} T_{B_1 \to B_2}$.

Satz 57. Seien V, W zwei endlich-dimensionale $\mathbb{K}$-Vektorräume, $h\colon V \to W$ linear und $M \in \mathbb{K}^{n \times m}$ die Abbildungsmatrix von h bezüglich geordneter Basen A, B von V, W. Weiter seien $v\colon V \to \mathbb{K}^m$ und $w\colon W \to \mathbb{K}^n$ die Abbildungen, die jedem $x \in V$ bzw. jedem $y \in W$ die Koordinatendarstellungen dieser Vektoren bezüglich A bzw. B zuordnen. Dann gilt $w(h(x)) = Mv(x)$ für alle $x \in V$.

$$\begin{array}{ccc} V & \xrightarrow{h} & W \\ {\scriptstyle v}\downarrow & & \downarrow{\scriptstyle w} \\ \mathbb{K}^m & \xrightarrow{M} & \mathbb{K}^n \end{array}$$

Beweis. Da alle beteiligten Abbildungen linear sind, genügt es, die Aussage für die Elemente der Basis von V zu zeigen. Ist a_j das j-te Basiselement, so ist $v(b_j) = e_j$ und also $Mv(b_j)$ die j-te Spalte von M. Nach Definition 36 ist das genau die Koordinatendarstellung von $h(b_j)$ bezüglich der gewählten Basis von W, also $w(h(b_j))$. ∎

Satz 58. Seien V_1, V_2, V_3 drei endlich-dimensionale $\mathbb{K}$-Vektorräume mit geordneten Basen B_1, B_2, B_3, seien $f\colon V_1 \to V_2$, $g\colon V_2 \to V_3$ lineare Abbildungen, und seien M_f, M_g die Abbildungsmatrix von f bezüglich B_1 und B_2 bzw. von g bezüglich B_2 und B_3. Dann ist $M_g M_f$ die Abbildungsmatrix von $g \circ f\colon V_1 \to V_3$ bezüglich B_1 und B_3.



Beweis. Nach Satz 57 gilt $v_2(f(x)) = M_f v_1(x)$ für alle $x \in V_1$, d. h. $f(x) = v_2^{-1}(M_f v_1(x))$. Außerdem gilt $v_3(g(y)) = M_g v_2(y)$ für alle $y \in V_2$, und damit auch

$$v_3(g(f(x))) = M_g v_2(f(x)) = M_g M_f v_1(x)$$

für alle $x \in V_1$. Da diese Gleichung dann insbesondere für die Basisvektoren von V_1 gilt, folgt die Behauptung. ∎

Aus dem Satz folgt, dass man eine Abbildungsmatrix M bezüglich zweier geordneter Basen B_1, B_2 in eine Abbildungsmatrix $\tilde{M}$ derselben Abbildung aber bezüglich zweier anderer geordneter Basen $\tilde{B}_1, \tilde{B}_2$ dadurch überführt, dass man sie mit den entsprechenden Basiswechselmatrizen multipliziert:

$$\tilde{M} = T_{B_2 \to \tilde{B}_2} M T_{\tilde{B}_1 \to B_1}.$$

Noch spezieller: Wenn $V_1 = V_2$, $B_1 = B_2$ und $\tilde{B}_1 = \tilde{B}_2$ ist, dann ist $T_{B_2 \to \tilde{B}_2} = T^{-1}_{\tilde{B}_1 \to B_1}$, d. h. die Basistransformation hat dann die einfache Form $\tilde{M} = T^{-1} M T$ für ein gewisses $T \in \mathrm{GL}(n, \mathbb{K})$. Es gilt dann

$$\begin{aligned} \det(\tilde{M}) &= \det(T^{-1} M T) \\ &= \det(T^{-1}) \det(M) \det(T) \\ &= \frac{1}{\det(T)} \det(M) \det(T) \\ &= \det(M). \end{aligned}$$

Das heißt, alle Abbildungsmatrizen einer linearen Abbildung $h\colon V \to V$ mit der gleichen Basis auf beiden Seite haben dieselbe Determinante. Der Wert der Determinante hängt also nur von der linearen Abbildung h ab und nicht von der gewählten Basis für V. Ähnliches gilt für den Rang einer Matrix. Das gestattet die folgenden Definitionen:

Definition 37.

1. Sei $h\colon V \to V$ linear, B eine beliebige geordnete Basis von V und $M \in \mathbb{K}^{n \times n}$ die Abbildungsmatrix von V bezüglich B und B. Dann heißt $\det h := \det M$ die *Determinante* von h.

2. Sei $h\colon V \to W$ linear, A, B beliebige geordnete Basen von V, W, und sei $M \in \mathbb{K}^{n \times m}$ die Abbildungsmatrix von h bezüglich A und B. Dann heißt $\operatorname{Rang} h := \operatorname{Rang} M$ der *Rang* von h.

18 Der Dualraum

Definition 38.

1. Sind V und W zwei $\mathbb{K}$-Vektorräume, so wird die Menge aller linearen Abbildungen $h\colon V \to W$ mit $\mathrm{Hom}(V, W)$ bezeichnet.

2. Im Spezialfall $V = W$ schreibt man $\mathrm{End}(V) := \mathrm{Hom}(V, V)$. Für die Menge aller Automorphismen schreibt man $\mathrm{Aut}(V)$.

3. Im Spezialfall $W = \mathbb{K}$ schreibt man $V^* := \mathrm{Hom}(V, W)$ und nennt dies den *Dualraum* von V. Die Elemente von V^* heißen *Funktionale.*

Beachte: $\mathrm{Hom}(V,W)$ bildet zusammen mit den Operationen

$$\underset{\text{in } \mathrm{Hom}(V,W)}{h_1 + h_2} := \big(\underset{\in V}{x} \mapsto \underset{\text{in } W}{h_1(x) + h_2(x)} \big), \qquad \underset{\text{in } \mathrm{Hom}(V,W)}{\alpha \cdot h} := \big(\underset{\in V}{x} \mapsto \underset{\text{in } W}{\alpha \cdot h(x)} \big)$$

einen Vektorraum über $\mathbb{K}$.
Auch $\mathrm{End}(V)$ ist ein Vektorraum.
Die Menge $\mathrm{Aut}(V)$ ist *kein* Vektorraum, aber zusammen mit der Komposition eine Gruppe.

Beispiel.

1. $V = \mathbb{R}^3$, $h\colon \mathbb{R}^3 \to \mathbb{R}$, $h(\begin{pmatrix} x \\ y \\ z \end{pmatrix}) = x + y - z$. Dann ist $h \in V^*$.
2. $V = \mathbb{Q}[X]$, $e\colon \mathbb{Q}[X] \to \mathbb{Q}$ definiert durch
$$e(a_0 + a_1 X + \cdots + a_n X^n) := a_0 + 3a_1 + 9a_2 + \cdots + 3^n a_n.$$
Dann ist $e \in V^*$.
3. Einige weitere Beispiele für lineare Abbildungen $V \to \mathbb{K}$ befinden sich in der Liste nach Definition 34.

Satz 59. Sind V, W zwei endlich-dimensionale $\mathbb{K}$-Vektorräume, $\dim V = n$, $\dim W = m$, dann ist
$$\mathrm{Hom}(V,W) \cong \mathbb{K}^{n \times m}.$$
Insbesondere gilt $\dim \mathrm{Hom}(V,W) = nm$ und $V^* \cong \mathbb{K}^{1\times m} \cong \mathbb{K}^m \cong V$ und $\dim V^* = \dim V$.

Beweis. Wir konstruieren einen Isomorphismus $h\colon \mathbb{K}^{n\times m} \to \mathrm{Hom}(V,W)$. Wähle dazu geordnete Basen $A = (a_1, \ldots, a_m)$ von V und $B = (b_1, \ldots, b_n)$ von W. Es sei $h_{i,j}\colon V \to W$ die nach Satz 50 eindeutig bestimmte lineare Abbildung mit $h(a_j) = b_i$ und $h(a_k) = 0$ für alle $k \neq j$.
Es bezeichne $e_{i,j} \in \mathbb{K}^{n\times m}$ die Matrix, die an Stelle (i,j) eine Eins und ansonsten nur Nullen enthält. Dann ist $\{ e_{i,j} : i = 1, \ldots, n, j = 1, \ldots, m \}$ eine Basis von $\mathbb{K}^{n\times m}$.
Es sei schließlich $h\colon \mathbb{K}^{n\times m} \to \mathrm{Hom}(V,W)$ die nach Satz 50 eindeutig bestimmte lineare Abbildung, die $e_{i,j}$ auf $h_{i,j}$ abbildet, für $i = 1, \ldots, m$ und $j = 1, \ldots, n$.
Diese Abbildung ist bijektiv: Die Umkehrabbildung $h^{-1}\colon \mathrm{Hom}(V,W) \to \mathbb{K}^{n\times m}$ ist die Funktion, die jedem $u \in \mathrm{Hom}(V,W)$ dessen Abbildungsmatrix bezüglich A und B zuordnet. ∎

Für $V = \mathbb{K}^m$ folgt aus dem Satz, dass jedes Element von V^* von der Form ist

$$x^*\colon V \to \mathbb{K}, \quad x^*(\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}) = \alpha_1 x_1 + \cdots + \alpha_m x_m = (\alpha_1, \ldots, \alpha_m) \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}$$

für gewisse Konstanten $\alpha_1, \ldots, \alpha_m \in \mathbb{K}$. Die („abstrakten“) Vektoren $x^* \in V^*$ lassen sich also auch durch („konkrete“) Vektoren $(\alpha_1, \ldots, \alpha_m) \in \mathbb{K}^m = V$ beschreiben. Die Abbildung

$$V \to V^*, \quad \underbrace{(\alpha_1, \ldots, \alpha_m)}_{\in V} \mapsto \underbrace{\big(\underset{\in V}{x} \mapsto (\alpha_1, \ldots, \alpha_m) x \big)}_{\in V^*}$$

ist ein Isomorphismus.
Im Fall $\dim V = \infty$ sind V und V^* nicht unbedingt isomorph. Zum Beispiel kann man zeigen, dass $\mathbb{K}[[X]]^* \cong \mathbb{K}[X] \ncong \mathbb{K}[[X]]$.

Satz 60. Ist $B = \{b_1, \dots, b_m\}$ eine Basis von V, so bildet die Menge $B^* = \{b_1^*, \dots, b_m^*\} \subseteq V^*$ mit

$$b_i^*(b_j) = \begin{cases} 1 & \text{falls } i = j \\ 0 & \text{sonst} \end{cases}$$

eine Basis von V^*. (Man nennt B^* die zu B *duale* Basis.)

Beweis. (a) B^* ist linear unabhängig: Seien $\alpha_1, \dots, \alpha_n \in \mathbb{K}$ mit

$$\alpha_1 b_1^* + \cdots + \alpha_n b_n^* = 0.$$

Das bedeutet $\alpha_1 b_1^*(x) + \cdots + \alpha_n b_n^*(x) = 0$ für alle $x \in V$. Für beliebiges $i \in \{1, \dots, n\}$ gilt daher insbesondere

$$0 = (\alpha_1 b_1^* + \cdots + \alpha_n b_n^*)(b_i) = \alpha_1 b_1^*(b_i) + \cdots + \alpha_n b_n^*(b_i) = \alpha_i.$$

(b) B^* ist ein Erzeugendensystem: Sei $x^* \in V$ beliebig. Sei $\alpha_i := x^*(b_i)$ für $i = 1, \dots, n$. Für die lineare Abbildung $y^* := \alpha_1 b_1^* + \cdots + \alpha_n b_n^*$ gilt ebenfalls $\alpha_i = y^*(b_i)$ für $i = 1, \dots, n$. Da nach Satz 50 eine lineare Abbildung eindeutig durch die Bilder auf den Basiselementen bestimmt ist, folgt $x^* = y^*$. Und da x^* beliebig war und y^* eine Linearkombination von $b_1^*, \dots, b_n^*$ ist, folgt, dass B^* ein Erzeugendensystem von V^* ist. ∎

Definition 39. Seien V, W zwei $\mathbb{K}$-Vektorräume, $h \in \mathrm{Hom}(V, W)$. Dann wird die Abbildung $h^\top \in \mathrm{Hom}(W^*, V^*)$ definiert durch $h^\top(y^*) := (\ x \mapsto y^*(h(x))\ )$ für alle $y^* \in W^*$.

Beispiel. $V = \mathbb{R}^2$, $W = \mathbb{R}^3$, $h(x) = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} x$. Dann ist $h^\top \colon W^* \to V^*$ die Abbildung, die eine Abbildung

$$y^* \colon W \to \mathbb{K}, \quad y^*\left(\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}\right) = (\beta_1, \beta_2, \beta_3) \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$$

in die Abbildung

$$\begin{aligned} h^\top(y^*) \colon V \to \mathbb{K}, \quad h^\top(y^*)\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) &= (\beta_1, \beta_2, \beta_3) \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \\ &= (\beta_1 + 3\beta_2 + 5\beta_3)x_1 + (2\beta_1 + 4\beta_2 + 6\beta_3)x_2 \end{aligned}$$

überführt.
Einfacher lässt es sich ausdrücken, wenn man die Elemente der Dualräume durch die entsprechenden Vektoren in V bzw W ausdrückt. Dann ist nämlich einfach

$$h^\top\left(\begin{pmatrix} \beta_1 \\ \beta_2 \\ \beta_3 \end{pmatrix}\right) = \begin{pmatrix} 1 & 3 & 5 \\ 2 & 4 & 6 \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_2 \\ \beta_3 \end{pmatrix}.$$

Wie man sieht, ist die Abbildungsmatrix von $h^\top$ gerade die Transponierte der Abbildungsmatrix von h. Das ist natürlich kein Zufall:

Satz 61. Seien V, W zwei $\mathbb{K}$-Vektorräume.

1. Die Abbildung $\cdot^\top \colon \operatorname{Hom}(V,W) \to \operatorname{Hom}(W^*, V^*)$, $h \mapsto h^\top$ ist linear.
2. Seien V, W beide endlich-dimensional und seien A, B geordnete Basen von V bzw. W. Weiter seien A^* und B^* die dualen Basen von A und B. Dann gilt: Ist $M \in \mathbb{K}^{n\times m}$ die Abbildungsmatrix von $h \in \operatorname{Hom}(V,W)$ bezüglich A und B, so ist $M^\top \in \mathbb{K}^{m\times n}$ die Abbildungsmatrix von $h^\top$ bezüglich B^* und A^*.

Beweis.

1. Übung.
2. Sei $\tilde{M}$ die Abbildungsmatrix von $h^\top$ bezüglich B^* und A^*. Schreibe $A = \{a_1, \dots, a_m\}$, $B = \{b_1, \dots, b_n\}$, $A^* = \{a_1^*, \dots, a_m^*\}$, $B^* = \{b_1^*, \dots, b_n^*\}$.

   An Position (i,j) von $\tilde{M}$ steht die i-te Koordinate von $h^\top(b_j^*)$ bezüglich A^*. Zu zeigen: diese ist identisch mit der j-ten Koordinate von $h(a_i)$ bezüglich B.

   Aufgrund der Definiton der Dualbasis ist die i-te Koordinate eines Funktionals $x^* \in V^*$ gerade $x^*(a_i)$, und $b_j^*(y)$ ist die j-te Koordinate von $y \in W$. Daher:

$$\begin{aligned}
&i\text{-te Koordiante von } h^\top(b_j^*) \text{ bezüglich } A^* \\
&= h^\top(b_j^*)(a_i) \\
&= b_j^*(h(a_i)) \\
&= j\text{-te Koordinate von } h(a_i) \text{ bezüglich } B,
\end{aligned}$$

   wie behauptet. ∎

Der Satz ist eine Verallgemeinerung der Matrixtransposition auf Homomorphismen zwischen beliebigen Vektorräumen. Es bietet sich deshalb an dieser an, auch die Begriffe Ko-Kern und Ko-Bild für beliebige Homomorphismen zu definieren. Für $h \colon V \to W$ war ja bereits definiert $\ker h = \{x \in V : h(x) = 0\}$ und $\operatorname{im} h = \{h(x) : x \in V\}$. Darüber hinaus definieren wir jetzt $\operatorname{coker} h = \{x \in W^* : h^\top(x) = 0\}$ und $\operatorname{coim} h = \{h^\top(x) : x \in W^*\}$. Man beachte, dass $\operatorname{coker} h$ ein Unterraum von W^* und $\operatorname{coim} h$ ein Unterraum von V^* ist.

Satz 62. Sei V ein $\mathbb{K}$-Vektorraum und $V^{**} := (V^*)^*$ der Dualraum des Dualraums von V (V^{**} ist der sogenannte *Bidualraum* von V). Die Abbildung

$$h \colon V \to V^{**}, \quad h(x) = (\ f \mapsto f(x)\ )$$

ist linear und injektiv, und im Fall $\dim V < \infty$ auch bijektiv.

Beweis. Linearität: Für alle $\alpha, \beta \in \mathbb{K}$ und alle $x, y \in V$ gilt:

$$\begin{aligned}
h(\alpha x + \beta y) &= (\ f \mapsto f(\alpha x + \beta y)\ ) \\
&= (\ f \mapsto \alpha f(x) + \beta f(y)\ ) \\
&= \alpha(\ f \mapsto f(x)\ ) + \beta(\ f \mapsto f(y)\ ) \\
&= \alpha h(x) + \beta h(y).
\end{aligned}$$

Injektivität: Für alle $x, y \in V$ gilt

$$\begin{aligned} h(x) = h(y) \quad &\Rightarrow \quad h(x-y) = 0 \\ &\Rightarrow \quad (\ f \mapsto f(x-y)\ ) = 0 \\ &\Rightarrow \quad \forall\ f \in V^* : f(x-y) = 0 \\ &\Rightarrow \quad x = y. \end{aligned}$$

Bijektivität im Fall $\dim V < \infty$ folgt aus Satz 52 und $\dim V^{**} = \dim V^* = \dim V$. ∎

Teil IV

Anwendungen

19 Affine und Projektive Geometrie

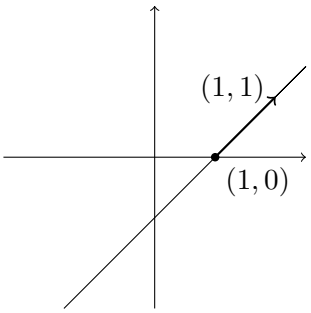
Definition 40. Sei $U \subseteq \mathbb{K}^n$ ein Untervektorraum und $x \in \mathbb{K}^n$. Dann heißt

$$x + U := \{\, x + u : u \in U \,\} \subseteq \mathbb{K}^n$$

ein *affiner Unterraum* (engl. *affine subspace*) von $\mathbb{K}^n$.
Im Fall $\dim U = 0$ / 1 / 2 / $n-1$ spricht man von einem *Punkt* / einer *Geraden* / einer *Ebene* / einer *Hyperebene*. (engl: *point*, *line*, *plane*, *hyper plane*)

Beispiel.

1. $G = \{ \begin{pmatrix}1\\0\end{pmatrix} + \lambda \begin{pmatrix}1\\1\end{pmatrix} : \lambda \in \mathbb{R} \} = \begin{pmatrix}1\\0\end{pmatrix} + \langle \begin{pmatrix}1\\1\end{pmatrix} \rangle \subseteq \mathbb{R}^2$ ist die Gerade durch den Punkt $\begin{pmatrix}1\\0\end{pmatrix}$ in Richtung $\begin{pmatrix}1\\1\end{pmatrix}$.



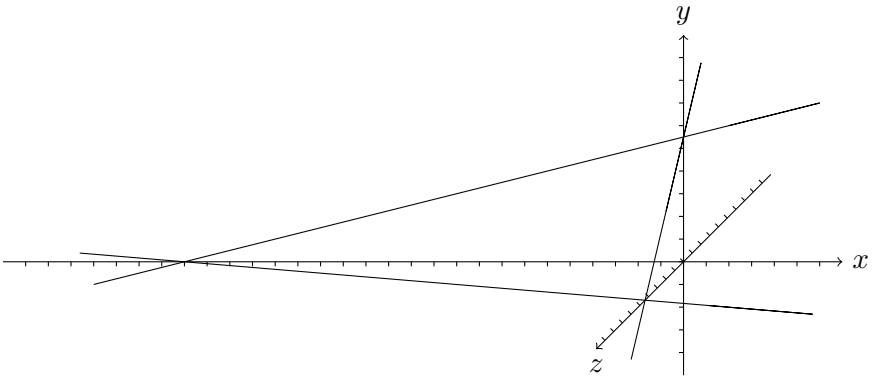
   $G' = \begin{pmatrix}0\\-1\end{pmatrix} + \langle \begin{pmatrix}-1\\-1\end{pmatrix} \rangle \subseteq \mathbb{R}^2$ ist eine andere Schreibeweise für dieselbe Gerade.

2. $E = \begin{pmatrix}1\\2\\3\end{pmatrix} + \langle \begin{pmatrix}1\\-1\\1\end{pmatrix}, \begin{pmatrix}1\\4\\-3\end{pmatrix} \rangle$ ist eine Ebene. Um sich die Lage der Ebene im dreidimensionalen Raum zu veranschaulichen, kann man die Schnittgeraden mit den drei Koordinatenebenen bestimmen:

$$E \cap \underbrace{\langle \begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix} \rangle}_{(x,y)\text{-Ebene}} = \begin{pmatrix}2\\6\\0\end{pmatrix} + \langle \begin{pmatrix}4\\1\\0\end{pmatrix} \rangle$$

$$E \cap \underbrace{\langle \begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix} \rangle}_{(x,z)\text{-Ebene}} = \begin{pmatrix}3\\0\\5\end{pmatrix} + \langle \begin{pmatrix}5\\0\\1\end{pmatrix} \rangle$$

$$E \cap \underbrace{\langle \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix} \rangle}_{(y,z)\text{-Ebene}} = \begin{pmatrix}0\\3\\2\end{pmatrix} + \langle \begin{pmatrix}0\\5\\-4\end{pmatrix} \rangle.$$



Den Schnitt zweier affiner Unterräume kann man berechnen, indem man ein inhomogenes lineares Gleichungssystem löst. Zum Beispiel bekommt man die erste Schnittgerade, indem man alle $\alpha, \beta, \lambda, \mu$ bestimmt, für die gilt:

$$\begin{pmatrix}1\\2\\3\end{pmatrix} + \alpha \begin{pmatrix}1\\-1\\1\end{pmatrix} + \beta \begin{pmatrix}1\\4\\-3\end{pmatrix} = \lambda \begin{pmatrix}1\\0\\0\end{pmatrix} + \mu \begin{pmatrix}0\\1\\0\end{pmatrix}.$$

Die Schnittgerade mit einer Koordinatenebene kann man auch einfacher ausrechnen. Dazu nutzt man aus, dass z. B. die (x, y)-Ebene gerade die Menge aller Punkte $(x, y, z) \in \mathbb{R}^3$ mit der Eigenschaft $z = 0$ ist. Der Schnitt dieser Ebene mit E ist also auch die Menge aller Punkte aus E, deren letzte Koordinate 0 ist. Um diese Punkte zu finden, braucht man nur das inhomogene Gleichungssystem

$$3 + \alpha \cdot 1 + \beta \cdot (-3) = 0$$

zu lösen.

Satz 63. Der Schnitt zweier affiner Unterräume von $\mathbb{K}^n$ ist entweder die leere Menge oder wieder ein affiner Unterraum von $\mathbb{K}^n$.

Beweis. Seien $x_1 + U_1$ und $x_2 + U_2$ zwei affine Unterräume von $\mathbb{K}^n$. Falls deren Schnitt leer ist, ist nichts zu zeigen. Anderenfalls gibt es ein $x \in \mathbb{K}^n$ mit $x \in (x_1 + U_1) \cap (x_2 + U_2)$, etwa $x = x_1 + u_1 = x_2 + u_2$ für gewisse $u_1 \in U_1$ und $u_2 \in U_2$. Wir zeigen, dass dann $(x_1 + U_1) \cap (x_2 + U_2) = x + (U_1 \cap U_2)$ gilt.

„$\subseteq$“ Sei $z \in (x_1 + U_1) \cap (x_2 + U_2)$. Zu zeigen: $z \in x + (U_1 \cap U_2)$, d. h. $x - z \in U_1 \cap U_2$. Nach Voraussetzung gilt $z \in x_1 + U_1$ und $z \in x_2 + U_2$, also $z = x_1 + \tilde{u}_1 = x_2 + \tilde{u}_2$ für gewisse $\tilde{u}_1 \in U_1$ und $\tilde{u}_2 \in U_2$. Also gilt

$$z - x = \begin{cases} u_1 - \tilde{u}_1 \in U_1 \\ u_2 - \tilde{u}_2 \in U_2 \end{cases}$$

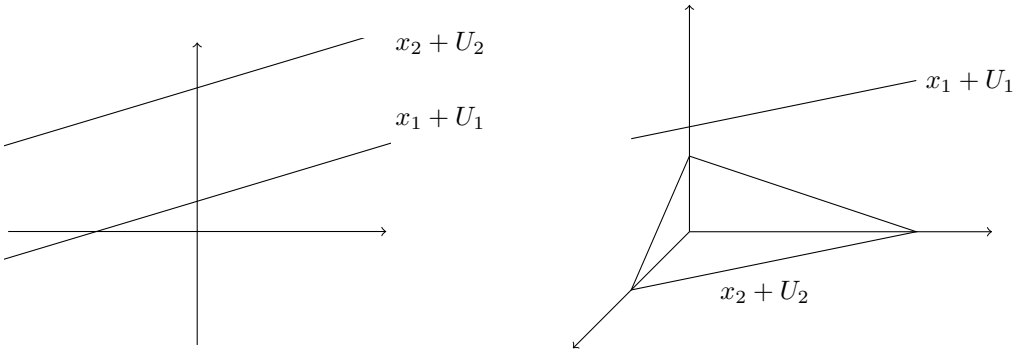
und damit $z - x \in U_1 \cap U_2$.

„$\supseteq$“ Sei $z \in x + (U_1 \cap U_2)$. Zu zeigen: $z \in x_1 + U_1$ und $z \in x_2 + U_2$. Aus Symmetriegründen genügt es, $z \in x_1 + U_1$ zu zeigen. Nach Voraussetzung gilt

$$z \in \underset{\substack{\uparrow \\ = x_1 + u_1}}{x} + \underbrace{(U_1 \cap U_2)}_{\subseteq U_1} \subseteq x_1 + \underbrace{u_1 + U_1}_{= U_1}.$$

■

Definition 41. Zwei affine Unterräume x_1+U_1, x_2+U_2 von $\mathbb{K}^n$ heißen (zueinander) *parallel,* falls $U_1 \subseteq U_2$ oder $U_2 \subseteq U_1$ ist.



Zwei Geraden im Raum $\mathbb{K}^2$, die sich nicht schneiden, sind stets zueinander parallel. (Beweis: Übung.) Zwei Geraden im Raum $\mathbb{K}^3$ können sich jedoch auch dann verfehlen, wenn sie nicht parallel sind.

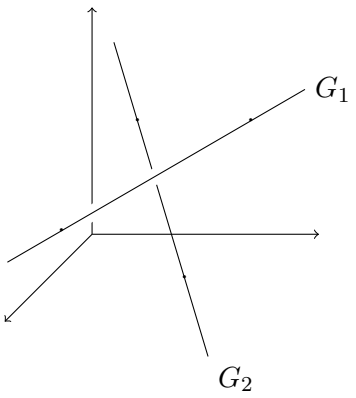
Beispiel. Betrachte die beiden Geraden

$$G_1 = \begin{pmatrix}1\\2\\3\end{pmatrix} + \langle \begin{pmatrix}2\\1\\-1\end{pmatrix} \rangle, \qquad G_2 = \begin{pmatrix}2\\5\\0\end{pmatrix} + \langle \begin{pmatrix}4\\-5\\5\end{pmatrix} \rangle.$$

Der Schnitt $G_1 \cap G_2$ ist leer, weil das inhomogene Gleichungssystem

$$\begin{pmatrix}1\\2\\3\end{pmatrix} + \alpha \begin{pmatrix}2\\1\\-1\end{pmatrix} = \begin{pmatrix}2\\5\\0\end{pmatrix} + \beta \begin{pmatrix}4\\-5\\5\end{pmatrix}$$

keine Lösung hat. Trotzdem sind diese Geraden nicht parallel, weil $\begin{pmatrix}2\\1\\-1\end{pmatrix}$ und $\begin{pmatrix}4\\-5\\5\end{pmatrix}$ linear unabhängig sind.



Zwei Ebenen im $\mathbb{K}^3$ sind entweder zueinander parallel oder sie schneiden sich in einer Gerade. Zwei Ebenen im $\mathbb{K}^4$ können als Schnittmenge eine Gerade, einen einzelnen Punkt, oder die leere Menge haben, und zwar auch dann, wenn sie nicht parallel sind.

Beispiel. Für die beiden Ebenen

$$E_1 = \begin{pmatrix}1\\2\\3\\4\end{pmatrix} + \langle \begin{pmatrix}1\\-1\\1\\-1\end{pmatrix}, \begin{pmatrix}0\\1\\-1\\0\end{pmatrix} \rangle, \qquad E_2 = \begin{pmatrix}1\\2\\-2\\1\end{pmatrix} + \langle \begin{pmatrix}4\\3\\2\\1\end{pmatrix}, \begin{pmatrix}1\\2\\4\\8\end{pmatrix} \rangle$$

gilt

$$E_1 \cap E_2 = \{ \begin{pmatrix}5\\5\\0\\0\end{pmatrix} \}.$$

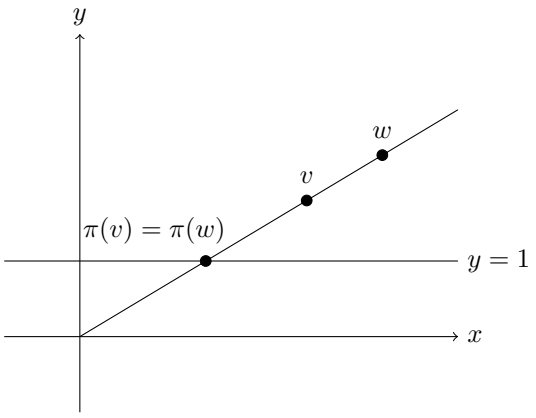
Definition 42. Für $v, w \in \mathbb{K}^{n+1} \setminus \{0\}$ sei definiert

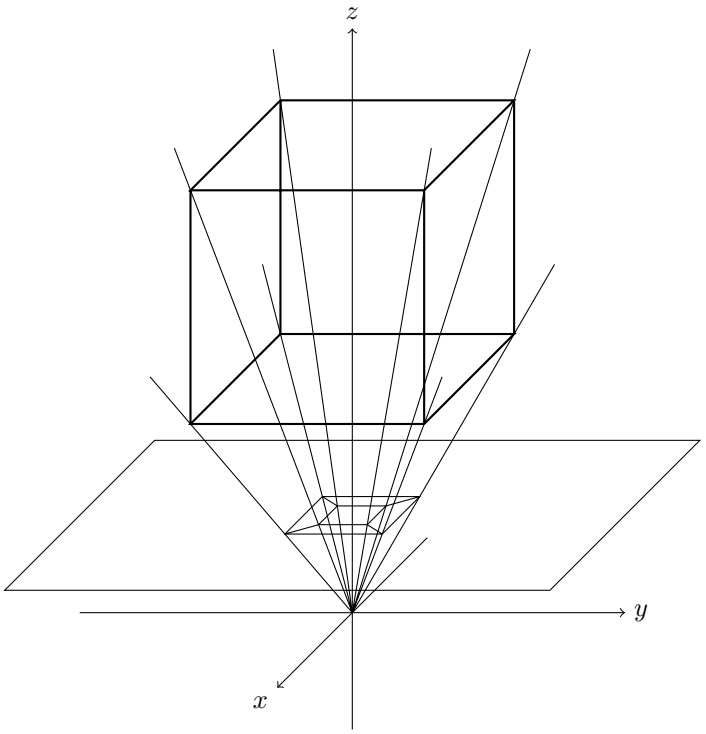
$$v \sim w \quad :\Longleftrightarrow \quad \exists\, \lambda \in \mathbb{K} \setminus \{0\} : v = \lambda w.$$

Dann heißt $\mathbb{P}^n := (\mathbb{K}^{n+1} \setminus \{0\})/\sim$ der *projektive Raum* der Dimension n über $\mathbb{K}$.

Statt $[(x_0, \ldots, x_n)]_\sim$ schreibt man $(x_0 : \cdots : x_n)$ und spricht von *projektiven Koordinaten.*

Anschauung: Das Auge eines Betrachters am Ursprung $(0, \ldots, 0)$ des Raums $\mathbb{K}^{n+1}$ kann zwei Punkte $v, w \in \mathbb{K}^{n+1}$ nicht voneinander unterscheiden, wenn $v \sim w$ gilt, d. h. wenn diese Punkte auf derselben Geraden durch den Ursprung liegen. Mit Ausnahme der Geraden auf der Grundfäche $x_{n+1} = 0$ schneiden alle diese Geraden den affinen Unterraum $\mathbb{K}^n \times \{1\} \subseteq \mathbb{K}^{n+1}$ in genau einem Punkt. Dieser Punkt bietet sich als kanonischer Repräsentant der jeweiligen Äquivalenzklassen an. Man kann sich den affinen Unterraum $\mathbb{K}^n \times \{1\}$ geometrisch als Projektionsfläche vorstellen. Betrachtet man ein geometrisches Objekt im $\mathbb{K}^{n+1}$ als ein Objekt in $\mathbb{P}^n$, so geht ein Teil der Information über Lage und Form des Objekts verloren. Was an Information übrig bleibt, entspricht genau dem Bild der Projektion auf der Projektionsfläche.





Die Projektion bildet den Punkt $(x_0 : \cdots : x_n) \in \mathbb{P}^n$ mit $x_n \neq 0$ auf den Punkt $(\frac{x_0}{x_n}, \ldots, \frac{x_{n-1}}{x_n}) \in \mathbb{K}^n$ ab. Die restlichen Punkte $(x_0 : \cdots : x_{n-1} : 0) \in \mathbb{P}^n$ bilden zusammengenommen eine Kopie von $\mathbb{P}^{n-1}$. Diese Punkte kann man sich anschaulich als Punkte vorstellen, die „unendlich weit“ vom Ursprung entfernt liegen. Im Fall $n = 1$ entsprechen die Punkte $(x_0 : x_1)$ mit $x_1 = 0$ genau den Punkten auf der x_0-Achse, die die zu ihr parallel verlaufende Projektionsgerade $x_0 = 1$ in einem gedachten unendlich fernen Punkt $(1 : 0) \in \mathbb{P}^1$ schneidet. Es gilt also „$\mathbb{P}^1 \cong \mathbb{K}^1 \cup \mathbb{P}^0$“. Im Fall $n = 2$ verlaufen die Grundebene $\{\, (x_0, x_1, x_2) : x_2 = 0 \,\}$ und die Projektionsebene $\{\, (x_0, x_1, x_2) : x_2 = 1 \,\}$ zueinander parallel. Sie schneiden sich in einer gedachten Gerade, die aus lauter unendlich fernen Punkten besteht, je einen für jede Richtung $(x_0 : x_1)$. Es gilt also „$\mathbb{P}^2 \cong \mathbb{K}^2 \cup \mathbb{P}^1$“.

Durch die Hinzunahme von unendlich fernen Punkte lassen sich die lästigen Fallunterscheidungen, die beim Rechnen mit affinen Räumen auftreten, vermeiden. Statt der inhomogenen Gleichungssysteme

$$x + \alpha_1 v_1 + \cdots + \alpha_m v_m = 0,$$

die da auftreten, hat man es im projektiven Raum nur mit homogenen Gleichungsystemen

$$\lambda x + \alpha_1 v_1 + \cdots + \alpha_m v_m = 0$$

zu tun.

In der Computergraphik wird grundsätzlich mit projektiven Koordinaten gearbeitet. Objekte in einem dreidimensionalen virtuellen Raum werden dargestellt durch Punkte im projektiven Raum $\mathbb{P}^3$. Positionsänderungen der Objekte lassen sich durch die Anwendung geeigneter 4×4-Matrizen ausdrücken. Für eine Matrix $A \in \mathbb{K}^{(n+1)\times(n+1)}$ und einen Punkt $[x]_\sim \in \mathbb{P}^n$ mit $x \in \mathbb{K}^{n+1} \setminus \{0\}$ definiert man $A[x]_\sim := [Ax]_\sim$. Eine solche Definition ist zulässig, weil das Ergebnis wegen $x' = Ax \iff \forall\, \lambda \neq 0 : \lambda x' = A(\lambda x)$ nicht von der Wahl des Repräsentanten abhängt.

So kann man zum Beispiel im projektiven Raum auch die Verschiebung eines Punktes $(x_0 : x_1 : x_2 :$

$x_3) \in \mathbb{P}^3$ um den Vektor $(y_0, y_1, y_2) \in \mathbb{K}^3$ als eine lineare Abbildung schreiben:

$$\begin{pmatrix} x'_0 \\ x'_1 \\ x'_2 \\ x'_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & y_1 \\ 0 & 1 & 0 & y_2 \\ 0 & 0 & 1 & y_3 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix}.$$

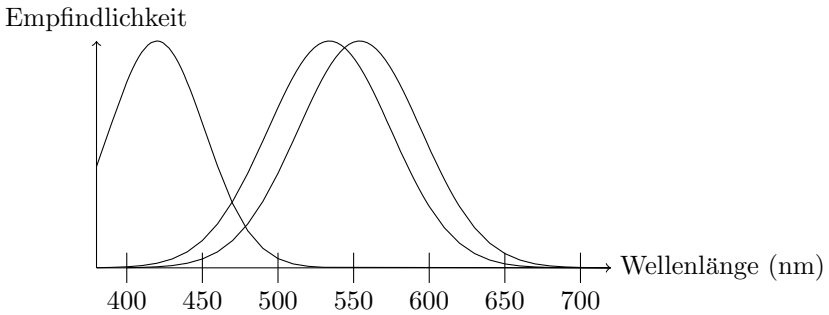
Im Raum $\mathbb{K}^3$ ist die Verschiebung um (y_1, y_2, y_3) dagegen keine lineare Abbildung.

Zur Darstellung der dreidimensionalen virtuellen Realiät auf einem zweidimensionalen Bildschirm betrachtet man die Bildschirmoberfläche als projektiven Raum $\mathbb{P}^2$ und verwendet eine Matrix $A \in \mathbb{K}^{3\times 4}$, um die Punkte in $\mathbb{P}^3$ auf Punkte im $\mathbb{P}^2$ abzubilden. Die Einträge von A codieren Lage, Blickrichtung, Drehwinkel und Brennweite (Zoom) der virtuellen Kamera. Wie das genau funktioniert, erfahren Sie in den einschlägigen Lehrveranstaltungen des Instituts für Angewandte Geometrie von Prof. Jüttler.

20 Farbräume

Das Spektrum des sichtbaren Lichts umfasst die elektromagnetische Strahlung mit Wellenlängen von ca. 400nm (violett) bis ca. 700nm (rot). Jede Wellenlänge entspricht einer bestimmten (Spektral-)Farbe, und jeder andere Farbeindruck einspricht einer bestimmten Überlagerung solcher Spektralfarben. Weisses Licht ergibt sich zum Beispiel aus der gleichmäßigen Mischung von Licht in allen Farben des Spektrums. In der Sprache der linearen Algebra kann man die Farben als einen Vektorraum auffassen, der von den Spektralfarben erzeugt wird. Jede Wellenlänge entspricht dann einem anderen Basisvektor, und jede Farbe ist eine Linearkombination, deren Koeffizienten angeben, wie stark der Lichtanteil der entsprechenden Spektralfarbe ist.

Wenn jede Wellenlänge einem Basisvektor entsprechen soll, dann ist der Farbraum offenbar unendlich dimensional. Das mag aus physikalischer Sicht auch eine adäquate Beschreibung der Natur des Lichts sein, aber für praktische Anwendungen sind so viele Dimensionen weder nützlich noch nötig. Das menschliche Auge kann so viele Farben gar nicht unterscheiden. Auf der Netzhaut des Auges gibt es vier verschiedene Arten von lichtempfindliche Zellen, von denen drei für das farbige Sehen zuständig sind. Jede dieser drei Zellarten reagiert auf Licht mit einer bestimmten Wellenlänge λ besonders stark, und auf Licht mit anderen Wellenlängen umso schwächer, je stärker die andere Wellenlänge von λ abweicht.



Der Farbeindruck, den wir subjektiv wahrnehmen, ergibt sich daraus, wie stark die drei verschiedenen Zelltypen vom eintreffenden Licht angeregt werden. Das Auge codiert also jede Farbe als einen Vektor (x, y, z), in dem die Koordinaten angeben, wie stark jeder der drei Zelltypen von der Farbe angeregt wird. Vereinfachend kann man sich vorstellen, dass die Koordinaten zwischen 0 (gar keine Anregung) und 1 (maximale Anregung) liegen.

Die Basis in diesem Modell bilden die drei „Grundfarben“ rot, grün und blau, für die jeweils einer der drei Zelltypen auf der Netzhaut maximal angeregt wird. Das Mischen von Farben entspricht der

Linearkombination von Vektoren. Wenn man dabei nichtnegative Koeffizienten wählt, die sich zu (höchstens) 1 aufaddieren, dann ist gewährleistet, dass der Ergebnisvektor wieder Koordinaten hat, die zwischen 0 und 1 liegen und damit einen gültigen Farbvektor darstellen. Solche Linearkombinationen $\alpha_1 a_1 + \cdots + \alpha_m a_m$ mit $\alpha_1, \ldots, \alpha_m \geq 0$ und $\alpha_1 + \cdots + \alpha_m = 1$ nennt man auch *Konvexkombinationen.*
Beispiele:

$(0,0,0) =$ ■, $(1,0,0) =$ ■, $(0,1,0) =$ ■, $(0,0,1) =$ ■,
$(0,1,1) =$ ■, $(1,0,1) =$ ■, $(1,1,0) =$ ■, $(1,1,1) =$ ■,
$(\frac{1}{3}, 1, \frac{2}{3}) =$ ■, $(\frac{1}{2}, 0, 0) =$ ■, $(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}) =$ ■, $(0, \frac{1}{4}, 1) =$ ■.

Ausgabegeräte wie zum Beispiel Monitore erzeugen Farben, indem sie rotes, grünes und blaues Licht in genau dem Mischungsverhältnis ausstrahlen, das im Auge des Betrachters den gewünschten Farbeindruck hervorruft.

Ein Bild kann man als eine Funktion auffassen, die jedem Punkt der Ebene eine Farbe zuordnet. Farbige Bilder werden im Computer als Überlagerung dreier einfarbiger Bilder dargestellt, die den Anteil der drei Basisfarben am Gesamtbild angeben. Typischerweise verwendet man dabei rot, grün und blau (RGB) als Basisfarben:

Abhängig von der Anwendungssituation kann es von Vorteil sein, verschiedene Basen zu verwenden. Es kann zum Beispiel sein, dass es für die drei Basislichtquellen in einem Monitor technisch leichter ist, statt R, G und B drei andere Farben A, B und C zu verwenden. Die Farbinformation, die der Computer in der RGB-Basis an den Monitor leitet, muss dann vom Monitor in die ABC-Basis umgewandelt werden. Die Basistransformation geschieht natürlich durch Multiplikation des RGB-Vektors mit der 3×3-Matrix, deren Zeilen die Koordinatendarstellung der Farben in der RGB-Basis sind.

Personen, die an Rot-Grün-Blindheit leiden, haben auf ihrer Netzhaut nur zwei verschiedene Typen von farbempfindlichen Zellen. Für diese Personen ist der Farbraum deshalb nur zweidimensional, und es ergibt sich in etwa der folgende Eindruck:

Wenn Betroffene jetzt einwenden, dass für sie die Abbildung auf der linken Seite der Gleichung nicht identisch aussieht wie die Abbildung auf der linken Seite der dreidimensionalen Zerlegung, dann liegt

das daran, dass die Wellenlängen, bei denen die Farbrezeptoren im Auge maximal angeregt werden, von Mensch zu Mensch leicht verschieden sind. Den exakt gleichen Eindruck bekommt man nur dann, wenn man in der Rechnung ein rot und ein blau verwendet, die gemeisam den gleichen Untervektorraum aufspannen wie das rot und das blau, die die Zellen im Auge der betreffenden Person wahrnehmen. Darüber hinaus müsste sichergestellt sein, dass das verwendete Grafikprogram sowie der Drucker bzw. der Bildschirm exakt die gleichen Farbtöne als Basisfunktion verwenden, was technisch nur sehr schwer umzusetzen ist.

Wenn Sie dieses Skriptum auf einem Schwarz-Weiss-Drucker ausgedruckt haben, dann hat Ihr Computer die Farben in den Abbildungen dieses Abschnitts in Grautöne umwandeln müssen. Ein Grauton ist eine reelle Zahl zwischen 0 (schwarz) und 1 (weiss). Um ein Farbbild in ein Graustufenbild umzuwandeln, wählt man Grauwerte $g_R, g_G, g_B \in [0,1]$, auf die die Basisfarben R, G, B abgebildet werden sollen. Eine beliebige Farbe (c_R, c_G, c_B) des RGB-Raums wird dann abgebildet auf den Grauwert

$$(g_R, g_G, g_B) \begin{pmatrix} c_R \\ c_G \\ c_B \end{pmatrix}.$$

Die Abbildung, die jeder RGB-Farbe einen Grauwert zuordnet, ist also ein Funktional.

Umgekehrt: Vögel werden die Bilder, die auf unseren Monitoren angezeigt werden, vermutlich nicht besonders realistisch finden. Sie verfügen nämlich über eine Netzhaut mit vier verschiedenen Typen von Farbrezeptoren und genießen daher einen vierdimensionalen Farbraum. Sie können deshalb viele Farben voneinander unterscheiden, die für uns identisch sind.

21 Graphentheorie

Definition 43. Sei V eine Menge und E eine Relation auf V. Dann heißt das Paar $G = (V, E)$ ein *Graph*. Die Elemente von V heißen *Knoten* (engl. *vertex*) und die Elemente von E heißen *Kanten* (engl. *edge*) des Graphen. Eine Kante der Form (v, v) heißt *Schleife* (engl. *loop*).

Ein Graph in diesem Sinne hat nichts mit Funktionsgraphen zu tun. Es handelt sich viel mehr um eine Art Netzwerk, wie wir bereits im Abschnitt 2 als Beispiel für eine Relation gesehen haben. Graphen kann man sich graphisch veranschaulichen, indem man für die Knoten irgendwelche Punkte in der Ebene wählt und je zwei Punkte $v_1, v_2 \in V$ genau dann durch einen Pfeil von v_1 nach v_2 verbindet, wenn $(v_1, v_2) \in E$ ist.

Um einen Graph im Computer zu speichern, kann man einfach eine Liste mit den Elementen von V sowie eine Liste mit den Elementen von E speichern. Für manche Anwendungen ist es zweckmäßiger, die Kantenmenge E durch eine Matrix darzustellen, deren Einträge für je zwei Knoten v_1, v_2 angeben, ob es eine Kante von v_1 nach v_2 gibt oder nicht.

Definition 44. Es sei $G = (V, E)$ ein Graph mit $|V| = n < \infty$. Weiter sei $v\colon \{1, \dots, n\} \to V$ eine bijektive Funktion. Die *Adjazenzmatrix* von G (bezüglich v) ist definiert als die Matrix $A = ((a_{i,j}))_{i,j=1}^n \in \mathbb{Q}^{n \times n}$ mit

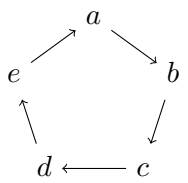
$$a_{i,j} = \begin{cases} 1 & \text{falls } (v(i), v(j)) \in E \\ 0 & \text{sonst} \end{cases}$$

für $i, j = 1, \dots, n$.

Die Funktion v in der obigen Definition bedeutet bloß, dass die Knoten in einer beliebigen aber bestimmten Weise angeordnet werden sollen. Welche Reihenfolge gewählt wird, ist egal, aber für zwei verschiedene Wahlen von v erhält man im allgemeinen verschiedene Adjazenzmatrizen.

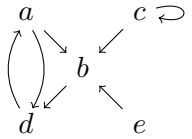
Beispiel. Im folgenden ist für die Adjazenzmatrix A immer angenommen, dass v die Knoten in der Reihenfolge durchnumeriert, in der sie notiert sind.

1. $G_1 = (V_1, E_1)$ mit $V_1 = \{a, b, c, d, e\}$, $E_1 = \{(a, b),\ (b, c),\ (c, d),\ (d, e),\ (e, a)\}$



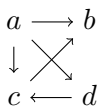
$$A_1 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

2. $G_2 = (V_2, E_2)$ mit $V_2 = \{a, b, c, d, e\}$,
   $E_2 = \{(a, b),\ (a, d),\ (c, c),\ (c, b),\ (e, b),\ (d, a),\ (b, d)\}$



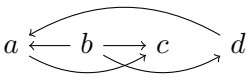
$$A_2 = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

3. $G_3 = (V_3, E_3)$ mit $V_3 = \{a, b, c, d\}$, $E_3 = \{(a, b),\ (a, c),\ (a, d),\ (c, b),\ (d, c)\}$



$$A_3 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

4. $G_4 = (V_4, E_4)$ mit $V_4 = \{a, b, c, d\}$, $E_4 = \{(a, c),\ (b, a),\ (b, c),\ (b, d),\ (d, a)\}$



$$A_4 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Definition 45. Seien $G = (V, E)$ und $G' = (V', E')$ zwei Graphen. Eine Funktion $h\colon V \to V'$ mit

$$\forall\ v_1, v_2 \in V : (v_1, v_2) \in E \iff (h(v_1), h(v_2)) \in E'$$

heißt *(Graphen-)Homomorphismus* von G nach G'. Ist h bijektiv, spricht man von einem *(Graphen-)Isomorphismus* und sagt, die Graphen G und G' seien (zueinander) *isomorph.* Schreibweise in diesem Fall: $G \cong G'$.

Beispiel. Von den vier Graphen im vorigen Beispiel sind nur der dritte und der vierte zueinander isomorph. Die Abbildung $h\colon V_3 \to V_4$, die durch folgende Wertetabelle definiert ist, ist ein Isomorphismus.

v	a	b	c	d
$h(v)$	b	c	a	d

Um das zu zeigen, rechnet man nach, dass die Mengen E_4 und

$$h(E_3) := \{\, (h(v), h(w)) : (v, w) \in E_3 \,\} \subseteq V_4^2$$

identisch sind. (Sie sind es.)

Dass G_1 und G_2 nicht isomorph sein können, sieht man zum Beispiel daran, dass der zweite Graph eine Schleife hat und der erste nicht. Ein Isomorphismus muss aber Schleifen (v, v) auf Schleifen $(h(v), h(v))$ abbilden.

Außerdem kann weder G_1 noch G_2 isomorph zu G_3 oder G_4 sein, weil ein Isomorphismus bijektiv sein muss und Graphen deshalb nur dann isomorph sein können, wenn sie die gleiche Anzahl von Knoten haben.

Anfänger glauben oft, dass zwei Graphen G_1 und G_2 isomorph sind, wenn für jedes $n \in \mathbb{N}$ die Zahl der Knoten in G_1, die mit genau n Knoten durch eine Kante verbunden sind, mit der Zahl der Knoten in G_2, die mit genau n durch eine Kante verbunden sind, übereinstimmt. Das ist aber falsch. Tatsächlich handelt es sich hierbei nur um eine notwendige Bedingung, aber nicht um eine hinreichende.

Satz 64. Seien $G = (V, E)$ und $G' = (V', E')$ zwei Graphen mit endlichen Kantenmengen V, V'. Sei A eine Adjazenzmatrix von G und A' eine Adjazenzmatrix von G'. Dann gilt: G und G' sind genau dann isomorph, wenn $|V| = |V'|$ gilt und es eine Permutationsmatrix $P \in \mathbb{Q}^{|V|\times|V|}$ gibt mit $A' = PAP^{-1}$.

Beweis. Seien $v\colon \{1, \ldots, |V|\} \to V$ und $v'\colon \{1, \ldots, |V'|\} \to V'$ die zu den gegebenen Adjazenzmatrizen A und A' gehörenden Bijektionen.

"$\Rightarrow$" Sei $h\colon V \to V'$ ein Isomorphismus. Da h als Isomorphismus insbesondere bijektiv ist, ist $\pi := (v')^{-1} \circ h \circ v$ eine Bijektion von $\{1, \ldots, |V|\}$ nach $\{1, \ldots, |V'|\}$. Damit gilt $|V| = |V'|$ und somit ist π eine Permutation. Sei $P \in \mathbb{Q}^{|V|\times|V|}$ die zu π gehörende Permutationsmatrix. Wir zeigen $A' = PAP^{-1}$. Betrachte dazu eine beliebige Position $(i, j) \in \{1, \ldots, |V|\}^2$. Bezeichnen wir mit $a_{i,j}$ und $a'_{i,j}$ den Eintrag von A bzw. A' an Position (i, j), so gilt

$$\begin{aligned} a_{i,j} = 1 &\iff (v(i), v(j)) \in E \\ &\iff (h(v(i)), h(v(j))) \in E' \\ &\iff a'_{(v')^{-1}(h(v(i))),(v')^{-1}(h(v(j)))} = 1 \\ &\iff a'_{\pi(i),\pi(j)} = 1. \end{aligned}$$

Damit folgt die Behauptung aus Teil 3 von Satz 19.

"$\Leftarrow$" Sei $\pi\colon \{1, \ldots, |V|\} \to \{1, \ldots, |V|\}$ die zu P gehörige Permutation. Wir zeigen, dass $h\colon V \to V'$, $h = v' \circ \pi \circ v^{-1}$ ein Isomorphismus ist. Bezeichnen wir mit $a_{i,j}$ und $a'_{i,j}$ wieder den Eintrag von A bzw. A' an Position (i, j), so gilt nach Teil 3 von Satz 19 $a_{i,j} = 1 \iff a'_{\pi(i),\pi(j)}$. Für zwei beliebige Knoten $u, w \in V$ gilt dann

$$(u, v) \in E \iff a_{v(u),v(w)} = 1$$

$$\iff a'_{\pi(v(u)),\pi(w(u))} = 1$$
$$\iff a'_{v'(h(u)),v'(h(w))} = 1$$
$$\iff (h(u), h(w)) \in E',$$

was zu zeigen war. ∎

Beispiel. Betrachten wir noch einmal die Graphen G_3 und G_4 aus dem Beispiel nach Definition 44. Die dort angegebenen Adjazenzmatrizen

$$A_3 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{und} \quad A_4 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

gelten beide bezüglich der Funktion $v\colon \{1,2,3,4\} \to \{a,b,c,d\}$ mit $v(1) = a$, $v(2) = b$, $v(3) = c$, $v(4) = d$.

Ist $h\colon \{a,b,c,d\} \to \{a,b,c,d\}$ der Isomorphismus aus dem vorigen Beispiel, so ist die Permutation $\pi = v^{-1} \circ h \circ v$ gegeben durch

i	1	2	3	4
$\pi(i)$	2	3	1	4

.

Die zugehörige Permutationsmatrix lautet

$$P_\pi = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

In der Tat gilt

$$P_\pi^{-1} A_3 P_\pi = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} = A_4.$$

Definition 46. Sei $G = (V, E)$ ein Graph. Ein Tupel $((v_0, v_1), (v_2, v_3), \ldots, (v_{m-1}, v_m)) \in E^m$ heißt *Pfad* (engl. *path*) von $v_1 \in V$ nach $v_2 \in V$ von G der Länge m. Statt

$$((v_0, v_1), (v_2, v_3), \ldots, (v_{m-1}, v_m))$$

schreibt man einen Pfad auch in der Form $v_0{-}v_1{-}\cdots{-}v_m$.

Ein Pfad mit $v_0 = v_m$ heißt *geschlossener Pfad* oder *Zyklus* (engl. *cycle*) von G (der Länge m).

Beispiel.

1. Die Pfade der Länge 1 entsprechen genau den Kanten des Graphen, und die Zyklen der Länge 1 entsprechen genau seinen Schleifen.

2. Der Graph G_2 auf Seite 130 enthält den Pfad $c{-}c{-}b{-}d{-}a{-}b{-}d{-}a{-}d{-}a$. Dieser Pfad hat die Länge 9. Der Pfad ist kein Zyklus, aber z. B. die Pfade $a{-}b{-}d{-}a$ und $a{-}d{-}a$ sind Zyklen von G_2.

   Der Graph G_3 enthält dagegen keine Zyklen.

Satz 65. Sei $G = (V, E)$ ein Graph mit endlicher Knotenmenge, $v\colon \{1, \ldots, |V|\} \to V$ bijektiv und A die Adjazenzmatrix von G bezüglich v. Weiter seien $i, j \in \{1, \ldots, |V|\}$.

1. Der (i, j)-te Eintrag in der Matrix A^n ist genau die Anzahl der Pfade von $v(i)$ nach $v(j)$ der Länge n.
2. Der (i, j)-te Eintrag in der Matrix $A + A^2 + \cdots + A^n$ ist genau die Anzahl der Pfade von $v(i)$ nach $v(j)$ der Länge höchstes n.
3. Ein Pfad von $v(i)$ nach $v(j)$ existiert genau dann, wenn ein Pfad von $v(i)$ nach $v(j)$ der Länge höchstens $|V|$ existiert.

Beweis.

1. Induktion nach n. Für $n = 1$ folgt die Behauptung direkt aus Def. 44. Nehmen wir an, die Behauptung gilt für n. Sei $(i, j) \in \{1, \ldots, |V|\}^n$. Zu zeigen ist, dass der (i, j)-te Eintrag von A^{n+1} die Anzahl der Pfade von $v(i)$ nach $v(j)$ der Länge $n+1$ ist. Jeder solche Pfad lässt sich auffassen als ein Pfad von $v(i)$ nach $v(k)$ für ein $k \in \{1, \ldots, n\}$ gefolgt von der Kante $(v(k), v(j))$, falls diese existiert. Die Anzahl der Pfade von $v(i)$ nach $v(k)$ ist nach Voraussetzung der (i, k)-te Eintrag $a_{i,k}^{[n]}$ von A^n, und die Kante $(v(k), v(j))$ existiert nach Def. 44 genau dann, wenn $a_{k,j} = 1$ ist. Da $a_{k,j}$ im anderen Fall 0 ist, lässt sich die Anzahl der Pfade von $v(i)$ nach $v(j)$ der Länge $n + 1$ schreiben als

   $$a_{i,1}^{[n]} a_{1,j} + a_{i,2}^{[n]} a_{2,j} + \cdots + a_{i,|V|}^{[n]} a_{|V|,j}.$$

   Nach Definition der Matrizenmultiplikation ist dies genau der (i, j)-te Eintrag von $A^n A = A^{n+1}$.
2. Folgt direkt aus Teil 1.
3. Wir zeigen: aus jedem Pfad von u nach v der Länge $m > |V|$ lässt sich ein Pfad von u nach v mit einer Länge $< m$ konstruieren. Sei also P ein Pfad von u nach v der Länge $m > |V|$. Dann muss es in P mindestens einen Knoten w geben, der mehr als einmal besucht wird. Das heißt, wenn etwa $P = v_0 - v_1 - \cdots - v_m$ mit $v_0 = u$ und $v_m = v$ ist, dann muss es ein Paar (i, j) mit $i < j$ geben, so dass $v_i = v_j = w$ ist. In diesem Fall ist

   $$P' := v_0 - \cdots - v_{i-1} - v_i - v_{j+1} - v_{j+2} - \cdots - v_m$$

   ein Pfad von u nach v der Länge $m - (j - i) < m$. Beachte, dass $(v_i, v_{j+1}) = (v_j, v_{j+1})$ eine Kante von G ist, weil sie bereits im ursprünglichen Pfad P vorkommt. ∎

Beispiel.

1. Betrachten wir noch einmal den Graphen G_2 von Seite 130. Für $n = 7$ erhalten wir

   $$A_2^7 = \begin{pmatrix} 3 & 2 & 0 & 4 & 0 \\ 2 & 1 & 0 & 2 & 0 \\ 4 & 4 & 1 & 6 & 0 \\ 2 & 2 & 0 & 3 & 0 \\ 1 & 1 & 0 & 2 & 0 \end{pmatrix}.$$

Der Eintrag 6 an Position $(3,4)$ sagt aus, dass es genau 6 Möglichkeiten gibt, in genau sieben Schritten von c nach d zu gelangen. In der Tat sind das die folgenden Pfade:

$$\begin{aligned}
&c{-}b{-}d{-}a{-}b{-}d{-}a{-}d,\\
&c{-}b{-}d{-}a{-}b{-}a{-}b{-}d,\\
&c{-}c{-}c{-}b{-}d{-}a{-}b{-}d,\\
&c{-}c{-}c{-}c{-}b{-}d{-}a{-}d,\\
&c{-}c{-}c{-}c{-}c{-}c{-}a{-}d.
\end{aligned}$$

2. Für den Graphen G_3 auf Seite 130 gilt $A_3^4 = 0$. Es gibt in diesem Graphen also keine Pfade der Länge 4. Längere Pfade kann es dann natürlich auch nicht geben. Die Gesamtzahl sämtlicher Pfade (beliebiger Länge) von einen Knoten zu einem anderen ist deshalb gegeben durch

$$A_3 + A_3^2 + A_3^3 = \begin{pmatrix} 0 & 3 & 2 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

   Man kann sich überlegen, dass ein Graph $G = (V, E)$ mit Adjazenzmatrix A genau dann einen Zyklus enthält wenn $A^{|V|} \neq 0$ ist.

3. Statt der Anzahl der Pfade von u nach v kann man sich auch fragen, wie lang der kürzeste Pfad von u nach v ist. Man nennt die Länge eines kürzesten Pfades von u nach v die *Distanz* von u nach v, Schreibweise: $d(u, v)$. (Beachte: im allgemeinen gilt $d(u, v) \neq d(v, u)$.) Wenn es gar keinen Pfad von u nach v gibt, setzt man $d(u, v) = \infty$.

   Wir wollen für alle Knotenpaare u, v die Distanz $d(u, v)$ bestimmen. Dazu ist es hilfreich, eine Hilfsgröße

$$d_m(u,v) = \begin{cases} d(u,v) & \text{falls } d(u,v) \leq m \\ \infty & \text{sonst} \end{cases}$$

   einzuführen. Dann bedeutet $d_m(u, v) = \infty$, dass $d(u, v) > m$ ist, und $d_m(u, v) = k \in \mathbb{N}$, dass $d(u, v) = k$ ist. Nach Teil 3 von Satz 65 gilt für je zwei Knoten u, v eines Graphen $G = (V, E)$ stets $d(u, v) \leq |V|$ oder $d(u, v) = \infty$. Es genügt also, $d_{|V|}(u, v)$ zu berechnen.

   Ist $V = \{v_1, \ldots, v_n\}$, so gilt offenbar

$$d_{m_1+m_2}(u,v) = \min\big(d_{m_1}(u,v_1) + d_{m_2}(v_1,v), \ldots,\ d_{m_1}(u,v_n) + d_{m_2}(v_n,v)\big),$$

   denn wenn man auf einem kürzesten Pfad P von u nach v nach m_1 Schritten an einem Knoten v_i anhält, dann kann es nicht sein, dass es von u nach v_i einen Pfad mit weniger als m_1 Schritten gibt, sonst ließe sich daraus ein Pfad von u nach v konstruieren, der noch kürzer ist als P. (Wir nehmen hier an, dass min und + auf $\mathbb{N} \cup \{\infty\}$ so definiert sind, dass $\min(\infty, \infty) = \infty$, $\min(k, \infty) = k$ und $k + \infty = \infty + k = \infty + \infty = \infty$ für alle $k \in \mathbb{N}$ gilt.)

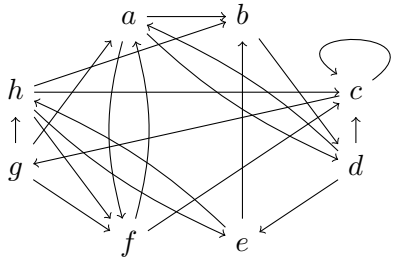
   Die obige Formel für $d_{m_1+m_2}(u, v)$ hat die gleiche Struktur wie die Formel für die Koeffizienten eines Matrixprodukts, wenn man + und $\cdot$ durch min und + ersetzt. Man

kann also eine Entfernungstabelle für einen Graphen G wie folgt berechnen. Wähle $v\colon \{1,\dots,|V|\} \to V$ und setze $D_1 = ((\, d_1(v(i),v(j))\,))_{i,j=0}^{\infty}$. Beachte dabei, dass

$$d_1(v(i),v(j)) = \begin{cases} 0 & \text{falls } i = j \\ 1 & \text{falls } i \neq j \text{ und } (v(i),v(j)) \in E \\ \infty & \text{sonst} \end{cases}$$

für alle i,j gilt. Berechne die Matrix-Potenz $D := D_1^{|V|+1}$, wobei min und + statt + und $\cdot$ verwendet werden. Der (i,j)-te Eintrag von D ist dann genau $d(v(i),v(j))$.

Beispiel: Für den Graph



erhält man die folgende Entfernungstabelle:

	a	b	c	d	e	f	g	h
a	0	1	2	1	2	1	3	3
b	2	0	2	1	2	3	3	3
c	2	3	0	3	3	2	1	2
d	1	2	1	0	1	2	2	2
e	3	1	2	2	0	2	3	1
f	1	2	1	2	3	0	2	3
g	1	2	2	2	2	1	0	1
h	2	1	1	2	1	1	2	0

22 C-finite Folgen

Definition 47.

1. Eine Funktion $a\colon \mathbb{N} \to \mathbb{K}$ heißt *Folge* (engl. *sequence*) in $\mathbb{K}$. Statt a schreibt man auch $(a_n)_{n=0}^{\infty}$.

2. Eine Folge a heißt *C-finit,* falls es einen Vektor $(c_0,\dots,c_r) \in \mathbb{K}^{r+1} \setminus \{0\}$ gibt, so dass für alle $n \in \mathbb{N}$ gilt

$$c_0 a(n) + c_1 a(n+1) + \cdots + c_r a(n+r) = 0.$$

Beispiel.

1. Die Folge $(F_n)_{n=0}^{\infty}$ der Fibonacci-Zahlen ist C-finit. Sie erfüllt die Rekurrenz

$$F_n + F_{n+1} - F_{n+2} = 0$$

für alle $n \in \mathbb{N}$.

2. Die Folge $a\colon \mathbb{N} \to \mathbb{Q}$ mit $a(n) = n^2$ ist C-finit. Eine Rekurrenz lautet

$$a(n) - 3a(n+1) + 3a(n+2) - a(n+3) = 0.$$

3. Die Folge $a\colon \mathbb{N} \to \mathbb{Q}$ mit $a(n) = n!$ ist nicht C-finit. Um das zu zeigen, muss man zeigen, dass sie keine lineare Rekurrenz mit konstanten Koeffizienten erfüllt, egal wie groß die Ordnung r gewählt wird. Anders ausgedrückt ist zu zeigen, dass die Folgen $(n!)_{n=0}^{\infty}$, $((n+1)!)_{n=0}^{\infty}$, $\dots$, $((n+r)!)_{n=0}^{\infty}$ aufgefasst als Elemente des Vektorraums $\mathbb{Q}^{\mathbb{N}}$ linear unabhängig über $\mathbb{Q}$ sind. Dazu betrachte man Konstanten $c_0, \dots, c_r \in \mathbb{Q}$ mit

$$c_0 n! + c_1 (n+1)! + \cdots + c_r (n+r)! = 0$$

für alle $n \in \mathbb{N}$. Es ist zu zeigen, dass all diese Konstanten Null sein müssen. Wäre das nicht so, dann gäbe es zumindest ein i mit $c_i \neq 0$. O.B.d.A. können wir $i = r$ annehmen. Division durch $(n+r)!$ liefert die Gleichung

$$c_0 \frac{1}{(n+1)\cdots(n+r)} + c_1 \frac{1}{(n+2)\cdots(n+r)} + \cdots + c_{r-1} \frac{1}{n+r} + c_r = 0$$

für alle $n \in \mathbb{N}$. Auf der linken Seite steht nun eine Linearkombination von rationalen Ausdrücken. Aus der Analysis ist bekannt, dass $\lim_{n\to\infty} \frac{1}{p(n)} = 0$ ist für jedes Polynom p mit $\deg p > 0$. Der Grenzwert der linken Seite für $n \to \infty$ ist deshalb c_r. Der Grenzwert der rechten Seite ist aber 0. Also muss $c_r = 0$ sein, im Widerspruch zur Annahme.

Satz 66. Sei $(c_0, \dots, c_r) \in \mathbb{K}^{r+1}$ mit $c_r \neq 0$. Dann gilt:

1. $U := \{\, (a_n)_{n=0}^{\infty} \in \mathbb{K}^{\mathbb{N}} : \forall\ n \in \mathbb{N} : c_0 a_n + \cdots + c_r a_{n+r} = 0 \,\}$ ist ein Untervektorraum von $\mathbb{K}^{\mathbb{N}}$.

2. Die Abbildung

$$h\colon U \to \mathbb{K}^r, \quad h(a_0, a_1, \dots) := (a_0, \dots, a_{r-1})$$

ist ein Isomorphismus.

Beweis.

1. Zu zeigen: $0 \in U$ und für alle $u, v \in U$ und alle $\alpha, \beta \in \mathbb{K}$ gilt $\alpha u + \beta v \in U$. Dass 0 in U liegt, folgt aus
$$c_0 0 + c_1 0 + \cdots + c_r 0 = 0.$$
Sind $u, v \in U$, so gilt
$$c_0 u(n) + c_1 u(n+1) + \cdots + c_r u(n+r) = 0,$$
$$c_0 v(n) + c_1 v(n+1) + \cdots + c_r v(n+r) = 0$$
für alle $n \in \mathbb{N}$. Multiplikation der ersten Gleichung mit $\alpha \in \mathbb{K}$ und der zweiten mit $\beta \in \mathbb{K}$, und Addition der beiden resultierenden Gleichungen liefert
$$c_0\big(u(n) + v(n)\big) + c_1\big(u(n+1) + v(n+1)\big) + \cdots c_r\big(u(n+r) + v(n+r)\big) = 0$$
für alle $n \in \mathbb{N}$. Also ist auch $u + v \in U$.

2. Man überzeugt sich leicht, dass h ein Homomorphismus ist. Um zu zeigen, dass h bijektiv ist, genügt es zu zeigen, dass es für jeden Vektor $(a_0, \ldots, a_{r-1}) \in \mathbb{K}^r$ genau eine Folge $a \in U$ mit $h(a) = (a_0, \ldots, a_{r-1})$ gibt. Zunächst muss für jede solche Folge a offensichtlich zumindest $a(n) = a_n$ für $n = 0, \ldots, r-1$ gelten. Ferner gilt für beliebiges $n \geq r$, dass es wegen der Rekurrenz für den Wert von $a(n)$ genau eine Möglichkeit gibt, nämlich
$$a(n) = -\frac{1}{c_r}\big(c_0 a(n-r) + c_1 a(n-r+1) + \cdots + c_{r-1} a(n-1)\big).$$
Durch Induktion nach n erhält man, dass alle Terme der Folge a eindeutig festgelegt sind. ∎

Beispiel. Die Lösungsmenge der Rekurrenz
$$f(n) + f(n+1) - f(n+2) = 0$$
ist ein zwei-dimensionaler Vektorraum. Jede Lösung ist eindeutig festgelegt durch ihre beiden Anfangswerte $f(0)$ und $f(1)$.

Insbesondere gibt es eine Lösung f_1 mit $f_1(0) = 0$ und $f_1(1) = 1$ und eine Lösung f_2 mit $f_1(0) = 1$ und $f_1(1) = 0$. Die Folge f_1 ist die Folge der Fibonacci-Zahlen. Diese beiden Lösungen sind linear unabhängig, weil die Vektoren $h(f_1) = (0, 1)$ und $h(f_2) = (1, 0)$ linear unabhängig sind. Es ist also $\{f_1, f_2\}$ eine Basis von U.

Alle anderen Lösungen f lassen sich damit als Linearkombination $\alpha f_1 + \beta f_2$ schreiben. Die ersten Terme von f ergeben sich zu
$$\beta,\ \alpha,\ \alpha+\beta,\ \alpha+2\beta,\ 2\alpha+3\beta,\ 3\alpha+5\beta,\ 5\alpha+8\beta, \ldots$$

Satz 67. Es sei $a\colon \mathbb{N} \to \mathbb{K}$ eine C-finite Folge, die eine Rekurrenz der Ordnung r erfüllt. Dann gilt: Sind $c_0, \ldots, c_r \in \mathbb{K}$ so, dass
$$c_0 a(n) + c_1 a(n+1) + \cdots + c_r a(n+r) = 0$$
für $n = 0, \ldots, r-1$, so gilt
$$c_0 a(n) + c_1 a(n+1) + \cdots + c_r a(n+r) = 0$$
für alle $n \in \mathbb{N}$.

Beweis. Nach Annahme über a existieren gewisse Konstanten $\tilde{c}_0, \ldots, \tilde{c}_r \in \mathbb{K}$, von denen wenigstens eine von Null verschieden ist, und für die gilt

$$\tilde{c}_0 a(n) + \tilde{c}_0 a(n+1) + \cdots + \tilde{c}_r a(n+r) = 0$$

für alle $n \in \mathbb{N}$. Betrachte den Vektorraum $U \subseteq \mathbb{K}^{\mathbb{N}}$ bestehend aus allen Folgen f mit

$$\tilde{c}_0 f(n) + \tilde{c}_0 f(n+1) + \cdots + \tilde{c}_r f(n+r) = 0$$

für alle $n \in \mathbb{N}$. Nach Satz 66 gilt $\dim U \leq r$. Ferner gilt neben $a \in U$ auch $(a(n+i))_{n\geq 0} \in U$ für jedes fest gewählte $i \in \mathbb{N}$, denn wenn

$$\tilde{c}_0 a(n) + \tilde{c}_0 a(n+1) + \cdots + \tilde{c}_r a(n+r) = 0$$

für alle $n \in \mathbb{N}$ gilt, dann gilt auch

$$\tilde{c}_0 a(n+i) + \tilde{c}_0 a(n+i+1) + \cdots + \tilde{c}_r a(n+i+r) = 0$$

für alle $n, i \in \mathbb{N}$. Da U ein Vektorraum ist, gehört auch die Linearkombination

$$b(n) := c_0 a(n) + c_1 a(n+1) + \cdots + c_r a(n+r)$$

zu U.

Nach Voraussetzung gilt nun $b(0) = b(1) = \cdots = b(r-1) = 0$. Aus Teil 2 von Satz 66 folgt, dass $b(n) = 0$ für alle $n \in \mathbb{N}$. ∎

Beispiel. Satz 67 besagt, dass man die Koeffizienten der Rekurrenz für eine C-finite Folge a rekonstruieren kann, wenn man die Ordnung r der Rekurrenz sowie die Terme $a(0), \ldots, a(2r-1)$ kennt. Man braucht dazu bloß ein lineares Gleichungssystem zu lösen.

Ist etwa bekannt, dass $a\colon \mathbb{N} \to \mathbb{Q}$ eine Rekurrenz der Ordnung zwei erfüllt, so sucht man Konstanten $c_0, c_1, c_2 \in \mathbb{Q}$ mit

$$c_0 a(n) + c_1 a(n+1) + c_2 a(n+2) = 0$$

für alle $n \in \mathbb{N}$. Nach dem Satz genügt schon, dass diese Bedingung für $n = 0, 1$ erfüllt ist. Wenn man außerdem weiß, dass a mit den Termen 0, 1, 5, 19 beginnt, dann konkretisiert sich die obige Gleichung für $n = 0, 1$ zu

$$\begin{pmatrix} 0 & 1 & 5 \\ 1 & 5 & 19 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \end{pmatrix} = 0.$$

Der Lösungsraum dieses Gleichungssystems wird aufgespannt von $(6, -5, 1)$, und also erfüllt a nach Satz 67 die Rekurrenz

$$6a(n) - 5a(n+1) + a(n+2) = 0.$$

Wenn man die Ordnung r der Rekurrenz von a nicht kennt, dann kann man immer noch probieren, ob man für ein frei gewähltes r aus den bekannten Termen von a eine Rekurrenz rekonstruieren kann. Man macht dazu wie im vorherigen Beispiel einen Ansatz für die Koeffizienten und stellt ein lineares Gleichungssystem auf. Man sollte dabei r klein genug wählen, dass man aus den bekannten Termen von a ein überbestimmtes Gleichungssystem konstruieren kann (also eines mit mehr Gleichungen als Variablen). Solch ein System hat typischerweise keine Lösung außer 0. Wenn man trotzdem eine Lösung bekommt, dann ist das ein Indiz (aber natürlich noch kein Beweis), dass man die Koeffizienten der wahren Rekurrenz von a gefunden hat.

Beispiel. Betrachte die Folge $a\colon \mathbb{N} \to \mathbb{Q}$ mit $a(n) = n\,F_n$, wobei F_n die $n$te Fibonacci-Zahl ist. Die ersten 10 Terme von a lauten $0, 1, 2, 6, 12, 25, 48, 91, 168, 306, 550$. Ist a C-finit?

Versuchen wir es mit $r = 3$. Wenn

$$c_0 a(n) + c_1 a(n+1) + c_2 a(n+2) + c_3 a(n+3) = 0$$

für alle $n \in \mathbb{N}$ gelten soll, dann muss es auf jeden Fall auch für $n = 0, \ldots, 10 - 3$ gelten. Das führt auf das Gleichungssystem

$$\begin{pmatrix} 0 & 1 & 2 & 6 \\ 1 & 2 & 6 & 12 \\ 2 & 6 & 12 & 25 \\ 6 & 12 & 25 & 48 \\ 12 & 25 & 48 & 91 \\ 25 & 48 & 91 & 168 \\ 48 & 91 & 168 & 306 \\ 91 & 168 & 306 & 550 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix} = 0.$$

Diese Gleichungssystem hat nur die triviale Lösung $(0, 0, 0, 0)$. Daraus folgt, dass a ganz sicher keine Rekurrenz der Ordnung drei (oder kleiner) erfüllt.

Es folgt aber nicht, dass a nicht C-finit ist. Es kann immer noch eine Rekurrenz höherer Ordnung erfüllen. Zum Beispiel $r = 4$. In diesem Fall bekommt man mit den gleichen Daten das lineare Gleichungssystem

$$\begin{pmatrix} 0 & 1 & 2 & 6 & 12 \\ 1 & 2 & 6 & 12 & 25 \\ 2 & 6 & 12 & 25 & 48 \\ 6 & 12 & 25 & 48 & 91 \\ 12 & 25 & 48 & 91 & 168 \\ 25 & 48 & 91 & 168 & 306 \\ 48 & 91 & 168 & 306 & 550 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \end{pmatrix} = 0.$$

Obwohl es sich wieder um ein überbestimmtes System handelt, gibt es eine nichttriviale Lösung, nämlich $(1, 2, -1, -2, 1)$. Das legt die Vermutung nah, dass a die Rekurrenz

$$a(n) + 2a(n+1) - a(n+2) - 2a(n+3) + a(n+4) = 0$$

erfüllt.

In der Tat ist nicht schwer zu zeigen, dass diese Vermutung korrekt ist, indem man $n\,F_n$ in die Rekurrenz einsetzt und den entstehenden Ausdruck mithilfe der bekannten Rekurrenz $F_{n+2} = F_{n+1} + F_n$ zu 0 vereinfacht.

Satz 68. Es seien $(a_n)_{n=0}^{\infty}$ und $(b_n)_{n=0}^{\infty}$ zwei C-finite Folgen. Dann gilt:

1. $(a_n + b_n)_{n=0}^{\infty}$ ist C-finit.
2. $(a_n b_n)_{n=0}^{\infty}$ ist C-finit.
3. für jedes fixe $u \in \mathbb{N}$ ist $(a_{un})_{n=0}^{\infty}$ C-finit.
4. $(\sum_{k=0}^{n} a_k)_{n=0}^{\infty}$ ist C-finit.

Beweis. Wir zeigen den zweiten Teil. Die Beweise für die anderen Teile gehen ähnlich.
Nach Voraussetzung sind $(a_n)_{n=0}^{\infty}$ und $(b_n)_{n=0}^{\infty}$ C-finit. Es gibt also $(\alpha_0, \ldots, \alpha_r) \in \mathbb{K}^{r+1} \setminus \{0\}$ und $(\beta_0, \ldots, \beta_s) \in \mathbb{K}^{s+1} \setminus \{0\}$ mit

$$\begin{aligned} \alpha_0 a_n + \alpha_1 a_{n+1} + \cdots + \alpha_r a_{n+r} &= 0 \\ \beta_0 b_n + \beta_1 b_{n+1} + \cdots + \beta_s b_{n+s} &= 0. \end{aligned}$$

Durch geeignete Wahl von r und s können wir o.B.d.A. annehmen, dass $\alpha_r \neq 0$ und $\beta_s \neq 0$ ist. Aus den Rekurrenzen folgt dann, dass sich die Folgen $(a_{n+r})_{n=0}^{\infty}$ und $(b_{n+s})_{n=0}^{\infty}$ als Linearkombinationen der Folgen $(a_n)_{n=0}^{\infty}, \ldots, (a_{n+r-1})_{n=0}^{\infty}$ bzw. $(b_n)_{n=0}^{\infty}, \ldots, (b_{n+s-1})_{n=0}^{\infty}$ darstellen lassen. Allgemeiner folgt durch Induktion, dass sich für jedes fixe $i \in \mathbb{N}$ sogar die Folgen $(a_{n+i})_{n=0}^{\infty}$ und $(b_{n+i})_{n=0}^{\infty}$ als Linearkombinationen dieser Folgen darstellen lassen.
Für den Vektorraum $V \subseteq \mathbb{K}^{\mathbb{N}}$, der von den Folgen $(a_{n+i}b_{n+j})_{n=0}^{\infty}$ mit $i, j \in \mathbb{N}$ erzeugt wird, gilt deshalb $\dim V \leq rs$; als Erzeugendensystem genügen nämlich die Folgen $(a_{n+i}b_{n+j})_{n=0}^{\infty}$ mit $0 \leq i < r$ und $0 < i \leq s$.
Wegen $\dim V \leq rs$ müssen je $rs+1$ viele Elemente von V linear abhängig sein. Insbesondere muss es eine lineare Abhängigkeit zwischen den Folgen $(a_n b_n)_{n=0}^{\infty}, \ldots, (a_{n+rs}b_{n+rs})_{n=0}^{\infty}$ geben. Es gibt also Konstanten $\gamma_0, \ldots, \gamma_{rs} \in \mathbb{K}$, von denen mindestens eine von Null verschieden ist, und für die gilt

$$\gamma_0 a_n b_n + \gamma_1 a_{n+1} b_{n+1} + \cdots + \gamma_s a_{n+rs} b_{n+rs} = 0$$

für alle $n \in \mathbb{N}$. ∎

Beispiel.

1. Sei $a = (F_n)_{n=0}^{\infty}$ die Folge der Fibonacci-Zahlen und $b = (n)_{n=0}^{\infty}$. Es sei bekannt, dass a die Rekurrenz $a(n) + a(n+1) - a(n+2) = 0$ und b die Rekurrenz $b(n) - 2b(n+1) + b(n+2) = 0$ erfüllt. Gesucht sei eine Rekurrenz für $c = (nF_n)_{n=0}^{\infty}$.

   Es gilt

   $$\begin{aligned} a(n+2) &= a(n) + a(n+1) & b(n+2) &= -b(n) + 2b(n+1) \\ a(n+3) &= a(n) + 2a(n+1) & b(n+3) &= -2b(n) + 3b(n+1) \\ a(n+4) &= 2a(n) + 3a(n+1) & b(n+4) &= -3b(n) + 4b(n+1) \end{aligned}$$

   für alle $n \in \mathbb{N}$. Für die Produkte ergibt sich daraus

   $$\begin{aligned} a(n)b(n) &= a(n)b(n) \\ a(n+1)b(n+1) &= a(n+1)b(n+1) \\ a(n+2)b(n+2) &= -a(n)b(n) - a(n+1)b(n) + 2a(n)b(n+1) + 2a(n+1)b(n+1) \\ a(n+3)b(n+3) &= -2a(n)b(n) - 4a(n+1)b(n) + 3a(n)b(n+1) + 6a(n+1)b(n+1) \\ a(n+4)b(n+4) &= -6a(n)b(n) - 9a(n+1)b(n) + 8a(n)b(n+1) + 12a(n+1)b(n+1). \end{aligned}$$

   Die Koeffizienten der Rekurrenz findet man durch Lösen des linearen Gleichungssystems

   $$\begin{pmatrix} 1 & 0 & -1 & -2 & -6 \\ 0 & 0 & -1 & -4 & -9 \\ 0 & 0 & 2 & 3 & 8 \\ 0 & 1 & 2 & 6 & 12 \end{pmatrix} \begin{pmatrix} \gamma_0 \\ \gamma_1 \\ \gamma_2 \\ \gamma_3 \\ \gamma_4 \end{pmatrix} = 0.$$

Dass das System eine Lösung haben muss, sieht man sofort daran, dass es mehr Variablen als Gleichungen hat. Und tatsächlich stellt sich heraus, dass der Lösungsraum eindimensional ist und vom Vektor $(1, 2, -1, -2, 1)$ aufgespannt wird. Daraus folgt, dass die Folge $c = (nF_n)_{n=0}^{\infty}$ die Rekurrenz

$$c(n) + 2c(n+1) - c(n+2) - 2c(n+3) + c(n+4) = 0$$

erfüllt.

2. Auf der Grundlage von Satz 68 kann man ein Computerprogramm schreiben, das Identitäten für C-finite Folgen automatisch beweist. Um zum Beispiel die Summationsformel

$$\sum_{k=0}^{n} F_k^2 = F_n F_{n+1}$$

zu beweisen, beginnt das Programm mit der Rekurrenz $F_n + F_{n+1} - F_{n+2} = 0$ für die Fibonacci-Zahlen, die entweder vom Benutzer eingegeben oder aus einer Datenbank gelesen wird. Dann berechnet es wie im vorherigen Beispiel je eine Rekurrenz für $(F_n^2)_{n=0}^{\infty}$ und für $(F_n F_{n+1})_{n=0}^{\infty}$. Aus der Rekurrenz für $(F_n^2)_{n=0}^{\infty}$ lässt sich als nächstes eine Rekurrenz für die Summe $(\sum_{k=0}^{n} F_k^2)_{n=0}^{\infty}$ berechnen, und daraus schließlich eine Rekurrenz für die Differenz $d(n) := (\sum_{k=0}^{n} F_k^2) - F_n F_{n+1}$ von linker und rechter Seite. Das Ergebnis dieser Rechnung lautet

$$d(n) - 2d(n+1) - 2d(n+2) + d(n+3) = 0$$

für alle $n \in \mathbb{N}$. Um zu zeigen, dass $d(n) = 0$ für alle $n \in \mathbb{N}$ gilt, braucht man nach Teil 2 von Satz 66 nur noch nachzurechnen, dass $d(n) = 0$ für $n = 0, 1, 2$ gilt.

23 Kodierungstheorie

Digitale Informationsverarbeitung beruht auf dem Prinzip, jede mögliche Information als eine Folge von Nullen und Einsen darzustellen. Diese Folgen sind immer endlich, aber möglicherweise sehr lang. Die Datei dieses Skriptums ist zum Beispiel mehrere Megabyte groß. Das bedeutet, sie wird im Computer dargestellt als eine Folge von mehreren Millionen Vektoren $b \in \{0, 1\}^8$. Einen solchen Vektor nennt man ein *Byte*. Die Koordinaten eines Bytes nennt man *Bit*.

Ein Bit kann je nach Kontext zum Beispiel Informationen wie an/aus, schwarz/weiss, 0/1, wahr/falsch, rechts/links, männlich/weiblich codieren. In einem Byte kann man z. B. die natürlichen Zahlen von 0 bis 255 codieren:

$$\begin{aligned}
(0,0,0,0,0,0,0,0) &= 0,\\
(0,0,0,0,0,0,0,1) &= 1,\\
(0,0,0,0,0,0,1,0) &= 2,\\
(0,0,0,0,0,0,1,1) &= 3,\\
(0,0,0,0,0,1,0,0) &= 4, \text{ etc.}
\end{aligned}$$

Auch die Zeichen in einem Text kann man mit Bytes codieren, indem man z. B. durch eine Tabelle festlegt, welches Byte welchem Buchstaben entsprechen soll. Die 256 verschiedenen Bytes sind mehr als ausreichend, um die 52 Groß- und Kleinbuchstaben, die 10 Ziffern, das Leerzeichen und einige Interpunktions- und Sonderzeichen unterzubringen.

Mit Folgen von Bytes läßt sich quasi alles codieren: Zahlen, Formeln, Texte, Computerprogramme, geometrische Objekte, Kundendaten, Fahrpläne, Musik, Fotos, Videos, Wetter- und Klimamodelle, usw. In der Kodierungstheorie beschäftigt man sich mit dem Design solcher Codierungen. Allgemeiner stellt man sich die Frage, wie man eine gegebene Codierung (d. h. eine gegebene Bitfolge) in eine andere umwandeln kann, die zum Übertragen oder Speichern der Information besser geeignet sind. Typische Fragestellungen sind in diesem Zusammenhang:

- *Datenkompression:* Wie kann ich eine gegebene Bitfolge in eine kürzere Bitfolge umwandeln, die die gleiche Information enthält? Oder: Kann ich aus einer gegebenen Bitfolge die „wesentliche" Information von der „unwesentlichen" trennen, so dass ich nur die wesentliche speichern oder übertragen muss?
- *Fehlererkennung:* Wie kann ich eine gegebene Bitfolge so abändern, dass sich nach der Übertragung feststellen lässt, ob ein Teil der Bitfolge fehlerhaft übertragen wurde? Lassen sich die Fehler nachträglich reparieren?
- *Kryptographie:* Wie kann ich eine gegebene Bitfolge verschlüsseln, d. h. so abändern, dass die darin codierte Information ohne geeignetes geheimes Zusatzwissen nicht zu rekonstruieren ist. Oder: wie kann ich eine gegebene Bitfolge signieren, d. h. so abändern, dass ein Empfänger verifizieren kann, dass die Nachricht wirklich von mir stammt?

Es gibt zu jedem dieser Punkte zahlreiche Techniken. Manche davon verwenden lineare Algebra. Als Beispiel erklären wir hier eine einfache Methode zur Fehlererkennung. Für Verallgemeinerungen und andere Methoden sei auf entsprechende Lehrveranstaltungen oder die Literatur verwiesen.

Definition 48.

1. Das *Gewicht* eines Vektors $a = (a_1, \dots, a_n) \in \mathbb{Z}_2^n$ ist definiert als
$$w(a) := |\{\, i : a_i \neq 0 \,\}| \in \{0, \dots, n\}.$$
2. Für $a = (a_1, \dots, a_n), b = (b_1, \dots, b_n) \in \mathbb{Z}_2^n$ heißt $d(a, b) := w(a - b)$ die *Hamming-Distanz* von a und b.
3. Ein Untervektorraum $U \subseteq \mathbb{Z}_2^n$ der Dimension k heißt *linearer Code* von Länge n und Rang k. Elemente von U heißen *Codewörter*. Die *Distanz* eines linearen Codes $U \subseteq \mathbb{Z}_2^n$ ist definiert als
$$d = \min\{\, w(u) : u \in U \setminus \{0\} \,\} \in \mathbb{N}.$$
4. Ist $U \subseteq \mathbb{Z}_2^n$ ein Code, dann heißt eine geordnete Basis $A \in \mathbb{Z}_2^{n \times k}$ von U eine *Erzeugermatrix* und eine Matrix $B \in \mathbb{Z}_2^{(n-k) \times n}$ mit $\ker B = U$ eine *Prüfmatrix* für U.

Beispiel.

1. $w(1, 0, 0, 1, 1, 0, 1, 0) = 4$, $w(0, 0, 1, 0, 1, 1, 1, 1) = 5$, $w(0, 1, 1, 0, 1, 0, 1, 1) = 5$, etc.

   $d(a, b)$ ist die Anzahl der Positionen, an denen sich a und b voneinander unterscheiden, zum Beispiel:
$$d\big((1, 1, 0, 1, 0, 1, 1),\ (1, 1, 0, 1, 0, 0, 1)\big) = 1$$
$$d\big((1, 1, 0, 1, 0, 1, 1),\ (1, 1, 0, 1, 1, 0, 1)\big) = 2$$
$$d\big((1, 1, 0, 1, 0, 1, 1),\ (0, 1, 0, 1, 1, 0, 1)\big) = 3$$

$$d\big((1,1,0,1,0,1,1),\ (0,1,1,1,1,0,1)\big) = 4$$
$$d\big((1,1,0,1,0,1,1),\ (0,1,1,0,1,0,1)\big) = 5$$

Es gilt $d(a,b) = 0$ genau dann, wenn $a = b$ ist.

2. Der Unterraum $U \subseteq \mathbb{Z}_2^4$, der von $u_1 = (1,0,1,1)$ und $u_2 = (0,1,1,0)$ erzeugt wird, besteht aus den folgenden Codewörtern:

$$0u_1 + 0u_2 = (0,0,0,0) \qquad 0u_1 + 1u_2 = (0,1,1,0)$$
$$1u_1 + 0u_2 = (1,0,1,1) \qquad 1u_1 + 1u_2 = (1,1,0,1).$$

Die Distanz dieses Codes ist 2.

Eine Erzeugermatrix für U ist $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{pmatrix}$.

Eine Prüfmatrix für U ist $B = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$.

Angenommen, man will k Bits über einen Kanal übertragen. Rauschen auf dem Kanal kann jedes übertragene Bit mit einer bestimmten (kleinen) Wahrscheinlichkeit ändern. Wir wollen die k Bits so codieren, dass der Empfänger eine korrekte Übertragung von einer fehlerhaften unterscheiden kann, solange in der Übertragung weniger als d Fehler auftreten.

Man wählt dazu einen Code $U \in \mathbb{Z}_2^n$ vom Rang k und Distanz d. Statt des Codeworts $v \in \mathbb{Z}_2^k$ überträgt man $u := Av \in \mathbb{Z}_2^n$, wobei A eine Erzeugermatrix von U ist. Beim Empfänger kommt ein Vektor $\tilde{u} \in \mathbb{Z}_2^n$ an, den er sich als eine Überlagerung $\tilde{u} = u + r$ des (ihm unbekannten) korrekten Codeworts $u \in \mathbb{Z}_2^n$ und einem (ihm ebenfalls unbekannten) Bitvektor $r \in \mathbb{Z}_2^n$, der dem Effekt des Rauschens entspricht.

Wenn $\tilde{u} \in U$ gilt, dann ist auch $r = \tilde{u} - u \in U$ und $w(r) \geq d$ oder $r = 0$, nach der Definiton der Distanz von U. Wenn der Empfänger also ein Codewort $\tilde{u}$ enthält, dann ist entweder die Übertragung fehlerfrei gewesen oder es ist zu mindestens d Fehlern gekommen. Ob $\tilde{u}$ ein Codewort ist, kann der Empfänger mit einer Prüfmatrix B für U überprüfen: dies ist genau dann der Fall, wenn $B\tilde{u} = 0$ gilt.

Beispiel. Betrachte den Code $H \in \mathbb{Z}_2^7$ mit

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

als Erzeuger- bzw. Prüfmatrix. Dieser Code heißt *Hamming-Code.*

Die Länge ist $n = 7$, der Rang ist $k = 4$. Die Distanz ist nicht direkt offensichtlich, aber da es nur $2^k = 16$ Codewörter gibt, kann man leicht alle auflisten und sich vergewissern, dass $d = 3$ ist.

Bei der Übertragung zweier Codewörter u_1, u_2 durch einen verrauschten Kanal wurden die beiden Wörter $\tilde{u}_1 = (1,0,1,1,0,1,0)$ und $\tilde{u}_2 = (1,1,0,1,1,1,0)$ empfangen.

Wegen $B\tilde{u}_1 = (0,0,0)$ und $B\tilde{u}_2 = (1,1,1)$ wurde das zweite nicht fehlerfrei übertragen. Bei der Übertragung des ersten Worts gab es entweder keinen Fehler oder mehr als zwei.

Das zweite Wort enthält ein oder mehrere falsche Bits. Wenn wir annehmen, dass nur ein Bit verfälscht wurde, lässt sich das korrekte Codewort u_2 aus $\tilde{u}_2$ rekonstruieren. In diesem Fall ist $\tilde{u}_2 = u_2 + e_i$ für einen Einheitsvektor e_i. Wir haben $B\tilde{u}_2 = B(u_2 + e_i) = Bu_2 + Be_i = Be_i$. Da Be_i die i-te Spalte von B ist und $B\tilde{u}_2 = (1,1,1)$ gilt, muss $i = 4$ sein. Das gesendete Wort war also entweder $u_2 = (1,1,0,\mathbf{0},1,1,0)$, oder es gab bei der Übertragung mehr als einen Fehler.

Satz 69. Sei $U \subseteq \mathbb{Z}_2^n$ ein Code der Länge n mit Rang k und Distanz d. Dann gilt $k+d \leq n+1$.

Beweis. Wegen $|\mathbb{Z}_2| = 2$ und $\dim U = k$ gilt $|U| = 2^k$.

Nach Definition der Distanz gilt $w(u) \geq d$ für alle $u \in U \setminus \{0\}$. Für je zwei verschiedene Codewörter $u, v \in U$ gilt dann auch $d(u,v) = w(u-v) \geq d$. Wenn also $u = (u_1, \ldots, u_n)$ und $v = (v_1, \ldots, v_n)$ ist, dann muss auch $(u_d, \ldots, u_n) \neq (v_d, \ldots, v_n)$ gelten. Da es höchstens 2^{n-d+1} viele verschiedene Bitvektoren der Länge $n+d-1$ gibt, muss also $|U| \leq 2^{n-d+1}$ sein. Daraus folgt $2^k \leq 2^{n-d+1}$, und daraus $k \leq n-d+1$. ∎

Die Distanz d eines Codes sagt aus, wie viele Fehler auftreten dürfen, ohne dass dem Empfänger die Fehlerhaftigkeit des empfangenen Wortes entgehen kann. Die Differenz $n-k$ gibt an, wie viele zusätzliche Bits der Code einsetzt, um diese Fehlererkennung zu gewährleisten. In der Praxis möchte man d möglichst groß und n (bzw. $n-k$) möglichst klein haben. Der obige Satz setzt diesem Zielkonflikt eine Grenze.

Der Hamming-Code erreicht diese Grenze nicht: $k+d = 3+2 = 5 < 8 = 7+1 = n+1$. Tatsächlich gibt es überhaupt keine (brauchbaren) Codes, für die $k+d = n+1$ gilt, zumindest solange man über dem Körper $\mathbb{Z}_2$ arbeitet. Codes, die für Speichermedien oder in Mobilfunknetzen verwendet werden, verwenden daher Körper $\mathbb{K}$ mit z. B. $2^8 = 256$ Elementen. Für solche Körper kann man (brauchbare) lineare Codes konstruieren, für die $k+d = n+1$ gilt. Ein Beispiel sind die sogenannten Reed-Solomon-Codes, deren Erklärung an dieser Stelle allerdings zu weit führen würde.

24 Lineare Algebra in Maple, Mathematica und Sage

Mit Vektoren und Matrizen von Hand zu rechnen ist mühsam, zweitaufwendig, fehleranfällig – und zum Glück heute nicht mehr nötig. Es gibt eine ganze Reihe von Computerprogrammen, die diese Arbeit bequem, schnell, und zuverlässig übernehmen. Grob einteilen lassen sich diese Programme in *numerische* und *symbolische* Software. Numerische Software ist auf den Fall spezialisiert, dass der Grundkörper $\mathbb{R}$ oder $\mathbb{C}$ ist. In diesen Körpern kann man im allgemeinen nur approximativ rechnen. Das hat sowohl theoretische Gründe (eine reelle Zahl ist erst dann eindeutig festgelegt, wenn man all ihre potentiell unendlich vielen Nachkommastellen kennt – die passen aber nicht in den endlichen Speicher eines Computers) als auch praktische (wenn es sich um Messwerte einer physikalischen Anwendung handelt, wird man von einer gewissen Fehlertoleranz bei der Messung ausgehen müssen). Wenn man mit gerundeten Zahlen rechnet, stellt sich die Frage, wieviel Genauigkeit man durch die Rechnung verliert, d. h. wie viele Nachkommastellen des Ergebnisses korrekt sind. Man kann sich dann auch fragen, ob eine andere Rechnung, die mathematisch äquivalent ist, eventuell eine bessere Genauigkeit liefert. Damit wollen wir uns hier nicht beschäftigen. Antworten auf Fragen dieser Art und einen Überblick über die entsprechenden Softwaresysteme bekommen Sie in den Lehrveranstaltungen des Instituts für Numerik.

Symbolische Software ist auf die Fälle spezialisiert, wo man die Elemente des Grundkörpers exakt darstellen und ohne Genauigkeitsverlust mit ihnen rechnen kann. Das ist insbesondere der Fall für den

Körper der rationalen Zahlen und für endliche Körper, aber zum Beispiel auch für den Körper $\mathbb{Q}(X)$ der rationalen Funktionen über $\mathbb{Q}$. Wir geben hier für drei solche Systeme einige Beispiele, wie man einfache Rechnungen mit Vektoren und Matrizen in diesen Systemen durchführt. Man darf sich vorstellen, dass intern das gleiche passiert, was auch bei einer Handrechnung passieren würde, auch wenn das nicht unbedingt der Fall ist. Was diese Systeme wirklich tun, werden wir am Ende des zweiten Semesters besprechen. Mehr dazu erfahren Sie am Institut für Symbolisches Rechnen oder am Institut für Algebra.

Beispiel.

1. *Maple.* Die Funktionalität für das Rechnen mit Vektoren und Matrizen wird in Maple in einem Paket LinearAlgebra zusammengefasst, das man zunächst laden muss, wenn man Funktionen aus diesem Paket verwenden will. Danach hat man Funktionen zur Verfügung, mit denen man Vektoren und Matrizen erzeugen, auf deren Komponenten zugreifen, sie addieren und multiplizieren und Gleichungssysteme lösen kann. Es ist zu beachten, dass Maple zwischen Zeilen und Spaltenvektoren unterscheidet.

   with(LinearAlgebra) :
   $v :=$ Vector$([7, 4, -3])$;

   $$\begin{bmatrix} 7 \\ 4 \\ -3 \end{bmatrix}$$

   $v[2]$

   $$4$$

   $5 \cdot v$

   $$\begin{bmatrix} 35 \\ 20 \\ -15 \end{bmatrix}$$

   $v +$ Vector$([1, 2, 3])$

   $$\begin{bmatrix} 8 \\ 6 \\ 0 \end{bmatrix}$$

   $A :=$ Matrix$([[1, 2, 3], [4, 5, 6], [7, 8, 9]])$

   $$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}$$

   $A[2, 3]$

   $$6$$

   Multiply(A, v)

   $$\begin{bmatrix} 8 \\ 26 \\ 44 \end{bmatrix}$$

   Multiply(v, A)
   `Error, (in Multiply) cannot multiply a column Vector and a Matrix`

   $vt :=$ Transpose(v);

$$\begin{bmatrix} 7 & -4 & 3 \end{bmatrix}$$

Multiply(vt, A)

$$\begin{bmatrix} 12 & 18 & 24 \end{bmatrix}$$

$B :=$ Matrix$([[1,1,1],[1,2,3],[1,4,9]])$

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 4 & 9 \end{bmatrix}$$

Multiply(A, B)

$$\begin{bmatrix} 6 & 17 & 34 \\ 15 & 38 & 73 \\ 24 & 59 & 112 \end{bmatrix}$$

$A\hat{}5$

$$\begin{bmatrix} 121824 & 149688 & 177552 \\ 275886 & 338985 & 402084 \\ 429948 & 528282 & 626616 \end{bmatrix}$$

$B\hat{}(-1)$

$$\begin{bmatrix} 3 & -\frac{5}{2} & \frac{1}{2} \\ -3 & 4 & -1 \\ 1 & -\frac{3}{2} & \frac{1}{2} \end{bmatrix}$$

NullSpace(A)

$$\left\{ \begin{bmatrix} 1 \\ -2 \\ 1 \end{bmatrix} \right\}$$

LinearSolve(B, v)

$$\begin{bmatrix} \frac{19}{2} \\ -2 \\ -\frac{1}{2} \end{bmatrix}$$

Standardmäßig werden Zahlen von Maple als rationale Zahlen interpretiert. Man kann aber auch mit Vektoren und Matrizen über einem endlichen Körper $\mathbb{Z}_p$ mit $p \in \mathbb{Z}$ prim rechnen. Funktionen dafür gibt es im Unterpaket LinearAlgebra/Modular.

Modular[Multiply]$(17, A, B)$

$$\begin{bmatrix} 6 & 0 & 0 \\ 15 & 4 & 5 \\ 7 & 8 & 10 \end{bmatrix}$$

Modular[Inverse]$(17, B)$

$$\begin{bmatrix} 3 & 6 & 9 \\ 14 & 4 & 16 \\ 1 & 7 & 9 \end{bmatrix}$$

2. *Mathematica.* Vektoren sind in Mathematica einfach die Listen ihrer Koordinaten. Eine Liste wird in Mathematica mit geschweiften Klammern geschrieben. Es handelt sich aber wirklich um Listen, nicht um Mengen, d. h. Reihenfolge und Vielfachheit von Elementen machen einen Unterschied. Vektoren kann man miteinander addieren oder mit einer Konstanten multiplizieren.

```
In[1]:= {1, 2, 3} == {1, 2, 3, 3}
Out[1]= False
In[2]:= {1, 2, 3} == {1, 3, 2}
Out[2]= False
In[3]:= v = {7, 4, -3}
Out[3]= {7, 4, -3}
In[4]:= Length[v]
Out[4]= 3
In[5]:= v[[2]]
Out[5]= 4
In[6]:= 5{1, 2, 3}
Out[6]= {5, 10, 15}
In[7]:= {1, 2, 3} + v
Out[7]= {8, 6, 0}
```

Matrizen werden in Mathematica als Listen von (Zeilen-)Vektoren dargestellt. Man kann Matrizen miteinander addieren und multiplizieren, oder mit Zahlen oder Vektoren multiplizieren. Außerdem gibt es Funktionen zum Transponieren, Invertieren, und zum Lösen von Gleichungssystemen.

```
In[8]:= A = {{1, 2, 3}, {4, 5, 6}, {7, 8, 9}}
Out[8]= {{1, 2, 3}, {4, 5, 6}, {7, 8, 9}}
In[9]:= A[[2, 3]]
Out[9]= 6
In[10]:= A.v
Out[10]= {6, 30, 54}
In[11]:= v.A
Out[11]= {2, 10, 18}
In[12]:= Transpose[A]
Out[12]= {{1, 4, 7}, {2, 5, 8}, {3, 6, 9}}
In[13]:= MatrixRank[A]
Out[13]= 2
```

In[14]:= **Nullspace[A]**

Out[14]= $\{\{1, -2, 1\}\}$

In[15]:= $B = \{\{1, 1, 1\}, \{1, 2, 3\}, \{1, 4, 9\}\}$

Out[15]= $\{\{1, 1, 1\}, \{1, 2, 3\}, \{1, 4, 9\}\}$

In[16]:= $2A - B$

Out[16]= $\{\{1, 3, 5\}, \{7, 8, 9\}, \{13, 12, 9\}\}$

In[17]:= $A.B$

Out[17]= $\{\{6, 17, 34\}, \{15, 38, 73\}, \{24, 59, 112\}\}$

In[18]:= **LinearSolve[B, v]**

Out[18]= $\{\frac{19}{2}, -2, -\frac{1}{2}\}$

In[19]:= $B.\% - v$

Out[19]= $\{0, 0, 0\}$

In[20]:= **Inverse[B]**

Out[20]= $\{\{3, -\frac{5}{2}, \frac{1}{2}\}, \{-3, 4, -1\}, \{1, -\frac{3}{2}, \frac{1}{2}\}\}$

Der Punkt beim Multiplizieren ist wesentlich: $A.B$ bedeutet Matrix-Matrix oder Matrix-Vektor-Multiplikation. Schreibt man $A * B$ oder AB, so werden die Einträge komponentenweise miteinander multipliziert – oder es gibt eine Fehlermeldung, falls das Format nicht passt. Vorsicht auch beim Potenzieren: Wenn man A^5 eingibt, nimmt Mathematica alle Einträge der Matrix einzeln hoch fünf, aber nicht die gesamte Matrix im Sinn der Matrixmultiplikation. Um das zu tun, verwendet man die Funktion **MatrixPower**

In[21]:= $A * B == A.B$

Out[21]= False

In[22]:= **A^5**

Out[22]= $\{\{1, 32, 243\}, \{1024, 3125, 7776\}, \{16807, 32768, 59049\}\}$

In[23]:= **MatrixPower[$A, 5$]**

Out[23]= $\{\{121824, 149688, 177552\}, \{275886, 338985, 402084\}, \{429948, 528282, 626616\}\}$

Standardmäßig interpretiert Mathematica Zahlen als rationale Zahlen. Will man stattdessen in einem endlichen Körper $\mathbb{Z}_p$ mit $p \in \mathbb{Z}$ prim rechnen, muss man den Modulus p der jeweiligen Funktion als optionales Argument mitgeben.

In[24]:= **Inverse[B, Modulus → 17]**

Out[24]= $\{\{3, 6, 9\}, \{14, 4, 16\}, \{1, 7, 9\}\}$

In[25]:= **LinearSolve[B, v, Modulus → 17]**

Out[25]= $\{1, 15, 8\}$

In[26]:= $\boldsymbol{B.\% - v}$

Out[26]= $\{17, 51, 136\}$

In[27]:= $\mathbf{Mod[\%, 17]}$

Out[27]= $\{0, 0, 0\}$

3. *Sage.* Dieses System basiert auf der Programmiersprache Python. Korrekter Python-Code ist (fast) immer auch korrekter Sage-Code. Darüber hinaus hat Sage einige Sprachkonstrukte, mit denen man mathematische Objekte beschreiben kann. Jedes solche Sage-Objekt ist entweder ein „Parent“ – dabei handelt es sich zum Beispiel um Gruppen, Ringe, Körper, Vektorräume – oder ein „Element“ – das sind Objekte, die zu einem Parent gehören.

```
2.parent()
```

Integer Ring

```
(1/3).parent()
```

Rational Field

```
v = vector(QQ, [7, 4, -3])
```

```
v
```

$(7, 4, -3)$

```
v.parent()
```

Vector space of dimension 3 over Rational Field

```
v[0]
```

7

```
A = matrix(QQ, [[1, 2, 3], [4, 5, 6], [7, 8, 9]])
```

```
B = matrix(QQ, [[1, 1, 1], [1, 2, 3], [1, 4, 9]])
```

```
A.parent()
```

Full MatrixSpace of 3 by 3 dense matrices over Rational Field

```
A[1, 2]
```

6

```
v * A
```

$(2, 10, 18)$

```
A * v
```

$(6, 30, 54)$

```
2 * A - B
```

$$\begin{pmatrix} 1 & 3 & 5 \\ 7 & 8 & 9 \\ 13 & 12 & 9 \end{pmatrix}$$

A.transpose()

$$\begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{pmatrix}$$

A.right_kernel()

Vector space of degree 3 and dimension 1 over Rational Field
Basis matrix:
(1 −2 1)

A.rank()

2

$A * B$

$$\begin{pmatrix} 6 & 17 & 34 \\ 15 & 38 & 73 \\ 24 & 59 & 112 \end{pmatrix}$$

A^5

$$\begin{pmatrix} 121824 & 149688 & 177552 \\ 275886 & 338985 & 402084 \\ 429948 & 528282 & 626616 \end{pmatrix}$$

B^(−1)

$$\begin{pmatrix} 3 & -5/2 & 1/2 \\ -3 & 4 & -1 \\ 1 & -3/2 & 1/2 \end{pmatrix}$$

B.solve_right(v)

$(19/2, -2, -1/2)$

Um über einem endlichen Körper zu rechnen, muss man bei der Erzeugung der Vektoren und Matrizen GF(p) für $\mathbb{Z}_p$ ($p \in \mathbb{Z}$ prim) statt QQ für $\mathbb{Q}$ angeben. Die Kommandos für die Rechnungen selbst ändern sich nicht.

$v = \text{vector}(\text{GF}(17), [7, 4, -3])$

$A = \text{matrix}(\text{GF}(17), [[1, 2, 3], [4, 5, 6], [7, 8, 9]])$

$A.v$

$(6, 13, 3)$

A.right_kernel()

Vector space of degree 3 and dimension 1 over Finite Field of size 17
Basis matrix:
(1 15 1)

Systeme wie Maple, Mathematica und Sage stellen tausende mathematische Funktionen bereit. Allein die Funktionen, die etwas mit linearer Algebra zu tun haben, sind zu zahlreich, um sie alle hier zu erwähnen. Einen vollständigen Überblick finden Sie in den Dokumentationen dieser Systeme.

Index