Vorlesung Lineare Algebra I - WS 2019-20

Prof. A. Rosenschon

1. Mengen und Abbildungen

Definition 1.1. Eine Menge M ist eine Zusammmenfassung von gewissen Objekten, den sogenannten Elementen von M. Die leere Menge $\emptyset$ ist die Menge, die kein Objekt enthält.

NB. Diese erste Definition ist nicht präzise; eine genaue Festlegung des Begriffs einer Menge, und der mit Mengen zulässigen Operationen, erfordert eine axiomatische Begründung der Mengenlehre, die für eine Einführung in die lineare Algebra nicht angebracht ist. Wir verwenden daher nur die obige, naive Definition.

- $m \in M$: m ist Element von M,
- $m \notin M$: m ist kein Element von M,
- $M = \{m_1, m_2, \dots\}$: M ist die Menge mit den Elemente $m_1, m_2 \dots$,
- $M = \{x \mid x \text{ erfüllt Eigenschaft } P\}$: Menge der x mit Eigenschaft P.

Beispiele 1.2. (a) $\mathbb{N} = \{1, 2, 3, \dots\}$ Menge der natürlichen Zahlen; $\mathbb{N}_0 = \{0, 1, 2, \dots\}$ die Menge der natürlichen Zahlen einschliesslich 0.
(b) $\mathbb{Z} = \{\dots, -1, 0, 1, 2, \dots\}$ Menge der ganzen Zahlen.
(c) $\mathbb{Q} = \{p/q \mid p, q \in \mathbb{Z},\ q \neq 0\}$ Menge der rationalen Zahlen.
(d) $\mathbb{R}$ Menge der reellen Zahlen.

Definition 1.3. Sei M eine Menge.
(a) Eine Menge N ist eine Untermenge (oder Teilmenge) von M, $N \subseteq M$, falls jedes Element von N in M liegt. Ist $N \subseteq M$ und gibt es wenigstens ein $m \in M$ mit $m \notin N$, so schreibe $N \subsetneq M$. Zwei Mengen M, N sind gleich, $M = N$, wenn $N \subseteq M$ und $M \subseteq N$ gilt. Die Potenzmenge $P(M)$ ist die Menge aller Teilmengen von M; es ist $\emptyset \in P(M)$.
(b) Seien $N_j \subseteq M, j \in J$, J eine nichtleere Indexmenge (nicht unbedingt endlich). Die Vereinigung und der Durchschnitt der N_j sind definiert als die Mengen

$$\begin{aligned} \bigcup_{j\in J} N_j &= \{m \in M \mid m \in N_j \text{ für ein } j\}, \\ \bigcap_{j\in J} N_j &= \{m \in M \mid m \in N_j \text{ für alle } j\}. \end{aligned}$$

Ist $J = \emptyset$, so setze $\cup_j N_j = \emptyset$ und $\cap_j N_j = M$.
(c) Ist $N_j \subseteq M, j = 1, 2$, so ist die Differenz von N_1 und N_2 die Menge

$$N_1 \setminus N_2 = \{n_1 \in N_1 \mid n_1 \notin N_2\}.$$

(d) Seien $M_i \neq \emptyset, i = 1, \dots, k$ Mengen. Betrachte geordnete k-Tupel $(m_1, \dots, m_k), m_i \in M_i$, d.h. $(m_1, \dots, m_k) = (m'_1, \dots, m'_k) \Leftrightarrow m_i = m'_i$

für $i = 1, \ldots, k$. Das (kartesische) Produkt der M_i ist definiert als

$$M_1 \times \cdots \times M_k = \{(m_1, \ldots, m_k) \mid m_i \in M_i \}.$$

Seien A, B, C, N_j für $j \in J$ Teilmengen einer Menge M. Dann gilt:

- $A \cup B = B \cup A$ und $A \cap B = B \cap A$.
- $A \cup (B \cup C) = (A \cup B) \cup C$ und $A \cap (B \cap C) = (A \cap B) \cap C$.
- $A \cap (\cup_j N_j) = \cup_j (A \cap N_j)$ und $A \cup (\cap_j N_j) = \cap_j (A \cup N_j)$.

Beispiel 1.4. Sei $M = \mathbb{N}$, $N_1, N_2 \subseteq M$ die Mengen $N_1 = \{1\}$ und $N_2 = \{1, 2\}$. Dann ist $N_1 \cup N_2 = \{1, 2\}$, $N_1 \cap N_2 = \{1\}, N_1 \setminus N_2 = \emptyset, N_2 \setminus N_1 = \{2\}, N_1 \times N_2 = \{(1, 1), (1, 2)\}$ und $N_2 \times N_1 = \{(1, 1), (2, 1)\}$.

Definition 1.5. Sei M eine Menge und $N_j \subseteq M, j \in J$, Teilmengen. Die N_j bilden eine Partition von M, falls jedes $m \in M$ in genau einer der Teilmengen N_j liegt d.h. falls gilt

$$M = \cup_j N_j \text{ und } N_j \cap N_k = \emptyset \text{ für } j \neq k, \ j, k \in J.$$

Beispiel 1.6. Sei $N \subseteq M$ und $\overline{N} = M \setminus N$ (d.h. $\overline{N}$ ist das Komplement von N in M). Dann bilden N und $\overline{N}$ eine Partition von M.

Wir wollen Partitionen einer Menge charakterisieren. Ist $M = \cup_j N_j$ eine Partition, so nennen wir zwei Elemente $m, m' \in M$ äquivalent, $m \sim m'$, falls $m, m' \in N_j$ für ein j gilt. Für $m, m', m'' \in M$ folgt:

(i) $m \sim m$,
(ii) $m \sim m' \Rightarrow m' \sim m$,
(iii) $m \sim m'$ und $m' \sim m'' \Rightarrow m \sim m''$.

Wir zeigen, dass umgekehrt (i)-(iii) eine Partition bestimmen.

Definition 1.7. (a) Eine Relation R auf einer Menge M ist eine Teilmenge $R \subseteq M \times M$. Sind $m, m' \in M$ und gilt $(m, m') \in R$, so schreibe mRm' (m und m' stehen zueinander in Relation R).

(b) Eine Relation R auf einer Menge M ist eine Äquivalenzrelation, falls für alle Elemente $m, m', m'' \in M$ gilt:

(i) mRm (Reflexivität),
(ii) $mRm' \Rightarrow m'Rm$ (Symmetrie),
(iii) mRm' und $m'Rm'' \Rightarrow mRm''$ (Transitivität)

Ist R eine Äquivalenzrelation, so schreibe $\sim$ für R und $m \sim m'$ für mRm'; die Menge der zu einem $m \in M$ äquivalenten Elemente bildet die Äquivalenzklasse $[m]$ von m:

$$[m] = \{m' \in M \mid m \sim m'\} \subseteq M.$$

Lemma 1.8. *Sei M eine Menge und $\sim$ eine Äquivalenzrelation auf M. Dann gilt für $m, m' \in M$ entweder $[m] \cap [m'] = \emptyset$ oder $[m] = [m']$;*

die verschiedenen Äquivalenzklassen bezüglich $\sim$ bilden eine Partition von M.

NB. Partition von $M \leftrightarrow$ Äquivalenzrelation auf M.

Beweis. Klar ist $\cup_m [m] \subseteq M$. Wegen (i) gilt für $m \in M$ stets $m \in [m]$, also ist auch $M \subseteq \cup_m [m]$ und somit $M = \cup_m [m]$. Sei $\emptyset \neq [m] \cap [m']$, zu zeigen ist $[m] = [m']$. Ist $m_0 \in [m] \cap [m']$, so gilt $m_0 \sim m$ und $m_0 \sim m'$. Sei $m_1 \in [m]$, d.h. $m_1 \sim m$. Wegen (ii) folgt aus $m_0 \sim m$ auch $m \sim m_0$, und (iii) angewandt auf $m_1 \sim m$ und $m \sim m_0$ liefert $m_1 \sim m_0$. Nochmalige Anwendung von (iii) auf $m_1 \sim m_0$ und $m_0 \sim m'$ zeigt $m_1 \sim m'$, also ist $m_1 \in [m']$ und $[m] \subseteq [m']$. Aus Symmetriegründen (vertauschen der Rollen von m und m') folgt genauso die umgekehrte Inklusion $[m'] \subseteq [m]$, d.h. es gilt $[m] = [m']$. □

Beispiele 1.9. (a) Sei $M = \mathbb{R}^2$ und $L \subseteq M$ die Menge der Geraden in M. Für $l_1, l_2 \in L$ definiert

$$l_1 \sim l_2 \Leftrightarrow l_1 \,||\, l_2 \quad \text{(d.h. die Geraden sind parallel)}$$

eine Äquivalenzrelation auf L.

(b) Sei $M = \mathbb{Z}$ und $m \geq 1$ eine ganze Zahl. Für $n_1, n_2 \in \mathbb{Z}$ definiere

$$n_1 \equiv n_2 (mod\ m) \Leftrightarrow m | (n_1 - n_2).$$

Dann definiert $\equiv$ eine Äquivalenzrelation auf $\mathbb{Z}$:

(i) $n \equiv n (mod\ m)$, wegen $m | n - n = 0$,

(ii) $n_1 \equiv n_2 (mod\ m)$ heisst $n_1 - n_2 = km$ für ein $k \in \mathbb{Z}$; in diesem Fall folgt $-km = n_2 - n_1$, d.h. $n_2 \equiv n_1 (mod\ m)$.

(iii) Ist $n_1 \equiv n_2 (mod\ m)$, $km = n_1 - n_2$ und $n_2 \equiv n_3 (mod\ m)$, $lm = n_2 - n_3$, so folgt $(k+l)m = n_1 - n_3$, also $n_1 \equiv n_3 (mod\ m)$.

Sei $\mathbb{Z}/m\mathbb{Z}$ die Menge der Äquivalenzklassen dieser Äquivalenzrelation

$$\mathbb{Z}/m\mathbb{Z} = \{[r] \mid r \in \mathbb{Z}\} = \{\{r + mk \mid k \in \mathbb{Z}\}\}.$$

Nach Lemma 1.8 bilden die *verschiedenen* Äquivalenzklassen eine Partition von $\mathbb{Z}$; dies sind die Mengen $[r]$ für $0 \leq r < m$ (d.h. die verschiedenen Äquivalenzklassen entsprechen den möglichen Resten bei 'Division durch m' und werden daher auch 'Restklassen' genannt).

Ist $m = 2$, so besteht die Restklasse $[0]$ aus den geraden und die Restklasse $[1]$ aus den ungeraden ganzen Zahlen, d.h. $\mathbb{Z}/2\mathbb{Z} = \{[0], [1]\}$ und die entsprechene Partition von $\mathbb{Z}$ hat die Form

$$\mathbb{Z} = [0] \cup [1] = \{\text{geraden ganzen Zahlen}\} \cup \{\text{ungerade ganze Zahlen}\}.$$

Definition 1.10. Seien $M \neq \emptyset \neq N$ Mengen.

(a) Eine Abbildung f von M nach N, $f : M \to N$, ordnet jedem

$m \in M$ genau ein $n \in N$ zu; im Fall $f : m \mapsto n$ schreibe $f(m) = n$ (genauer: eine Abbildung ist eine Teilmenge $F \subseteq M \times N$, so dass es für jedes $m \in M$ genau ein $n \in N$ mit $(m, n) \in F$ gibt; in diesem Fall definiere $f(m) = n$). Zwei Abbildungen $f, g : M \to N$ sind gleich, $f = g$, falls $f(m) = g(m)$ für alle $m \in M$ gilt. Setze

$$\mathrm{Abb}(M, N) = \{f \mid f : M \to N \text{ Abbildung } \}.$$

(b) Die Identitätsabbildung auf M ist definiert durch $\mathrm{id}_M : M \to M,\ \mathrm{id}_M(m) = m$ für $m \in M$.

(c) Seien M_i nichtleere Mengen, $i = 1, 2, 3,\ f \in \mathrm{Abb}(M_1, M_2)$ und $g \in \mathrm{Abb}(M_2, M_3)$. Das Kompositum $g \circ f$ von f und g ist die Abbildung

$$g \circ f : M_1 \to M_3,\ m_1 \mapsto g(f(m_1)),\ m_1 \in M_1.$$

• Für $f \in \mathrm{Abb}(M_1, M_2),\ g \in \mathrm{Abb}(M_2, M_3)$ und $h \in \mathrm{Abb}(M_3, M_4)$ gilt: $h \circ (g \circ f) = (h \circ g) \circ f$ (d.h. die Bildung von $\circ$ ist assoziativ).

• Ist $f \in \mathrm{Abb}(M, N)$, so gilt $f = \mathrm{id}_N \circ f$ und $f = f \circ \mathrm{id}_M$.

Definition 1.11. Seien $M \neq \emptyset \neq N$ Mengen und $f \in \mathrm{Abb}(M, N)$.

(a) Ist $U \subseteq M$, so ist das Bild von U unter f die Menge

$$f(U) = \{f(u) \mid u \in U \} \subseteq N.$$

(b) Ist $V \subseteq N$, so ist das Urbild von V unter f die Menge

$$f^{-1}(V) = \{m \mid f(m) \in V \} \subseteq M.$$

(c) f ist surjektiv, falls $f(M) = N$ gilt, d.h. zu jedem $n \in N$ gibt es ein $m \in M$ mit $f(m) = n$.

(d) f ist injektiv, falls aus $f(m_1) = f(m_2)$ mit $m_1, m_2 \in M$ stets $m_1 = m_2$ folgt; in diesem Fall besteht das Urbild eines jeden $n \in N$ aus maximal einem Element.

(e) f ist bijektiv, falls f injektiv und surjektiv ist.

Lemma 1.12. *Seien $M \neq \emptyset \neq N$ Mengen und sei $f \in \mathrm{Abb}(M, N)$.*

(a) f ist genau dann injektiv, wenn es ein $g \in \mathrm{Abb}(N, M)$ gibt, sodass gilt: $g \circ f = \mathrm{id}_M$.

(b) f ist genau dann surjektiv, wenn es ein $g \in \mathrm{Abb}(N, M)$ gibt, sodass gilt: $f \circ g = \mathrm{id}_N$.

(c) f ist genau dann bijektiv, wenn es ein $g \in \mathrm{Abb}(N, M)$ mit

$$g \circ f = \mathrm{id}_M \text{ und } f \circ g = \mathrm{id}_N$$

gibt; in diesem Fall ist g eindeutig bestimmt und ebenfalls bijektiv.

Beweis. Übung. □

Definition 1.13. Sei $f \in \mathrm{Abb}(M, N)$ bijektiv. Dann gibt es nach Lemma 1.12 eine eindeutig bestimmte Abbildung $g \in \mathrm{Abb}(N, M)$, sodass gilt: $g \circ f = \mathrm{id}_N$ und $f \circ g = \mathrm{id}_M$. In diesem Fall ist g ebenfalls bijektiv; $g = f^{-1}$ ist die zu f inverse Abbildung.

• Seien $f \in \mathrm{Abb}(M_1, M_2)$ und $g \in \mathrm{Abb}(M_2, M_3)$ bijektiv. Dann ist auch $g \circ f$ bijektiv und es gilt: $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. Genauer: Da die Bildung des Kompositums von Abbildungen assoziativ ist, gilt

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ (f \circ (f^{-1} \circ g^{-1})) = g \circ ((f \circ f^{-1}) \circ g^{-1}) = \\ = g \circ (\mathrm{id}_{M_2} \circ g^{-1}) = g \circ g^{-1} = \mathrm{id}_{M_3};$$

ähnlich folgt $(f^{-1} \circ g^{-1}) \circ (g \circ f) = \mathrm{id}_{M_1}$. Nach Lemma 1.12(c) ist daher $g \circ f$ bijektiv und $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Bemerkung 1.14. Zwei Mengen M, N sind *gleichmächtig*, falls es eine Bijektion von M auf N gibt, in diesem Fall schreibe $|M| = |N|$. Ist $M = \emptyset$, so setzte $|M| = 0$. Eine Menge M ist endlich, falls $M = \emptyset$ oder es eine Bijektion von M auf $\{1, \dots n\} \subseteq \mathbb{N}$ für ein geeignetes $n \in \mathbb{N}$ gibt. In diesem Fall ist n durch M eindeutig bestimmt, und $|M| = n$. Für endliche Mengen gilt: Ist $N \subseteq M$ und $|N| = |M|$, so ist $N = M$.

Für *unendliche* Mengen, d.h. nicht endliche Mengen, gilt dies nicht. Zum Beispiel, es ist $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q}$, aber $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}|$; Mengen mit der Eigenschaft, dass $|M| = |\mathbb{N}|$ gilt heissen *abzählbar* unendlich; die Menge $\mathbb{R}$ ist nicht abzählbar unendlich.

Die Frage, ob für eine unendliche Teilmenge $M \subseteq \mathbb{R}$ entweder $|M| = |\mathbb{N}|$ oder $|M| = |\mathbb{R}|$ gilt wurde von D. Hilbert 1900 als die *Kontinuumshypothese* formuliert. P. Cohen zeigte 1963, dass sich diese Frage mit den üblichen Axiomen der Mengenlehre weder beweisen noch widerlegen lässt.

Lemma 1.15. *Seien M, N nichtleere endliche Mengen mit $|M| = |N|$ und sei $f \in \mathrm{Abb}(M, N)$. Dann sind gleichwertig:*

(a) *f ist bijektiv,*
(b) *f ist injektiv,*
(c) *f ist surjektiv.*

NB. Das obige Lemma gilt nicht für unendlichen Mengen: Zum Beispiel, die Abbildung $f : \mathbb{Z} \to \mathbb{Z}$, $f(n) = 2n$ ist eine Abbildung zwischen zwei (unendlichen) Mengen der gleichen Mächtigkeit, und ist injektiv, aber nicht surjektiv.

Beweis. (a)⇒(b): Trivial nach Definition. (b)⇒ (c): Da f injektiv ist, gilt $|M| = |f(M)|$, und wegen $|M| = |N|$ ist somit $|f(M)| = |N|$. Da $f(M) \subseteq N$ und $|M| = |N|$ endlich ist, folgt $f(M) = N$, also ist f

surjektiv. (c)⇒ (a): Für $n_1, n_2 \in N$, $n_1 \neq n_2$, ist $f^{-1}(n_1) \cap f^{-1}(n_2) = \emptyset$, d.h. die Urbilder $f^{-1}(n)$ der $n \in N$ definieren eine Partition von M

$$M = \bigcup_{n \in N} f^{-1}(n).$$

Da f surjektiv ist, gilt $|f^{-1}(n)| \geq 1$ für alle $n \in N$, damit folgt

$$|M| = |\bigcup_{n \in N} f^{-1}(n)| = \sum_{n \in N} |f^{-1}(n)| \geq \sum_{n \in N} 1 = |N|.$$

Da nach Annahme $|N| = |M|$ gilt, folgt $|f^{-1}(n)| = 1$ für $n \in N$, d.h. f ist injektiv. □

Lemma 1.16. *Sei $f : M \to N$ eine Abbildung und seien $M_1, M_2 \subseteq M$ und $N_1, N_2 \subseteq N$ Teilmengen. Dann gilt:*

(a) $f(M_1 \cup M_2) = f(M_1) \cup f(M_2)$,
(b) $f(M_1 \cap M_2) \subseteq f(M_1) \cap f(M_2)$,
(c) $f^{-1}(N_1 \cup N_2) = f^{-1}(N_1) \cup f^{-1}(N_2)$,
(d) $f^{-1}(N_1 \cap N_2) = f^{-1}(N_1) \cap f^{-1}(N_2)$.

Beweis. Übung. □

2. Gruppen I

Eine Menge G hat die Struktur einer (abelschen) Gruppe, wenn es eine 'Addition' mit den Eigenschaften der Addition in den ganzen Zahlen $\mathbb{Z}$ gibt; allgemein ist eine Gruppenstruktur auf einer Menge eine (nicht unbedingt kommutative) 'Verknüpfung' von Elementen mit den folgenden Eigenschaften:

Definition 2.1. Sei G eine nichtleere Menge. Eine Verknüpfung $\cdot$ auf G ist eine Abbildung $\cdot : G \times G \to G$, d.h. $\cdot$ ordnet jedem geordneten Paar $(a, b) \in G \times G$ ein Element $c \in G$ zu; schreibe $c = a \cdot b$. Eine Menge G, zusammen mit einer Verknüfung $\cdot$ ist eine Gruppe, falls gilt:

(1) $\cdot$ ist assoziativ: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ für alle $a, b, c \in G$.
(2) es gibt ein (links)-neutrales Element $e \in G$ mit $e \cdot a = a$ für alle $a \in G$.
(3) zu jedem $a \in G$ gibt es ein (links)-inverses Element, d.h. ein $b \in G$ mit $b \cdot a = e$.

Die Gruppen G ist kommutativ oder abelsch, falls zusätzlich gilt:

(4) $a \cdot b = b \cdot a$ für $a, b \in G$.

NB. Ist $(G, \cdot)$ eine abelsche Gruppe, so schreibt man oft $a + b$ anstelle von $a \cdot b$ (analog zu der kommutativen Addition $+$ in $\mathbb{Z}$).

• Aufgrund des Assoziativgesetzes (1) lassen sich Produkte von Elementen in einer Gruppe $(G, \cdot)$ beliebig klammern. Seien $a, b, c \in G$ mit $ba = b \cdot a = e$ und $cb = c \cdot b = e$. Dann gilt

$$ab = (ea)b = ((cb)a)b = (c(ba))b = (ce)b = c(eb) = cb = e,$$

d.h. $ba = e$ impliziert $ab = e$ (das links-inverse Element ist auch ein rechts-inverses Element). Weiter folgt damit auch

$$ae = a(ba) = (ab)a = ea = a,$$

also liefert $ea = a$ auch $ae = a$ (das links-neutrale Element e ist auch ein rechts-neutrales Element).

• Ist $(G, \cdot)$ eine Gruppe, so schreibe $e = 1$ (Einselement) und $b = a^{-1}$ für das zu a inverse Element. Sind $a_1, a_2, \ldots, a_n \in G$, so schreibe $\prod_{i=1}^{n} a_i = a_1 \cdot \cdots \cdot a_n$; nach Definition gilt $\prod_{i=1}^{0} a_i = 1$.

Ist $(G, +)$ eine abelsche Gruppe, so setze $e = 0$ (Nullelement) und bezeichne das zu a inverse Element mit $-a$. In diesem Fall bezeichnet $\sum_{i=1}^{n} a_i$ die Summe der endlich vielen Elemente $a_1, \ldots, a_n$; nach Definition ist $\sum_{i=1}^{0} a_i = 0$.

Beispiele 2.2. (a) $(\mathbb{Z}, +)$ ist abelsche Gruppe (übliche Addition).

(b) $(\mathbb{Q}, +)$ und $(\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}, \cdot)$ (übliche Addition und Multiplikation) sind abelsche Gruppen, genauso für $(\mathbb{R}, +)$ und $(\mathbb{R}^\times = \mathbb{R} \setminus \{0\}, \cdot)$.

(c) Die Menge $\mathbb{Z}[x]$ der Polynome in einer Variablen x mit ganzzahligen Koeffizienten bildet eine abelsche Gruppe mittels der Addition

$$f = \sum_{i=0}^{n} a_i x^i, g = \sum_{j=0}^{m} b_j x^j \Rightarrow f + g = \sum_{k=0}^{n+m} (a_k + b_k) x^k;$$

genauso ist die Menge solcher Polynome mit rationalen Koeffizienten $\mathbb{Q}[x]$ bzw. reellen Koeffizienten $\mathbb{R}[x]$ eine abelsche Gruppe.

(d) Sei M eine Menge und $\mathrm{Bij}(M)$ die Menge der bijektiven Abbildungen $M \to M$. Dann bildet $\mathrm{Bij}(M)$ mittels der Komposition $\circ$ von Abbildungen einer Gruppe: Sind $f, g \in \mathrm{Bij}(M)$, so ist auch $g \circ f \in \mathrm{Bij}(M)$, das neutrale Element ist die Identitätsabbildung id_M, und das zu einem $f \in \mathrm{Bij}(M)$ inverse Element ist die inverse Abbildung f^{-1}.

Ist $M = \{1, \ldots, n\} \subseteq \mathbb{N}$, so schreibe $S_n = \mathrm{Bij}(M)$; im Fall $n \geq 3$, ist die Gruppe S_n nicht abelsch.

(e) Sei $m \geq 1$ eine ganze Zahl. Für $a \in \mathbb{Z}$ betrachte die Äquivalenzklasse

$$[a] = \{a + mk \mid k \in \mathbb{Z}\} = a + m\mathbb{Z} \subseteq \mathbb{Z}$$

derjenigen Elemente von $\mathbb{Z}$, die zu a kongruent modulo m sind. Setze

$$[a] + [b] = [a + b],$$

d.h. definiere '+' auf den Äquivalenzklassen durch den Ausdruck auf der rechten Seite. Diese Addition von $[a]$ und $[b]$ ist wohl-definiert:

Ist $[a_1] = [a_2], a_1 - a_2 = km$ und $[b_1] = [b_2], b_1 - b_2 = lm$, so folgt $a_1+b_1-(a_2+b_2) = a_1-a_2+(b_1-b_2) = (k+l)m$, d.h. $[a_1+b_1] = [a_2+b_2]$.

Aus den Eigenschaften der Addition in $\mathbb{Z}$ ergibt sich, dass die Menge

$$\mathbb{Z}/m\mathbb{Z} = \{[a] = a + m\mathbb{Z} \mid a \in \mathbb{Z}\}$$

bzgl. der oben definierten Verknüpfung + die Struktur einer abelschen Gruppe mit neutralem Element $[0]$ hat; es ist $|\mathbb{Z}/m\mathbb{Z}| = m$.

Das nächste Lemma liefert elementare Rechenregeln in Gruppen:

Lemma 2.3. *Sei $(G, \cdot)$ eine Gruppe, $a, b, c \in G$.*

(a) $ab = ac \Rightarrow b = c$ *und* $ac = bc \Rightarrow a = b$,
(b) $(a^{-1})^{-1} = a$,
(c) $(ab)^{-1} = b^{-1}a^{-1}$.

Beweis. (a): Ist $ab = ac$, so liefert Multiplikation mit a^{-1} von links $a^{-1}(ab) = a^{-1}(ac)$ Wegen $a^{-1}(ab) = (a^{-1}a)b = eb = b$ und $a^{-1}(ac) = c$ folgt $b = c$; analog mit Multiplikation mit c^{-1} von rechts für den zweiten Fall. (b): Nach Definiton ist $(a^{-1})^{-1}a^{-1} = e$, Multiplikation mit a von rechts liefert $(a^{-1})^{-1} = a$. (c): Wegen $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}(eb) = b^{-1}b = e$ ist $(ab)^{-1} = b^{-1}a^{-1}$. □

Eine Untergruppe $H \subseteq G$ einer Gruppe G (bzgl. $\cdot$) ist eine Teilmenge, sodass die Einschränkung von $\cdot$ auf H eine Gruppenstruktur auf H definiert, insbesondere muss dazu das Produkt von zwei Elementen aus H in H liegen, und H alle Inversen und die 1 enthalten; genauer:

Definition 2.4. Sei G eine Gruppe. Eine Teilmenge $H \subseteq G$ ist eine Untergruppe von G, $H \leq G$, falls gilt

(a) $1 \in H$
(b) $a, b \in H \Rightarrow ab \in H$
(c) $a \in H \Rightarrow a^{-1} \in H$.

NB. Ist $\emptyset \neq H \subseteq G$ eine *nichtleere* Teilmenge, so lassen sich die Kriterien (a)-(c) der obigen Definition zu einer Bedingung vereinfachen:

$$\emptyset \neq H \subseteq G \text{ ist Untergruppe, falls gilt: } a, b \in H \Rightarrow ab^{-1} \in H.$$

Konkret: Wegen $\emptyset \neq H$ gibt es ein $a \in H$ und die Bedingung impliziert $aa^{-1} = 1 \in H$, somit gilt (a). Ist $a \in H$ beliebig, so folgt aus $1 \in H$ nun $1a^{-1} = a^{-1} \in H$, also gilt (c). Da mit $a, b \in H$ auch $a, b^{-1} \in H$ ist, ist $a(b^{-1})^{-1} = ab \in H$, dies ist (b).

Beispiele 2.5. (a) In jeder Gruppe G gilt: $\{1\} \leq G$ und $G \leq G$ (die Untergruppen $\{1\}$ und G sind die trivalen Untergruppen von G).

(b) Als additiven Gruppen: $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R}$.

(c) Für die additiven Gruppen der Polynome mit ganzzahligen, rationalen und reellen Koeffizienten: $\mathbb{Z}[x] \leq \mathbb{Q}[x] \leq \mathbb{R}[x]$.

(d) Sei $m \geq 1$ eine ganze Zahl und $m\mathbb{Z} = \{mk \mid k \in \mathbb{Z}\} \subseteq \mathbb{Z}$. Dann ist $m\mathbb{Z} \leq \mathbb{Z}$ eine Untergruppe (für $m \geq 2$ ist $m\mathbb{Z} \subsetneq \mathbb{Z}$ und $|m\mathbb{Z}| = |\mathbb{Z}|$).

Nach Beispiel 2.5(d) bilden für eine ganze Zahl $m \geq 1$ die m-Vielfachen $m\mathbb{Z} \subseteq \mathbb{Z}$ eine Untergruppe von $\mathbb{Z}$. Nach Beispiel 1.9(b) definiert

$$n_1 \equiv n_2 (mod\ m) \Leftrightarrow m|(n_1 - n_2),\ n_1, n_2 \in \mathbb{Z}$$

eine Äquivalenzrelation auf $\mathbb{Z}$.

Schreibt man die additive Gruppenoperation in $G = \mathbb{Z}$ multiplikativ und setzt man $U = m\mathbb{Z} \leq \mathbb{Z}$, so entspricht der additiven Relation $m|(n_1 - n_2)$ die multiplikative Relation $n_1 n_2^{-1} \in U$. Wir zeigen, dass diese multiplikative Relation bzgl. einer Untergruppe $U \leq G$ allgemein eine Äquivalenzrelation auf G definiert:

Lemma 2.6. *Sei G eine Gruppe und $U \leq G$ eine Untergruppe. Dann definiert $a \sim b \Leftrightarrow ab^{-1} \in U$ $(a, b \in G)$ eine Äquivalenzrelation auf G.*

Beweis. Wegen $aa^{-1} = 1 \in U$ gilt $a \sim a$. Ist $a \sim b$, also $ab^{-1} \in U$, so folgt $(ab^{-1})^{-1} = ba^{-1} \in U$, d.h. $b \sim a$. Ist $a \sim b$ und $b \sim c$, so gilt $ab^{-1} \in U$ und $bc^{-1} \in U$. Es folgt $ac^{-1} = (ab^{-1})(bc^{-1}) \in U$ und so $a \sim c$. □

Definition 2.7. Sei G eine Gruppe, $U \leq G$ eine Untergruppe, und $\sim$ die durch U definierte Äquivalenzrelation auf G $(a \sim b \Leftrightarrow ab^{-1} \in U)$. Ist $a \in G$, so ist die entsprechende Äquivalenzklasse die Menge

$$[a] = \{b \in G \mid a \sim b\} = \{b \in G \mid ab^{-1} \in U\} = \{b \in G \mid b = Ua\} = Ua;$$

diese Mengen sind die Rechtsnebenklassen von U. Sind die Ua_j für $j \in J$ die verschiedenen Rechtsnebenklassen, so bilden diese eine Partition

$$G = \bigcup_{j \in J} Ua_j.$$

Ist $|J|$ endlich, so ist $|J|$ der Index von U in G; schreibe $|J| = |G : U|$.

• Genauso definiert $a \sim b \Leftrightarrow a^{-1}b \in$ eine Äquivalenzrelation auf G. Die Äquivalenzklasse von $a \in G$ ist die Linksnebenklasse

$$[a] = \{b \in G \mid a \sim nb\} = \{b \in G \mid a^{-1}b \in U\} = aU.$$

Ist G abelsch, so gilt $aU = Ua$; für eine nicht-abelsche Gruppe gilt dies im allgemeinen nicht.

• Der Versuch analog zur Definition der Addition auf $\mathbb{Z}/m\mathbb{Z}$ mittels der Addition auf $\mathbb{Z}$ eine Verknüpfung auf der Menge der Nebenklassen

$G/U = \{Ua \mid a \in G\}$ durch $Ua \cdot Ub = Uab$ zu definieren funktioniert für abelsche Gruppen, aber nicht für allgemeine Gruppen. Dies wird uns zu besonderen Untergruppen führen, den sogenannten Normalteilern.

Wir geben ein einfaches Kriterium für die Existenz von Untergruppen einer endlichen Gruppe:

Theorem 2.8. *(Satz von Lagrange) Sei G eine endliche Gruppe (d.h. die Menge G ist endlich) und $U \leq G$ eine Untergruppe. Dann gilt:*

$$|G| = |G : U||U|.$$

NB. Das Theorem besagt: Gibt es eine Untergruppe $U \leq G$, so ist $|U|$ ein Teiler von $|G|$; dies ist eine notwendige Bedingung für die Existenz von Untergruppen; zum Beispiel kann eine Gruppe G mit Primzahlordnung $|G| = p$ nur die trivialen Untergruppen $\{1\}$ und G enthalten.

Beweis. Betrachte die Partition $G = \cup_j Ua_j$. Für $a \in G$ ist die Abbildung $U \to Ua,\ u \mapsto ua$ surjektiv (ist $ua \in Ua$, so gilt $u \mapsto ua$) und injektiv (ist $u_1 a = u_2 a$, so folgt $u_1 = u_2$), also eine Bijektion. Es folgt $|aU| = |U|$ und $|G| = |J||U| = |G : U||U|$. □

Bemerkung 2.9. Die Umkehrung des Satzes von Lagrange gilt nicht, d.h. im allgemeinen gibt es zu einem Teiler der Gruppenordnung $|G|$ einer endlichen Gruppe keine Untergruppe dieser Ordnung. Ein grundlegendes Resultat in diesem Kontext ist das folgende Theorem von Sylow:

Sei G eine endliche Gruppe, $|G| = n$ und p eine Primzahl die n teilt. Sei p^m die maximale p-Potenz in n. Dann gibt es eine Untergruppe $U \leq G$ mit $|U| = p^m$.

Zum Beispiel: Jede Gruppe G mit $|G| = 24 = 3 \cdot 2^3$ besitzt (zumindestens eine) Untergruppe $U \leq G$ mit $|U| = 3$ und eine Untergruppe $V \leq G$ mit $|V| = 2^3 = 8$.

3. Körper

Ein Körper ist eine additiv geschriebene abelsche Gruppe, auf der zusätzlich eine Multiplikation definiert ist, die die Eigenschaften der Multiplikation von rationalen Zahlen erfüllt.

Definition 3.1. Ein Körper K ist eine Menge mit zwei Verknüpfungen $+$ und $\cdot$, für die gilt:

(1) $(K, +)$ ist eine abelsche Gruppe mit Nullelement 0,

(2) $(K \setminus \{0\}, \cdot)$ ist eine abelsche Gruppen mit Einselement $1 \neq 0$,

(3) $a \cdot (b + c) = a \cdot b + a \cdot c$ und $(a + b) \cdot c = a \cdot c + a \cdot b$.

In Körpern gelten viele der 'üblichen' Rechenregeln. Für $a, b \in K$ ist:

- $0a = a0 = 0$,
- $(-1)a = -a$,
- $(-a)b = a(-b) = -ab$,
- $ab = 0 \Rightarrow a = 0$ oder $b = 0$.

NB. Nicht alle Eigenschaften der rationalen Zahlen gelten für allgemeine Körper. Zum Beispiel, in $\mathbb{Q}$ folgt für $n \in \mathbb{N}$ und $a \in \mathbb{Q}$ aus $n \cdot a = (1 + \cdots + 1) \cdot a = 0$ stets $a = 0$, aber es gibt Körper mit der Eigenschaft, dass $n \cdot a = 0$ für $n \neq 0$ und $a \neq 0$.

Beispiele 3.2. (a) $\mathbb{Q}$ und $\mathbb{R}$ sind Körper.

(b) Sei p eine Primzahl und $\mathbb{Z}/p\mathbb{Z}$ die Menge der Restklassen modulo p. Dann bildet $\mathbb{Z}/p\mathbb{Z}\backslash\{[0]\}$ bzgl. der evidenten Multiplikation $[a]\cdot[b] = [ab]$ eine abelsche Gruppe, d.h. $\mathbb{Z}/p\mathbb{Z}$ ist ein Körper mit p Elementen; siehe Übung. In $\mathbb{Z}/p\mathbb{Z}$ gilt $pa = 0$ für alle $a \in \mathbb{Z}/p\mathbb{Z}$.

Analog zur Definition einer Untergruppe einer Gruppe ist ein Unterkörper oder Teilkörper eines Körpers K eine Teilmenge $L \subseteq K$ mit der Eigenschaft, dass sich $+$ und $\cdot$ auf K zu Verknüpfungen $L \times L \to L$ auf L einschränken, und L bezüglich dieser Verküpfungen einen Körper bildet.

Definition 3.3. Sei K ein Körper. Ein Unterkörper $L \subseteq K$ ist eine Teilmenge, sodass gilt:

(a) $a, b \in L \Rightarrow a + b, a \cdot b \in L$,
(b) $0, 1 \in L$,
(c) $a \in L \Rightarrow -a \in L$,
(d) $0 \neq a \in L \Rightarrow a^{-1} \in L$.

Beispiele 3.4. (a) $\mathbb{Q}$ ist ein Unterkörper von $\mathbb{R}$.

(b) Betrachte die Menge $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$. Dann ist $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ ein Unterkörper mit $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{2}) \subsetneq \mathbb{R}$ (der Körper $\mathbb{Q}(\sqrt{2})$ ist der 'kleinste' Teilkörper von $\mathbb{R}$, der $\sqrt{2}$ enthält):

Wir zeigen zunächst $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{2}) \subsetneq \mathbb{R}$: Angenommen $\sqrt{2} = p/q \in \mathbb{Q}$, $p, q \in \mathbb{Z}, q \neq 0$, p/q gekürzt. Dann ist $p^2 = 2q^2$, also ist p^2 und damit p gerade (das Quadrat einer ungeraden Zahl ist ungerade). Sei $p = 2k$ für ein $k \in \mathbb{Z}$. Wegen $4k^2 = (2k)^2 = p^2 = 2q^2$ ist $2k^2 = q^2$, also ist q gerade: Widerspruch zu p/q ist gekürzt; dies zeigt $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{2})$. Wir nehmen nun an, dass $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$ ist, d.h. $\sqrt{3} = a + b\sqrt{2}$ für $a, b \in \mathbb{Q}$. Dann ist $a \neq 0$ (sonst $\sqrt{3} = b\sqrt{2}$, also $3 = 2b^2$) und $b \neq 0$ (sonst wäre

$\sqrt{3} = a \in \mathbb{Q}$; ein ähnliches Argument wie für $\sqrt{2}$ zeigt, dass dies nicht gilt). Aus $\sqrt{3} = a + b\sqrt{2}$ folgt mit der binomischen Formel

$$3 = a^2 + 2ab\sqrt{2} + 2b^2,$$

und wegen $a \neq 0 \neq b$ dann $\sqrt{2} = (3 - a^2 - 2b^2)/2ab \in \mathbb{Q}$; Widerspruch zu $\sqrt{2} \notin \mathbb{Q}$. Also ist $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{2}) \subsetneq \mathbb{R}$.

Einfaches Nachrechnen (in $\mathbb{R}$!) liefert die Formeln

$$\begin{aligned}(a + b\sqrt{2}) + (c + \sqrt{2}d) &= (a + c) + \sqrt{2}(b + d),\\ (a + b\sqrt{2}) \cdot (c + d\sqrt{2}) &= (ac + 2bd) + (ad + bc)\sqrt{2},\end{aligned}$$

d.h. $\mathbb{Q}(\sqrt{2})$ ist abgeschlossen bzgl. $+$ und $\cdot$ und es gilt (a). Wegen $0 = 0 + 0\sqrt{2}$ und $1 = 1 + 0\sqrt{2}$ gilt (b). Da mit $a + b\sqrt{2}$ auch das additiv Inverse $-(a + b\sqrt{2}) = (-a) + (-b)\sqrt{2}$ in $\mathbb{Q}(\sqrt{2})$ liegt, haben wir (c). Für (d) sei $0 \neq a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Dann ist $a \neq 0$ oder $b \neq 0$ und damit $a + b\sqrt{2} \neq 0$ (ist $a + b\sqrt{2} = 0$, so folgt $\sqrt{2} = -a/b \in \mathbb{Q}$) sowie $a - b\sqrt{2} \neq 0$ (analog). Das multiplikative inverse Element $(a + b\sqrt{2})^{-1}$ ist damit durch die folgende Formel gegeben

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2});$$

dies zeigt die Bedingung (d).

4. Vektorräume

Eine (abelsche) Gruppe ist eine algebraische Struktur, die die Eigenschaften der Addition in den ganzen Zahlen abstrahiert. Ähnlich ist die Definition eines Körpers eine abtrakte Formulierung der Eigenschaften der Addition und Multiplikation von rationalen Zahlen.

Die algebraische Struktur eines Vektorraums ist motiviert durch die reelle Ebene $\mathbb{R}^2 = \{(a, b) \mid a, b \in \mathbb{R}\}$, zusammmen mit der Addition

$$v = (a, b),\ w = (c, d) \in \mathbb{R}^2 \Rightarrow v + w = (a + c, b + d),$$

und der Skalarmultiplikation

$$v = (a, b) \in \mathbb{R}^2, \alpha \in \mathbb{R}\ \Rightarrow \alpha \cdot v = (\alpha \cdot a,\ \alpha \cdot b).$$

In der abstrakten Formulierung werden die Vektoren Elemente einer Menge und die Skalare Elemente eines Körpers sein; zur Unterscheidung bezeichnen wir Vektoren mit lateinischen Buchstaben $a, b, c \ldots$ und Skalare mit griechischen Buchstaben $\alpha, \beta, \gamma, \ldots$.

Definition 4.1. Sei K ein Körper. Ein K-Vektorraum ist eine Menge V, zusammem mit einer (inneren) Verknüpfung $V \times V \to V,\ (v, w) \mapsto v + w$ (einer 'Addition' $+$) und einer (äusseren) Veknüpfung $K \times V \to$

V, $(\alpha, v) \mapsto \alpha \cdot v$ (einer 'Skalarmultiplikation' $\cdot$), sodass für $\alpha, \beta \in K$ und $v, w \in V$ gilt:

(1) V ist bzgl. $+$ eine abelsche Gruppe,

(2) $(\alpha + \beta) \cdot v = \alpha \cdot v + \beta \cdot v$ und $\alpha \cdot (v + w) = \alpha \cdot v + \beta \cdot w$,

(3) $(\alpha \cdot \beta) \cdot v = \alpha \cdot (\beta \cdot v)$,

(4) $1 \cdot v = v$.

Für K-Vektorräume gelten die folgenden Rechenregeln (hier ist 0_V das Nullelement in V und 0_K das Nullelement in K; im Weiteren werden diese Elemente nur mit 0 bezeichtnet, da es sich aus dem Kontext ergibt, welche 'Null' gemeint ist; weiter werden wir für $\alpha \cdot v$ oft einfach nur αv schreiben):

- $\alpha \cdot 0_V = 0_V$ für $\alpha \in K$,
- $0_K \cdot v = 0_V$ für $v \in V$,
- $(-\alpha) \cdot v = \alpha \cdot (-v)$ für $\alpha \in K$ und $v \in V$,
- $\alpha \cdot v = 0_V$ für $\alpha \in K$ und $v \in V$ impliziert $\alpha = 0_K$ oder $v = 0_V$,
- $\alpha \cdot (\sum_{i=1}^{n} v_i) = \sum_{i=0}^{n} (\alpha \cdot v_i)$ und $(\sum_{i=0}^{n} \alpha_i) \cdot v = \sum_{i=0}^{n} (\alpha_i \cdot v)$,
- $\sum_{i=0}^{n} \alpha_i \cdot v_i + \sum_{i=0}^{n} \beta_i \cdot v_i = \sum_{i=0}^{n} ((\alpha_i + \beta_i) \cdot v_i)$.

Beispiele 4.2. (a) Jede abelsche Gruppe enthält ein Nullelement 0 und ist daher eine nicht-leere Menge. Ist $V = \{0\}$ eine ein-elementige Menge, so ist V für jeden Körper K mittels $0 + 0 = 0$ und $\alpha \cdot 0 = 0$ ein K-Vektorraum; V ist der triviale K-Vektorraum oder Nullraum.

(b) Sei K ein Körper. Dann ist $K^n = \{(\alpha_1, \ldots, \alpha_n) \mid \alpha_i \in K \}$ mittels der komponentenweisen Addition und Skalarmultiplikation

$$\begin{aligned} (\alpha_1, \ldots, \alpha_n) + (\beta_1, \ldots, \beta_n) &= (\alpha_1 + \beta_1, \cdots, \alpha_n + \beta_n), \\ \alpha \cdot (\alpha_1, \cdots, \alpha_n) &= (\alpha \cdot \alpha_1, \cdots, \alpha \cdot \alpha_n) \end{aligned}$$

ein K-Vektorraum; für $n = 0$ ist $K^0 = \{0\}$ der Nullraum. Die K-Vektorräume K^n sind die zentralen Beispiele in der linearen Algebra.

(c) Sei K ein Körper und M ein Menge. Dann ist die Menge $V = \mathrm{Abb}(M, K)$ der Abbildungen $M \to K$ ein K-Vektorraum bezüglich der 'punktweise' definierten Verknüpfungen: $f, g \in V$, $\alpha \in K$,

$$\begin{aligned} f + g : &\quad M \to K, \quad m \mapsto f(m) + g(m), \\ \alpha \cdot f : &\quad M \to K, \quad m \mapsto \alpha \cdot f(m) \end{aligned}$$

Diese Beispiele von K-Vektorräumen treten oft in der Analysis auf; zum Beispiel, ist $I = [0, 1] \subseteq \mathbb{R}$ das Einheitsintervall, und $K = \mathbb{R}$, so ist $V = \mathrm{Abb}(I, \mathbb{R})$ der $\mathbb{R}$-Vektorraum der reellwertigen Funktionen auf dem Einheitsintervall.

(d) Sei K ein Körper und $K[x]$ die Menge der Polynome in x mit

Koeffizienten in K. Dann ist $K[x]$ bzgl. der üblichen Addition von Polynomen (Addition der Koeffizienten) und der Skalarmultiplikation

$$\alpha \in K,\ f = \sum_{i=0}^{n} \alpha_i x^i \Rightarrow \alpha \cdot f = \sum_{i=0}^{n} (\alpha\alpha_i) x^i$$

ein K-Vektorraum.

(e) Sei K ein Körper und $k \subseteq K$ ein Unterkörper. Nach Definition ist $k \leq K$ eine abelsche Untergruppe und die Einschränkung der Multiplikation $K \times K \to K$ auf $k \times K \to K$ definiert ein Skalarprodukt, d.h. K ist ein k-Vektorraum. Insbesondere ist wegen der Inklusionen von Unterkörpern $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$, $\mathbb{R}$ nicht nur ein $\mathbb{R}$-Vektorraum ($\mathbb{R} = \mathbb{R}^1$), sondern auch ein $\mathbb{Q}$-Vektorraum bzw. $\mathbb{Q}(\sqrt{2})$-Vektorraum.

Definition 4.3. Sei V ein K-Vektorraum. Eine Teilmenge $U \subseteq V$ ist ein K-Untervektorraum oder K-linearer Unterraum von V, falls gilt:

(a) $\emptyset \neq U$,
(b) $a, b \in U \Rightarrow a + b \in U$,
(c) $\alpha \in K, a \in U \Rightarrow \alpha \cdot a \in U$ (insbesondere: $a \in U \Rightarrow -a \in U$).

• Ist V ein K-Vektorraum und $U \subseteq V$ ein K-linearer Unterraum, so bezeichnen wir U oft einfach als linearen Unterraum (d.h. ein linearer Unterraum eines K-Vektorraums ist stets ein Untervektorraum über demselben Körper).

Beispiele 4.4. (a) Sei V ein K-Vektorraum. Dann ist $V \subseteq V$ stets ein Unterraum. Ist $v \in V$, so ist der von v erzeugte lineare Unterraum

$$K \cdot v = \{\alpha \cdot v \mid \alpha \in K\} \subseteq V.$$

Insbesondere enthält jeder K-Vektorraum V die linearen Unterräume $\{0\}$ ($v = 0$) und V; dies sind die trivialen linearen Unterräume.

(b) Sei $m \leq n$, und sei $K^m \subseteq K^n$ die kanonische Inklusion, die ein m-Tupel $(\alpha_1, \ldots, \alpha_m) \in K^m$ mit dem n-Tupel $(\alpha_1, \ldots, \alpha_m, 0, \ldots 0) \in K^n$ identifiziert. Dann ist $K^m \subseteq K^n$ ein linearer Unterraum.

(c) Sei K ein Körper und M eine Menge. Ist $V = \mathrm{Abb}(M, K)$ der K-Vektorraum der K-wertigen Funktionen auf M, so bilden die stetigen (bzw. differenzierbaren, Polynomfunktionen) einen Unterraum von V.

(d) Wegen der Inklusionen $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ sind $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$ und $\mathbb{R}$ $\mathbb{Q}$-lineare Unterräume des $\mathbb{Q}$-Vektorraums $\mathbb{R}$.

Wir betrachten Untervektorräume eines K-Vektorraums V.

Lemma 4.5. *Sei V ein K-Vektorraum und sei $\{U_i\}_{i \in I}$ eine Familie von linearen Unterräumen von V. Dann ist $U = \cap_{i \in I} U_i \subseteq V$ ebenfalls ein linearer Unterraum.*

Beweis. Aus $0 \in U_i$ für alle i folgt $0 \in U$, d.h. $U \neq \emptyset$. Sind $u, u' \in U$ und $\alpha \in K$, so ist $u + u' \in U_i$ und $\alpha \cdot u \in U_i$ für alle i, da die U_i lineare Unterräume sind. Damit folgt $u + u' \in U$ und $\alpha \cdot u \in U$. □

Wir wollen zu einer beliebigen Teilmenge $A \subseteq V$ eines K-Vektorraums den 'kleinsten' linearen Unterraum $\langle A \rangle \subseteq V$ bestimmen, der die gegebene Menge A enthält. Klar ist, dass dieser lineare Unterraum $\langle A \rangle$ alles Elemente der Form

$$\sum_{i=1}^{n} \alpha_i a_i, \ n \in \mathbb{N}, \ \alpha_i \in K, \ a_i \in A$$

enthalten muss. Wir zeigen, dass die Menge dieser Elemente bereits den gewünschten linearen Unterrraum bildet:

Lemma 4.6. *Sei V ein K-Vektorraum und $A \subseteq V$ eine Teilmenge. Dann ist die Menge*

$$\langle A \rangle = \{\sum_{i=1}^{n} \alpha_i a_i \mid n \in \mathbb{N}, \alpha_i \in K, a_i \in A\} \subseteq V.$$

ein linearer Unterraum (der von A erzeugte lineare Unterrraum). Weiter ist $\langle A \rangle = \cap\{U \mid U \subseteq V$ linearer Unterraum, $A \subseteq U\}$, d.h. $\langle A \rangle$ ist der kleinste lineare Unterraum, der die gegebene Teilmenge A enthält.

NB. Ist $\{a_i\}_{i \in I} \subseteq V$ eine Familie von Elementen von V, so definiert man analog den von den Elementen a_i erzeugten linearen Unterraum $\langle a_i \mid i \in I \rangle \subseteq V$ als den von der Menge $A = \{a_i\}_{i \in I}$ erzeugten Unterraum. Klar ist damit:

- $\langle \emptyset \rangle = \{0\}$,
- $A \subseteq \langle A \rangle$ für jede Teilmenge $A \subseteq V$,
- $U = \langle U \rangle$ für jeden linearen Unterraum $U \subseteq V$,
- Sind $A, B \subseteq V$ Teilmengen, so gilt $A \subseteq B \Rightarrow \langle A \rangle \subseteq \langle B \rangle$ und $A \subseteq \langle B \rangle \Rightarrow \langle A \rangle \subseteq \langle B \rangle$.

Beweis. Nach Definition der leeren Summe ist $\sum_{i=1}^{0} \alpha_i \cdot a_i = 0$, also ist $0 \in \langle A \rangle$ (auch wenn $A = \emptyset$ ist). Sei $\alpha \in K$ und seien $a, b \in \langle A \rangle$, d.h. $a = \Sigma_{i=1}^{r} \alpha_i a_i$ und $b = \Sigma_{j=1}^{s} \beta_j b_j$. Dann ist

$$\begin{aligned} \alpha a &= \textstyle\sum_{i=1}^{r} (\alpha \alpha_i) a_i \\ a + b &= \textstyle\sum_{i=1}^{r} \alpha_i a_i + \sum_{j=1}^{s} \beta_j b_j = \sum_{i=1}^{r+s} \alpha_i a_i, \end{aligned}$$

wobei $\alpha_{r+j} = \beta_j$ und $a_{r+j} = b_j$ für $j = 1, \ldots, s$ sei. Da αa und $a + b$ in $\langle A \rangle$ liegen definiert $\langle A \rangle$ einen linearer Unterraum.

Sei $U \subseteq V$ ein linearer Unterraum, der A enthält. Dann muss U auch die $\langle A \rangle$ definierenden Ausdrücke enthalten, also ist $\langle A \rangle \subseteq U$ und da

dies für jeden solchen Unterraum U gilt folgt $\langle A\rangle \subseteq \cap\{U \mid A \subseteq U\}$. Wegen $A \subseteq \langle A\rangle$ (da $1\cdot a = a$ für $a \in A$) ist auch $\langle A\rangle$ ein Unterraum, der A enthält. Also ist $\cap\{U \mid A \subseteq U\} \subseteq \langle A\rangle$ und damit gilt Gleichheit. $\square$

Beispiele 4.7. (a) Sei $V = \mathbb{R}^2$. Ist $0 \neq a \in \mathbb{R}^2$ ein beliebiger nicht-trivialer Vektor, so ist

$$\langle a\rangle = \{\alpha \cdot a \mid \alpha \in \mathbb{R}\} \subseteq \mathbb{R}^2$$

genau die Gerade durch den Ursprung, die durch a erzeugt wird. Ist $0 \neq b \in \mathbb{R}^2$ ein weiterer Vektor mit $a \neq \alpha \cdot b$ für alle $\alpha \in \mathbb{R}$ (d.h. die Vektoren a und b liegen nicht auf derselben Geraden), so ist

$$\langle a, b\rangle = \{\alpha \cdot a + \beta \cdot b \mid \alpha, \beta \in \mathbb{R}\} = \mathbb{R}^2.$$

Also gibt es zu *jedem* Vektor $c \in \mathbb{R}^2$ Skalare $\alpha, \beta \in \mathbb{R}$, sodass gilt

$$c = \alpha a + \beta b.$$

(b) Sei $V = \mathbb{Q}[x]$ der $\mathbb{Q}$-Vektorraum aller Polynome in x mit rationalen Koeffizienten. Dann gilt $\langle 1\rangle = \{\text{konstante Polynome }\} = \mathbb{Q}$, $\langle \{1, x\}\rangle = \{\text{Polynome vom Grad } \leq 1\}$, $\langle\{1, x, x^2\}\rangle = \{\text{Polynome vom Grad } \leq 2\}$, etc., d.h. keine *endliche* Teilmenge der Form $A = \{1, x, x^2, \ldots, x^n\}$ hat die Eigenschaft, dass $\langle A\rangle = \mathbb{Q}[x]$ ist. Allerdings ist $\langle A\rangle = \mathbb{Q}[x]$ für $A = \{x^n \mid k \in \mathbb{N}_0\ \}$ (da $x^0 = 1$ ist).

Was zeichnen diejenigen Teilmengen $A \subseteq V$ aus, für die $\langle A\rangle = V$ ist:

Definition 4.8. Eine Menge $A = \{a_i\}_{i\in I} \subseteq V$ von Elementen eines K-Vektorraums V ist ein Erzeugendensystem von V, falls $\langle A\rangle = V$ gilt, d.h. falls jeder Vektor $v \in V$ eine Darstellung als endliche Summe

$$v = \sum_{i=1}^{n} \alpha_i a_i,\ \alpha_i \in K,\ a_i \in A$$

besitzt. Der Vektorraum V ist endlich erzeugt (über K), falls V eine endliches Erzeugensystem $A = \{a_1, \cdots, a_n\}$ besitzt.

NB. Ist $\langle A\rangle = V$, so besagt dies, dass *jeder* Vektor $v \in V$ sich als eine endliche Summe $v = \sum_{i=1}^{n} \alpha_i a_i$ mit $\alpha_i \in K$ und $a_i \in A$ darstellen lässt. Aber: diese Darstellung ist nicht unbedingt eindeutig. Zum Beispiel, ist $A = \{(1,0), (0,1), (1,1)\} \subseteq \mathbb{R}^2$, so ist $\langle A\rangle = \mathbb{R}^2$, aber der Nullvektor lässt sich auf verschiedene Weise darstellen

$$\begin{aligned}(0,0) &= 0\cdot(1,0) + 0\cdot(0,1)\\ (0,0) &= 1\cdot(1,0) + 1\cdot(0,1) + (-1)\cdot(1,1)\end{aligned}$$

Beispiele 4.9. (a) Fürt jeden K-Vektorraum V gilt $\langle V\rangle = V$; $\langle V\rangle$ ist das triviale Erzeugendensystem.

(b) Nach Beispiel 4.7(a) bilden je zwei nicht-triviale Vektoren und

nicht-kollineare (nicht auf einer Geraden liegenden) Vektoren $a, b \in \mathbb{R}^2$ ein Erzeugendensystem, also ist $\mathbb{R}^2$ endlich erzeugt; jede Teilmenge $A \subseteq \mathbb{R}^2$ die mindestens zwei nicht-triviale und nicht-kollineare Vektoren enthält ist ein Erzeugendensystem, d.h. $\mathbb{R}^2$ lässt sich von zwei (nicht unbedingt 'orthogonalen') Elementen erzeugen. Allgemein besitzt $\mathbb{R}^n$ ein Erzeugendensystem aus n Elementen: Setze $e_i = (0, \ldots, 1, \ldots, 0)$ d.h. e_i ist der Vektor in $\mathbb{R}^n$ mit 1 in der i-ten Komponente und 0 in allen anderen. Ist $v = (\alpha_1, \ldots, \alpha_n) \in \mathbb{R}^n$ ein beliebiger Vektor, so ist

$$v = \sum_{i=1}^{n} \alpha_i e_i.$$

Analog ist für jeden Körper K der K-Vektorraum K^n von den n Vektoren $e_i,\ i = 1, \ldots, n$, erzeugt.

(c) Der $\mathbb{Q}$-Vektorraum $\mathbb{Q}[x]$ ist nicht endlich erzeugt: ist $A \subseteq \mathbb{Q}[x]$ eine endliche Menge von Polynomen $f_1, \ldots, f_n$, so ist die maximale Potenz von x in endliche Summen der Form $\sum_{i=1}^{n} q_i f_i,\ q_i \in \mathbb{Q}$, beschränkt und jedes Polynom mit einer höheren Potenz von x kann nicht als eine solche Summe dargestellt werden.

(d) Sei $V = \mathbb{Q}(\sqrt{2})$. Da V ein Körper ist, ist V ein $\mathbb{Q}(\sqrt{2})$-Vektorraum und es ist $\langle 1 \rangle = V$ für V als $\mathbb{Q}(\sqrt{2})$-Vektorraum. Da $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ ein Unterkörper ist, ist V auch ein $\mathbb{Q}$-Vektorraum; für V als $\mathbb{Q}$-Vektorraum gilt $\langle 1, \sqrt{2} \rangle = V$.

Uns interessieren Erzeugendensysteme $A \subseteq V$ mit der Eigenschaft, dass sich jedes $v \in V$ *eindeutig* als eine endliche Linearkombination

$$v = \sum_{i=1}^{n} \alpha_i a_i,\ \alpha_i \in K,\ a_i \in A$$

schreiben lässt. Diese Bedingung lässt sich wie folgt formulieren: Sei $A = \{a_1, \ldots, a_n\}$ endlich. Lässt sich jeder Vektor eindeutig als eine endliche Linearkombination der a_i darstellen, so gilt dies insbesondere für den Nullvektor. Wegen $0 = 0 \cdot a_1 + 0 \cdot a_2 + \cdots + 0 \cdot a_n$ folgt dann

$$(\#) \qquad \sum_{i=0}^{n} \alpha_i a_i = 0 \Rightarrow \alpha_i = 0 \text{ für alle } i = 0, \ldots, n.$$

Gilt umgekehrt $(\#)$, und ist $v = \sum_{i=1}^{n} \alpha_i a_i = \sum_{i=1}^{n} \beta_i a_i$, so folgt wegen

$$0 = v - v = \sum_{i=1}^{n} (\alpha_i - \beta_i) a_i$$

aus $(\#)$ die Gleichheit der Koeffizienten $\alpha_i = \beta_i$ für $i = 0, \ldots, n$, d.h. die Darstellung von v als $v = \sum_{i=1}^{n} \alpha_i a_i$ ist eindeutig.

Dies führt zu dem Begriff der linearen Unabhängigkeit.

Definition 4.10. Sei V ein K-Vektorraum und seien $\{a_i\}_{i\in I}$ Vektoren in V. Die Menge $\{a_i\}_{i\in I}$ ist linear unabhängig (die a_i sind linear unabhängig), falls für jede endliche Teilmenge $J \subseteq I$ gilt

$$\sum_{j\in J} \alpha_j a_j = 0 \Rightarrow \alpha_j = 0 \text{ für alle } j \in J.$$

Sind die a_i nicht linear unabhängig, so sind sie linear abhängig.

NB. Vektoren $\{a_1, \ldots, a_n\}$ sind linear unabhängig genau dann, wenn $\langle a_1, \ldots, a_n\rangle$ ein minimales Erzeugendensystem ist (d.h. kein a_i hat eine Darstellung als $a_i = \sum_{j\neq i} \alpha_j a_j,\ \alpha_j \in K$): Sind $\{a_1, \ldots, a_n\}$ linear abhängig, so gilt $\sum_{i=1}^n \alpha_i a_i = 0$ mit nicht alle $\alpha_i = 0$. Ist $\alpha_i \neq 0$, so ist $a_i = \sum_{j\neq i} -\alpha_i^{-1}\alpha_j a_j$ und $\langle a_1, \ldots, a_n\rangle$ ist nicht minimal. Ist umgekehrt $\langle a_1, \ldots, a_n\rangle$ nicht minimal, so gibt es ein a_i mit $a_i = \sum_{j\neq i} \alpha_j a_j$ und daher $(-1)a_i + \sum_{j\neq i} \alpha_j a_j = 0$, d.h. $\{a_1, \ldots, a_n\}$ sind linear abhängig.

- Die aus dem Nullvektor $\{0\}$ bestehende Menge ist linear abhängig.
- Eine Menge die einen Vektor und ein Skalarvielfaches dieses Vektors enthält ist linear abhängig.
- Die aus einem Nichtnullvektor $\{v \neq 0\}$ bestehende Menge ist linear unabhängig.
- Die leere Menge $\emptyset$ ist linear unabhängig.

Beispiele 4.11. (a) Ist $V = \mathbb{R}^2$, so sind die Vektoren $e_1 = (1, 0)$ und $e_2 = (0, 1)$ linear unabhängig. Dies folgt formal, da die Gleichung

$$(0, 0) = \alpha \cdot (1, 0) = \beta \cdot (0, 1) = (\alpha, \beta)$$

nur die Lösung $\alpha = 0 = \beta$ hat. Die lineare Unabhängigkeit von e_1 und e_2 ist geometrisch klar: Jeder Vektor $a \in \mathbb{R}^2$ lässt sich auf genau eine Weise als Summe ('Parallelogramm') von Vielfachen von e_1 und e_2 darstellen. Aus dem gleichen Grund sind je zwei nicht-triviale und nicht-kollineare Vektoren $a, b \in \mathbb{R}^2$ linear unabhängig.
(b) Sei $V = K^n$ und sei $e_i = (0, \ldots, 1, \ldots, 0)$ der Vektor mit 1 in der i-ten Komponente, $i = 1, \ldots, n$. Für alle Skalare $\alpha_i \in K$ gilt somit

$$(\alpha_1, \ldots, \alpha_n) = \sum_{i=1}^n \alpha_i e_i.$$

Also ist $\sum_{i=1}^n \alpha_i e_i = 0$ genau dann, wenn $\alpha_i = 0$ für $i = 1, \ldots, n$ und die $e_1, \ldots, e_n$ sind linear unabhängig.

(c) Ist $V = \mathbb{Q}[x]$ der $\mathbb{Q}$-Vektorraum der Polynome mit rationalen Koeffizienten, so sind die Mengen $A_n = \{1, x, \ldots, x^n \mid n \geq 0\} \subseteq \mathbb{Q}[x]$ linear unabhängig: Aus $\sum_{i=0}^{n} \alpha_i x^i = 0 = \sum_{i=0}^{n} 0x^i$ folgt $\alpha_i = 0$ für $i = 0, \ldots, n$.

Definition 4.12. Sei V ein K-Vektorraum. Eine Basis von V ist eine Erzeugendensystem $B = \{b_i \mid i \in I\} \subseteq V$ von V (sodass $\langle B \rangle = V$), welches aus linear unabhängigen Vektoren besteht.

NB. Ist $B \subseteq V$ eine Basis, so besagt die erste Bedingung, dass jeder Vektor in V sich als (endliche) Linearkombination von Elementen aus B mit Koeffizienten aus K darstellen lässt. Die zweite Bedingung impliziert, dass diese Darstellung eindeutig ist. Inbesondere gilt das Prinzip des Koeffizientenvergleichs: Ist $B = \{b_i \mid i \in I\} \subseteq V$ eine Basis und ist $J \subseteq I$ eine endliche Teilmenge der Indexmenge, so gilt

$$\sum_{j \in J} \alpha_j b_j = \sum_{j \in J} \beta_j b_j \;\Rightarrow\; \alpha_j = \beta_j \text{ für } j \in J.$$

Theorem 4.13. *Sei V ein endlich erzeugter K-Vektorraum, $V = \langle a_1, \ldots, a_n \rangle$. Sei $0 \leq k \leq n$ und seien $c_1, \ldots, c_k$ linear unabhängige Vektoren in V. Dann gibt es eine Basis $\{b_1, \ldots, b_m\}$ von V, sodass gilt*

$$\{c_1, \ldots, c_k\} \subseteq \{b_1, \ldots, b_m\} \subseteq \{a_1, \ldots, a_n\},$$

d.h. jede linear unabhängige Menge $\{c_1, \ldots, c_k\}$ lässt sich durch Hinzunahme geeigneter Vektoren aus einem Erzeugendensystem zu einer Basis von V ergänzen.

NB. 1. Das Theorem besagt, dass jeder endlich erzeugte K-Vektorraum eine Basis besitzt: Ist $V = \{0\}$, so ist $\{\emptyset\}$ eine Basis. Ist $V \neq \{0\}$, so gibt es einen Vektor $0 \neq c \in V$, der linear unabhängig ist, und $\{c\}$ lässt sich durch Hinzunahme geeigneter Vektoren aus einem Erzeugendensystem von V zu einer Basis von V ergänzen.

2. Der Beweis impliziert, dass folgende Aussagen gleichwertig sind:

(a) $\{b_1, \ldots, b_m\}$ ist eine Basis von V,
(b) $\{b_1, \ldots, b_m\}$ ist maximale linear unabhängige Teilmenge in V,
(c) $\langle b_1, \ldots b_m \rangle$ ist minimales Erzeugendensystem von V.

Beweis. Wir können oBdA annehmen, dass $\{c_1, \ldots, c_k\} \subseteq \{a_1, \ldots, a_n\}$ ist; sei also $a_i = c_i$ für $i = 1, \ldots, k$. Betrachte die Teilmengen

$$\{a_1, \ldots, a_k\} \subseteq \{a_1, \ldots, a_m\} \subseteq \{a_1, \ldots, a_n\},$$

wobei $1 \leq k \leq m \leq n$ ist, und $\{a_1, \ldots, a_m\}$ eine maximale linear unabhängige Teilmenge von $\{a_1, \ldots, a_n\}$ bildet. Ist $m < j \leq n$ so sind

die Vektoren $a_1, \ldots, a_m, a_j$ linear abhängig, d.h. es gibt eine Relation

$$\sum_{i=1}^{m} \alpha_i a_i + \alpha_j a_j = 0,$$

wobei entweder ein $\alpha_i \neq 0$ oder $\alpha_j \neq 0$ ist. Da die $a_1, \ldots a_m$ linear unabhängig sind, folgt aus der Annahme $\alpha_j = 0$ dann $\alpha_1 = \cdots = \alpha_m = 0$, Widerspruch. Somit ist $\alpha_j \neq 0$ und $a_j \in \langle a_1, \ldots a_m \rangle$, da

$$a_j = -\sum_{i=1}^{n} (\alpha_j^{-1} \alpha_i) a_i \in \langle a_1, \ldots, a_m \rangle.$$

Also ist $\langle a_1, \ldots, a_m \rangle = V$ und $\{a_1, \ldots a_m\}$ ist eine Basis von V. □

Nach Theorem 4.13 hat jeder endlich erzeugte K-Vektorraum eine Basis. Klar ist, dass eine solche Basis nicht eindeutig bestimmt ist (zum Beispiel ist für $V = \mathbb{R}^2$ sowohl $\{(1,0),(0,1)\}$, als auch $\{(1,0),(1,1)\}$ eine Basis). Wir zeigen, dass die Anzahl der Basiselemente eine Invariante des Vektorraums und unabhängig von der Wahl der Basis ist.

Lemma 4.14. *Sei V ein K-Vektorraum und sei $B = \{b_1, \ldots, b_n\} \subseteq V$ eine Basis von V. Ist $b = \sum_{1=1}^{n} \alpha_i b_i$ mit $\alpha_i \in K$ und $\alpha_1 \neq 0$, so ist auch $B' = \{b, b_2, \ldots, b_n\} \subseteq V$ eine Basis.*

• Analog gilt: Ist $b = \sum_{i=1}^{n} \alpha_i b_i$ mit $\alpha_m \neq 0$, so bildet auch die Menge $\{b_1, \ldots, b_{m-1}, b, b_{m+1}, \ldots, b_n\}$ eine Basis.

Beweis. Aus der Definition von b ergibt sich sofort

$$b_1 = \alpha_1^{-1}(b - \sum_{i=2}^{n} \alpha_i b_i) \in \langle b, b_2, \ldots, b_n \rangle,$$

also ist $\langle b, b_2, \ldots b_n \rangle = \langle b_1, \ldots, b_n \rangle = V$. Es bleibt zu zeigen: Die Vektoren $b, b_2, \ldots b_n$ sind linear unabhängig. Sei

$$\beta b + \sum_{i=2}^{n} \beta_i b_i = 0, \quad \beta, \beta_i \in K.$$

Dann ist

$$(\beta\alpha_1) b_1 + \sum_{i=2}^{n} (\beta_i + \beta\alpha_i) b_i = 0.$$

Die lineare Unabhängigkeit der $b_1, \ldots, b_n$ liefert dann

$$\beta\alpha_1 = \beta_i + \beta\alpha_i = 0 \text{ für } i = 2, \ldots, n.$$

Wegen $\alpha_1 \neq 0$ ist $\beta = 0$ und damit dann $\beta_i = 0$ für $i = 2, \ldots, n$. □

Theorem 4.15. *(Austauschsatz von Steinitz) Sei V ein K-Vektorraum und $\{b_1, \ldots, b_n\} \subseteq V$ eine Basis von V. Ist $\{a_1, \ldots a_m\} \subseteq V$ eine linear unabhängige Teilmenge, so ist $m \leq n$ und mit geeigneter Numerierung der b_i ist $\{a_1, \ldots, a_m, b_{m+1}, \ldots, b_n\}$ auch eine Basis von V (d.h. jede linear unabhängige Menge von Vektoren aus V lässt sich durch Hinzunahme geeigneter Vektoren aus einer Basis zu einer Basis erweitern).*

Beweis. Induktion nach m. Ist $m = 1$, so ist $a_1 \neq 0$ und $a_1 = \sum_{i=1}^{n} \alpha_i b_i$ mit $\alpha_i \neq 0$ für ein i; oBdA ist $\alpha_1 \neq 0$. Nach Lemma 4.14 ist dann die Menge $\{a_1, b_2, \ldots, b_n\}$ wieder eine Basis von V. Sei nun $1 < m \leq n$. Da die $a_1, \ldots, a_{m-1}$ linear unabhängig sind gibt es nach Induktion eine Basis $\{a_1, \ldots, a_{m-1}, b_m, \ldots b_n\}$ von V. Angenommen

$$a_m = \sum_{j=1}^{m-1} \beta_j a_j + \sum_{i=m}^{n} \gamma_i b_i, \ \beta_j, \gamma_i \in K.$$

Da die $a_1, \ldots, a_m$ linear unabhängig sind ist a_m keine Linearkombination von $a_1, \ldots, a_{m-1}$ und es gibt ein $\gamma_i \neq 0$; wir können durch Umnumerierung annehmen, dass $\gamma_m \neq 0$ ist. Nach Lemma 4.14 können wir dann b_m durch a_m ersetzen, und erhalten eine Basis $\{a_1, \ldots, a_m, b_{m+1}, \ldots, b_n\}$. Ist $\{a_1, \ldots, a_m\}$ eine linear unabhängige Teilmenge mit $m > n$, so folgt wie oben, dass $\{a_1, \ldots, a_m\}$ eine Basis von V bildet. Insbesondere ist wegen $a_{n+1} \in V$ dann $a_{n+1} \in \langle a_1, \ldots, a_m \rangle$, was der linearen Unabhängigkeit von $\{a_1, \ldots, a_m\}$ widerspricht, also ist $m \leq n$. □

Theorem 4.16. *Sei V ein endlich erzeugter K-Vektorraum. Dann hat V eine Basis $\{b_1, \ldots, b_n\}$ und jede Basis hat genau n Elemente.*

Beweis. Theorem 4.13 besagt, dass V eine Basis $\{b_1, \ldots, b_n\}$ besitzt. Sei $\{b'_i \mid i \in I\} \subseteq V$ eine weitere Basis von V. Wäre $|I| > n$, so gäbe es in V eine linear unabhängige Menge $b'_1, \ldots, b'_{n+1}$ mit mehr als n Elementen; dies widerspricht Theorem 4.15. Also ist $|I| \leq n$. Vertauschung der Rollen der beiden Basen zeigt $n \leq |I|$, also ist $n = |I|$. □

Definition 4.17. Sei $0 \neq V$ ein endlich erzeugbarer K-Vektorraum. Die Dimension (oder K-Dimension) $\dim_K V$ ist die Anzahl der Elemente einer (und damit jeder) Basis von V. Ist $V = \{0\}$, so setze $\dim_K V = 0$.

NB. Mit Hilfe des 'Zornschen Lemmas' kann man die Existenz von Basen in beliebigen K-Vektorräumen (d.h. nicht unbedingt endlich erzeugbaren K-Vektorräumen) beweisen. Der Beweis liefert die Existenz, ist aber nicht konstruktiv. Je zwei Basen haben die gleiche Mächtigkeit. Ist V endlich erzeugt, so schreibe $\dim V < \infty$; ist V nicht endlich erzeugbar, so setze $\dim V = \infty$.

Beispiele 4.18. (a) Für jeden Körper K ist ist $\{e_1, \ldots, e_n\} \subseteq K^n$ eine Basis; die sogenannte Standardbasis. Also ist $\dim K^n = n$.

(b) Betrachte die Inklusionen von Körpern $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$. Der $\mathbb{Q}$ Vektorraum $\mathbb{Q} = \mathbb{Q}^1$ hat Dimension 1. Der $\mathbb{Q}$-Vektorraum $\mathbb{Q}(\sqrt{2})$ wird von $\{1, \sqrt{2}\}$ erzeugt. Da $\{1, \sqrt{2}\}$ auch linear unabhängig sind, ist $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) = 2$. Für die reellen Zahlen $\mathbb{R}$, aufgefasst als $\mathbb{Q}$-Vektorraum, gilt $\dim_{\mathbb{Q}} \mathbb{R} = \infty$: Hätte $\mathbb{R}$ eine endliche $\mathbb{Q}$-Basis, so wäre $\mathbb{R}$ abzählbar, Widerspruch.

(c) Für den $\mathbb{Q}$-Vektorraum $\mathbb{Q}[x]$ der Polynome mit rationalen Koeffizienten gilt ebenfalls $\dim_{\mathbb{Q}} \mathbb{Q}[x] = \infty$; eine (unendliche) Basis ist durch die Menge $\{1, x, x^2 \cdots\}$ gegeben.

(d) Sei K ein Körper, M eine Menge, und $V = \mathrm{Abb}(M, K)$ der K-Vektorraum der K-wertigen Funktionen. Für $m \in M$ sei $f_m : M \to K$ die Abbildung $f_m(m) = 1$ und $f_m(m') = 0$ für $m \neq m' \in M$. Seien $m_1, \ldots, m_n$ paarweise veschiedene Elemente von M und sei

$$\sum_{i=1}^{n} \alpha_i f_{m_i} = 0, \quad \alpha_i \in K.$$

Dann ist

$$0 = (\sum_{i=1}^{n} \alpha_i f_{m_i})(m_j) = \alpha_j \text{ für } j = 1, \ldots, n.$$

Also sind die $f_{m_1}, \ldots, f_{m_n}$ linear unabhängig. Ist $M = \infty$, so folgt $\dim_K V = \infty$. Ist $|M| = n < \infty$, so hat jedes Element $f \in V$ eine Darstellung als eine endliche Linearkombination

$$f = \sum_{m \in M} f(m) f_m,$$

d.h. die $\{f_m \mid m \in M\}$ bilden eine Basis von V und $\dim_K V = |M|$.

Sei V ein K-Vektorraum und seien $U_i \subseteq V$ lineare Unterräume, $i = 1, \ldots, k$. Die Summe der U_i ist definiert als die Menge

$$U_1 + \cdots U_k = \{u_1 + \cdots + u_k \mid u_i \in U_i\} \subseteq V.$$

Es ist $U_1 + \cdots U_k = \langle \cup_{i=1}^{k} U_i \rangle \subseteq V$, d.h. die Summe $U_1 + \cdots + U_k \subseteq V$ ist ein linearer Unterraum; siehe Übung.

Lemma 4.19. *Sei V ein K-Vektorraum mit $\dim V = n < \infty$ und $U \subseteq V$ ein linearer Unterraum. Dann gilt*

(a) $\dim U \leq \dim V$,

(b) *Ist $\{b_1, \ldots, b_k\} \subseteq U$ eine Basis, so gibt es eine Basis von V der Form $\{b_1, \ldots, b_k, b_{k+1}, \ldots, b_n\}$.*

(c) *Es gibt einen linearen Unterraum* $W \subseteq V$*, sodass gilt:* $V = U+W$ *und* $U \cap W = \{0\}$ *(der Unterraum* W *ist ein Komplement von* U *in* V*),*

(d) $\dim U = \dim V$ *genau dann, wenn* $U = V$*.*

Beweis. (a): Ist $U = \{0\}$, so ist $\dim U = 0 \leq n$. Ist $U \neq \{0\}$, so gilt für jede linear unabhängige Teilmenge $B \subseteq U$ nach Theorem 4.15 $|B| \leq n$. Insbesondere hat eine maximale linear unabhängige Teilmenge $B \subseteq U$, also eine Basis von U, maximal n Elemente und $\dim U \leq \dim V$.

(b): Folgt aus Theorem 4.13.

(c): Ist $\{b_1, \ldots, b_k\}$ eine Basis von U, so lässt sich diese nach (b) zu einer Basis $\{b_1, \ldots, b_k, b_{k+1}, \ldots, b_n\}$ von V ergänzen. Für den linearen Unterraum $W = \langle b_{k+1}, \ldots, b_n \rangle$ gilt $U + W = V$ und $U \cap W = \{0\}$.

(d): Sei $\dim U = \dim V = n$. Ist $\{b_1, \ldots, b_n\}$ eine Basis von U, so ist nach (b) $\{b_1, \ldots, b_n\}$ auch Basis von V, und $U = \langle b_1, \ldots, b_n \rangle = V$. Die Umkehrung ist trivial. □

Beispiel 4.20. Ist M eine Menge und $N \subseteq M$ eine Teilmenge, so ist das mengentheoretische Komplement $\overline{N} = M \setminus N = \{m \in M \mid m \notin N\}$ eindeutig bestimmt. Dies gilt im allgemeinen nicht für Komplemente von linearen Unterräumen: Ist V ein endlich erzeugter K-Vektorraum und $\{0\} \subsetneq U \subsetneq V$ ein linearer Unterraum, so hat U stets mehrere Komplemente. Ist $\{b_1, \ldots, b_k\}$ eine Basis von V und $\{b_1, \ldots, b_n\}$ eine Basis von V, so definiert für jedes $\alpha \in K$ der lineare Unterraum

$$W_\alpha = \langle b_{k+1}, \ldots, b_{n-1}, b_n + \alpha b_1 \rangle$$

ein Komplement von U in V. Klar ist, dass $U + W_\alpha = V$ ist. Ist

$$\sum_{j=k+1}^{n-1} \alpha_j b_j + \alpha_n (b_n + \alpha b_1) = \sum_{i=1}^{k} \alpha_i b_i \in U \cap W_\alpha,$$

so ergibt sich eine Darstellung der 0 und Koeffizientenvergleich zeigt $\alpha_1 = \cdots = \alpha_n = 0$, also ist $U \cap W_\alpha = \{0\}$. Für verschiedene $\alpha \in K$ sind die W_α verschieden; ist K unendlich, so gibt es sogar unendlich viele Komplemente von U in V. Konkret: Sei $V = \mathbb{R}^2$, $U = \langle (1,0) \rangle$ und $\{(1,0), (0,1)\}$ die Standardbasis von V. Für $\alpha \in \mathbb{R}$ ist $W_\alpha = \langle (\alpha, 1) \rangle$. Für $\alpha, \alpha' \in \mathbb{R}$, $\alpha \neq \alpha'$ ist $(\alpha, 1) \neq (\alpha', 1)$, d.h. die durch diese Vektoren erzeugten Unterräume W_α und $W_{\alpha'}$ sind verschiedene Geraden durch den Ursprung; jede von der Achse x-Achse $U = \langle (1,0) \rangle$ verschiedende Gerade durch den Ursprung liefert ein Komplement von U in V.

5. Lineare Abbildungen und Faktorräume

Wir wollen K-Vektorräume mittels Abildungen vergleichen. Ein Vektorraum ist eine Menge, zusammen mit einer 'algebraischen' Struktur ('Addition' und 'Skalarmultiplikation'), und wir verlangen, dass Abbildungen zwischen Vektorräumen diese Strukturen erhalten.

Abstrakt sollte eine strukturerhaltende Abbildung die folgende Eigenschaft haben: Ist M eine Menge mit einer Verküpfung $*_M$ und N eine Menge mit einer Verknüpfung $*_N$, so ist eine Abbildung von Mengen $f : M \to N$ mit diesen Verknüpfungen verträglich, falls gilt

$$f(m *_M m') = f(m) *_N f(m'),\ m, m' \in M,$$

d.h. es ist egal, ob man in M verknüpft und dann abbildet oder zuerst abbildet und dann in N verknüpft. Weiter sollte eine solche Abbildung das neutrale Element e_M bzgl. $*_M$ auf das neutrale Element e_N bzgl. $*_N$ abbilden. Die strukturerhaltenden Abbildungen werden Homomorphismen genannt.

Zum Beispiel: Sind G, H Gruppen, so ist ein Gruppenhomomorphismus eine Abbildung $f : G \to H$, sodass für alle $g, g' \in G$ gilt

$$f(g \cdot g') = f(g) \cdot f(g'),$$

(wegen $1_H \cdot f(1_G) = f(1_G \cdot 1_G) = f(1_G) \cdot f(1_G)$ gilt $f(1_G) = 1_H$).

Sind K, L Körper, so ist ein Körperhomomorphismus eine Abbildung $f : K \to L$, sodass für alle $a, b \in K$ die folgenden Formeln gelten

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

(wie oben folgt dann auch $f(1_K) = 1_L$).

Mittels strukturerhaltender Abbildung ergibt sich ein evidenter Begriff von 'gleichwertigen' oder 'isomorphen' algebraischen Strukturen: gibt es eine bijektive Abbildung (die beiden Mengen haben 'gleichviele' Elemente) die strukturerhaltend ist (es ist egal wo man verknüpft), so sind die Strukturen isomorph (aber nicht unbedingt identisch).

Wir betrachten strukturerhaltende Abbildungen von Vektorräume.

Definition 5.1. Sei K ein Körper und seien V, W K-Vektorräume.

(1) Eine Abbildung $f : V \to W$ heisst linear (oder Homomorphismus), falls für alle $a_1, a_2, a \in V$ und $\alpha \in K$ gilt:

$$f(a_1 + a_2) = f(a_1) + f(a_2) \text{ und } f(\alpha \cdot a) = \alpha \cdot f(a).$$

Sei $Hom(V, W) = Hom_K(V, W)$ die Menge aller linearen Abbildungen von V nach W; ist $V = W$, so schreibe $End_K(V) =$

$Hom_K(V,V)$, die Elemente von $End_K(V)$ sind die Endomorphismen von V.

(2) Ist $f \in Hom_K(V,W)$, so definiere Kern und Bild von f als

$$\begin{aligned} \ker(f) &= \{a \in V \mid f(a) = 0\} \subseteq V, \\ \mathrm{im}(f) &= \{f(a) \mid a \in V\} \subseteq W. \end{aligned}$$

(3) Sei $f \in Hom_K(V,W)$. Ist f mengentheoretisch injektiv (bzw. surjektiv), so heisst f Monomorphismus (bzw. Epimorphismus). Ist f bijektiv, so ist f ein Isomorphismus. Gibt es einen Isomorphismus $f : V \to W$, so sind V und W isomorph, $V \cong W$.

• Ist $f \in Hom_K(V,W)$, so gilt $f(0) = 0$ und $f(-a) = -f(a)$.

Lemma 5.2. *Seien V, W K-Vektorräume und sei $f \in Hom_K(V,W)$.*

(a) $\ker(f) \subseteq V$ *und* $\mathrm{im}(f) \subseteq W$ *sind lineare Unterräume.*

(b) f *ist ein Monomorphismus* $\Leftrightarrow \ker(f) = \{0\}$.

Beweis. (a): Wegen $0 = f(0)$ ist $0 \in \ker(f)$ und $\ker(f) \neq \emptyset$. Sind $a_1, a_2 \in \ker(f)$, so ist wegen $f(a_1 + a_2) = f(a_1) + f(a_2) = 0 + 0 = 0$ auch $a_1 + a_2 \in \ker(f)$. Für $a \in \ker(f)$ und $\alpha \in K$ ist $f(\alpha a) = \alpha f(a) = \alpha \cdot 0 = 0$, d.h. $\alpha a \in \ker(f)$. Der Beweis für $\mathrm{im}(f)$ ist ähnlich einfach.

(b): Ist f ein Monomorphismus und $a \in \ker(f)$, so ist $f(a) = 0 = f(0)$ und da f injektiv ist folgt $a = 0$, also ist $\ker(f) = \{0\}$. Sei umgekehrt $\ker(f) = \{0\}$. Sind $a_1, a_2 \in V$ mit $f(a_1) = f(a_2)$, so ist $0 = f(a_1) - f(a_2) = f(a_1 - a_2)$, d.h. $a_1 - a_2 \in \ker(f) = \{0\}$ und somit $a_1 = a_2$, d.h. f ist ein Monomorphismus. □

Beispiele 5.3. (a) Einfache Beispiele von linearen Abbildungen sind die Identität $\mathrm{id} : V \to V, a \mapsto a$ und die Nullabbildung $f : V \to W, a \mapsto 0$; ist $U \subseteq V$ ein Untervektorraum, so ist die Inklusion $i : U \to V$ linear.

(b) Sei $V = \mathbb{R}^3$ und $W = \mathbb{R}^2$. Seien $\alpha_{ij} \in \mathbb{R}, i = 1,2, j = 1,2,3$ gegeben. Wir ordnen diese Skalare als ein formales Schema an und betrachten die Elemente von V und W als Spaltenvektoren (x_j) und (y_i). Setze

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} \alpha_{11}x_1 + \alpha_{12}x_2 + \alpha_{13}x_3 \\ \alpha_{21}x_1 + \alpha_{22}x_2 + \alpha_{23}x_3 \end{pmatrix}$$

Dann definiert das obige Zuordnungsschema eine lineare Abbildung

$$f : \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} \alpha_{11}x_1 + \alpha_{12}x_2 + \alpha_{13}x_3 \\ \alpha_{21}x_1 + \alpha_{22}x_2 + \alpha_{23}x_3 \end{pmatrix}$$

Konkret ergibt sich damit für die folgende Wahl der Skalare

$$\begin{array}{lll} \alpha_{11} = 1 & \alpha_{12} = 2 & \alpha_{13} = -4 \\ \alpha_{21} = -7 & \alpha_{22} = 8 & \alpha_{23} = -10 \end{array}$$

die lineare Abbildung

$$f : \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 2 & -4 \\ -7 & 8 & -10 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1 + 2x_2 - 4x_3 \\ -7x_1 + 8x_2 - 10x_3 \end{pmatrix}.$$

Allgemein lassen sich so lineare Abbildungen $f : V = K^n \to K^m = W$ definieren: Sind $\alpha_{ij} \in K$, $i = 1, \ldots, m$, $j = 1, \ldots n$ fest gewählte Skalare, $(x_j) \in V$ und $(y_i) \in W$ Vektoren, so liefert die Zuordnung

$$f(x_j) = (y_i) \text{ mit } y_i = \sum_{j=1}^{n} \alpha_{ij} x_j,\ i = 1, \ldots m,$$

ein Element von $Hom_K(V, W)$. Der Kern von f sind die genau die gemeinsamen Lösungen der m Gleichungen

$$\sum_{j=1}^{n} \alpha_{ij} x_j = 0,\ i = 1, \ldots, m;$$

das Bild von f besteht aus genau denjenigen Vektoren (b_i), sodass

$$\sum_{j=1}^{n} \alpha_{ij} x_j = b_i,\ i = 1, \ldots m,$$

eine Lösung haben. Wir werden zeigen, dass jede lineare Abbildung $K^n \to K^m$ diese Form hat und Techniken zur Lösung solcher Gleichungssysteme entwickeln.

Das nächste wichtige Lemma zeigt, dass eine lineare Abbildung auf einer Basis festgelegt ist und man dabei eine solche lineare Abbildung durch beliebige Werte auf einer Basis vorgeben kann.

Lemma 5.4. *Seien V und W K-Vektorräume, $\{a_j \mid j \in J\}$ eine Basis von V und $\{b_i \mid i \in I\}$ eine Basis von W.*

(a) *Seien $c_j \in W$, $j \in J$ beliebig vorgegeben. Dann gibt es genau eine lineare Abbildung $f : V \to W$ mit $f(a_j) = c_j$ für $j \in J$.*

(b) *Seien $\alpha_{ij} \in K, i \in I, j \in J$, sodass für $j \in J$ nur endlich viele $\alpha_{ij} \neq 0$ sind. Dann gibt es genau ein $f \in Hom_K(V, W)$ mit*

$$f(a_j) = \sum_{i \in I} \alpha_{ij} b_i,\ j \in J.$$

NB. Seien $\{a_1, \ldots, a_n\}$ und $\{b_1, \ldots, b_m\}$ Basen von V und W. Nach (a) ist eine lineare Abbildung $f : V \to W$ durch die Bilder der Basisvektoren eindeutig bestimmt. Jedes der Bilder $f(a_j)$ besitzt eine eindeutige Darstellung als Linearkombination der b_j; d.h. für $j = 1, \ldots n$ ist somit

$$f(a_j) = \sum_{i=1}^{m} \alpha_{ij} b_i.$$

Wir ordnen die Skalare $\alpha_{1j}, \ldots \alpha_{mj}$ $(j = 1, \ldots n)$ die für diese Darstellung des j-ten Basisvektoren auftreten als die Spalten einer sogenannten Matrix an:

$$(\alpha_{ij}) = \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1m} \\ \alpha_{21} & \cdots & \alpha_{2m} \\ \cdots & \cdots & \cdots \\ \alpha_{m1} & \cdots & \alpha_{mn} \end{pmatrix}$$

Damit lässt sich die lineare Abbildung f bzgl. dieser Basen durch eine solche Matrix darstellen; wir werden die Frage, wie man durch eine geschickte Wahl dieser Basen eine 'einfache' Matrix bekommt später studieren. Umgekehrt besagt (b), dass ein Schema der Form (α_{ij}) eine eindeutige lineare Abbildung bestimmt.

Beweis. (a): Jeder Vektor $a \in V$ hat die Form $a = \sum_{k=1}^{n} \alpha_k a_k$. Ist $f : V \to W$ eine lineare Abbildung mit $f(a_i) = c_i$, so liefert die Linearität

$$f(a) = f(\sum_{k=1}^{n} \alpha_k a_k) = \sum_{k=1}^{n} \alpha_k f(a_k) = \sum_{k=1}^{n} \alpha_k c_k.$$

Also ist f durch die Werte $f(a_k)$ auf den Basiselementen a_k eindeutig festgelegt, d.h. falls es ein f mit $f(a_i) = c_i$ gibt, so ist f dadurch eindeutig bestimmt. Andererseits ist gerade die oben definierte Abbildung

$$f(a) = \sum_{k=1}^{n} \alpha_k c_k$$

linear: Sind $a = \sum_{k=1}^{n} \alpha_k a_k,\ a' = \sum_{k=1}^{m} \alpha'_k a_k$ Vektoren in V, so ist

$$a + a' = \sum_{k=1}^{n} \alpha_k a_k + \sum_{k=1}^{m} \alpha'_k a_k = \sum_{<\infty} (\alpha + \alpha') a_k$$

die eindeutige Darstellung von $a+a'$ als endliche Linearkombination der Basiselemente a_i ist. Nach Definition von f folgt dann sofort $f(a+a') = f(a) + f(a')$. Ein ähnliches Argument zeigt $\alpha f(a) = f(\alpha a)$.
(b): Folgt aus (a) mit $c_j = \sum_{j \in J} \alpha_{ij} b_i$. □

Beispiel 5.5. Betrachte die Abbildung $f : \mathbb{R}^2 \to \mathbb{R}^2,\ v \mapsto 2v$; offensichtlich ist f linear. Bzgl. der Basis $\{(1,0),(0,1)\}$ von $\mathbb{R}^2$ auf (beiden Seiten) ergibt sich

$$\begin{aligned}(1,0) &\mapsto (2,0) = 2\cdot(1,0) + 0\cdot(0,1),\\ (0,1) &\mapsto (0,2) = 0\cdot(1,0) + 2\cdot(0,1),\end{aligned}$$

also ist die Matrixdarstellung von f bzgl. $\{(1,0),(0,1)\}$ damit

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

Wählt man $\{(1,0),(0,1)\}$ als Basis für den 'Definitionsbereich' $\mathbb{R}^2$ und $\{(1,0),(1,1)\}$ als Basis für den 'Zielbereich' $\mathbb{R}^2$, so ist wegen

$$\begin{aligned}(1,0) &\mapsto (2,0) = 2\cdot(1,0) + 0\cdot(0,1),\\ (0,1) &\mapsto (0,2) = -2\cdot(1,0) + 2\cdot(1,1),\end{aligned}$$

die entsprechende Matrix

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

Theorem 5.6. *Seien V und W K-Vektorräume, und sei $\dim_K V = n < \infty$. Dann sind gleichwertig*

(a) $\dim_K W = n$,

(b) *Es gibt einen Isomorphismus $f : V \to W$, d.h. $V \cong W$.*

NB. Das Theorem besagt insbesondere, dass jeder n-dimensionale K-Vektorraum isomorph zu K^n ist. Der Beweis zeigt: jeder Isomorphismus bildet eine Basis wieder auf eine Basis ab; damit gilt für isomorphe K-Vektorräume $V \cong W$ (beliebiger Dimension) stets $\dim_K V = \dim_K W$.

Beweis. Sei $\dim_K W = n$ und seien $\{a_1,\dots,a_n\}$ und $\{b_1,\dots,b_n\}$ Basen von V und W. Nach Lemma 5.4(a) gibt es genau eine lineare Abbildung $f : V \to W$ mit $f(a_i) = b_i$ für $i = 1,\dots,n$. Wir zeigen f ist ein Epimorphismus: Ist $b = \sum_{i=1}^n \beta_i b_i \in W$, so gilt für $a = \sum_{i=1}^n \beta_i a_i \in V$

$$f(a) = \sum_{i=1}^n \beta_i f(a_i) = \sum_{i=1}^n \beta_i b_i = b.$$

Um zu zeigen, dass f ein Monomorphismus ist, genügt es nach Lemma 5.2(b) zu zeigen, dass $\ker(f) = \{0\}$ ist. Sei $a = \sum_{i=1}^n \alpha_i a_i \in \ker(f)$, sodass

$$0 = f(a) = \sum_{i=1}^n \alpha_i f(a_i) = \sum_{i=1}^n \alpha_i b_i;$$

da die b_i linear unabhängig sind folgt $\alpha_i = 0$ für alle i, d.h. $a = 0$.

Sei umgekehrt ein Isomorphismus $F : V \to W$ gegeben. Sei $b \in W$. Da f ein Epimorphismus ist gibt es ein $a \in V$ mit $f(a) = b$. Ist $\{a_1, \ldots, a_n\}$ eine Basis von V und $a = \sum_{i=1}^n \alpha_i a_i$, so folgt $b = f(a) = \sum_{i=1}^n \alpha_i f(a_i)$, also ist $b \in \langle f(a_1), \ldots, f(a_n)\rangle$ und da $b \in W$ beliebig war folgt $\langle f(a_1), \ldots, f(a_n)\rangle = W$. Wir zeigen $f(a_1), \ldots, f(a_n)$ sind linear unabhängig und bilden somit eine Basis: Angenommen

$$0 = \sum_{i=1}^n \alpha_i f(a_i) = f(\sum_{i=1}^n \alpha_i a_i).$$

Dann ist $\sum_{i=1}^n \alpha_i a_i \in \ker(f)$. Da f ein Monomorphismus ist zeigt nochmalige Anwendung von Lemma 5.2(b), dass $\ker(f) = \{0\}$ ist, also ist $\sum_{i=1}^n \alpha_i a_i = 0$ und da die a_i linear unabhängig sind folgt $\alpha_i = 0$ für alle i, d.h. $f(a_1), \ldots, f(a_n)$ sind linear unabhängig. □

Eine lineare Abbildung $f : V \to W$ ist durch die linearen Unterräume $\mathrm{im}(f) \subseteq W$ und $\ker(f) \subseteq V$ charakterisiert; das Bild $\mathrm{im}(f)$ sind die in W 'sichtbaren' Elemente, der Kern $\ker(f)$ die Elemente in V, die in W 'verlorengehen' (d.h. kein nicht-triviales Bild haben). Um diese linearen Räume studieren zu können führen wir Faktorräume ein.

Die Idee hier ist die, $\mathrm{im}(f)$ mit einem Quotienten- oder Faktorraum $V/\ker(f)$ zu identifizieren. Jeder lineare Unterraum $U \subseteq V$ ist insbesondere eine abelsche Untergruppe, sodass nach Lemma 2.6 $a_1 \sim a_2 \Leftrightarrow a_1 - a_2 \in U$ eine Äquivalenzrelation auf V definiert. Betrachte die Menge der (verschiedenen) Äquivalenzklassen

$$V/U = \{a + U \mid a \in V\},$$

zusammen mit der *surjektive* Abbildung $V \to V/U,\ a \mapsto a + U$.

Wir zeigen, dass die Addition und Skalarmultiplikation auf V analog eine Addition und Skalarmultiplikation auf V/U induziert, sodass V/U ein K-Vektorraum und $f : V \to V/U$ eine lineare Abbildung ist.

Definition 5.7. Sei V ein K-Vektorraum und $U \subseteq V$ ein linearer Unterraum. Für $a \in V$ setze $a + U = \{a + u \mid u \in U\} \subseteq V$. Der Quotienten- oder Faktorraum von V nach U ist die Menge

$$V/U = \{a + U \mid a \in V\}.$$

• Nach den obigen Vorbemerkungen gilt: $V = \dot{\bigcup}_{a \in V} (a + U)$ (Partition).

Lemma 5.8. *Sei V ein K-Vektorraum und $U \subseteq V$ ein linearer Unterraum. Dann ist der Faktorraum V/U ein K-Vektorraum mittels*

$$(a_1 + U) + (a_2 + U) = (a_1 + a_2) + U \text{ und } \alpha(a + U) = \alpha a + U.$$

Die Abbildung $q : V \to V/U,\ a \mapsto a + U$ ist ein Epimorphismus.

Beweis. Zu zeigen ist zunächst, dass die Operationen auf V/U wohldefiniert sind. Ist $a_1 + U = a_1' + U$ und $a_2 + U = a_2' + U$, so ist $a_1 - a_1' = u_1 \in U$ und $a_2 - a_2' = u_2 \in U$. Damit folgt

$$(a_1 + a_2) + U - [(a_1' + a_2') + U] = (u_1 + U) - (u_2 + U) = U.$$

Ähnlich für die Skalarmultiplikation: Ist $a_1 + U = a_2 + U$, also $a_1 - a_2 = u \in U$, so ist auch $\alpha(a_1 - a_2) = \alpha u \in U$, und damit $\alpha a_1 + U = \alpha a_2 + U$.

Weiter ist V/U mit dieser Addition und Skalarmultplikation ein K-Vektorraum; dies folgt, da diese Operationen von den entsprechenden Operationen auf dem K-Vektorraum V induziert sind. Zum Beispiel,

$$\alpha((a_1 + U) + (a_2 + U)) = \alpha(a_1 + U) + \alpha(a_2 + U)$$

da in V gilt $\alpha(a_1 + a_2) = \alpha a_1 + \alpha a_2$. Aus dem gleichen Grund ist die (surjektive) Abbildung $q : V \to V/U,\ a \mapsto a + U$ linear, d.h. ein Epimorphismus. □

Lemma 5.9. *Sei V ein K-Vektorraum und seien $U \subseteq W \subseteq V$ lineare Unterräume. Dann gilt:*

(a) *Sei $\{w_i + U \mid i \in I\}$ eine Basis von W/U und $\{v_j + W \mid j \in J\}$ eine Basis von V/W. Dann ist $\{w_i + U, v_j + U \mid i \in I, j \in J\}$ eine Basis von V/U.*
(b) *Ist $\dim V/U = n < \infty$, so ist $\dim V/U = \dim V - \dim U$.*
(c) *Ist $\dim V = n < \infty$, so ist $\dim V/W = \dim V - \dim W$.*

Beweis. (a): Ist $a \in V$, so ist $a + W = \sum_{j=1}^{n} \alpha_j (v_j + W)$ mit $\alpha_j \in K$ und $a - \sum_{j=1}^{n} \alpha_j v_j \in W$. Damit gibt es Skalare $\beta_i \in K$, sodass

$$(a - \sum_{j=1}^{n} \alpha_j v_j) + U = \sum_{i=1}^{m} \beta_i (w_i + U),$$

und weiter

$$a + U = \sum_{j=1}^{n} \alpha_j (v_j + U) + \sum_{i=1}^{m} \beta_i (w_i + U),$$

d.h. $V/U = \langle v_j + U, w_i + U \mid i \in I, j \in J \rangle$. Wir zeigen die $\{v_j + U, u_i + U \mid j \in J, i \in I\}$ sind linear unabhängig. Angenommen in V/U gilt

$$\sum_{j=1}^{n} \alpha_j (v_j + U) + \sum_{i=1}^{m} \beta_i (w_i + U) = 0$$

mit $\alpha_j, \beta_j \in K$. Es folgt $\sum_{j=1}^{n} \alpha_j v_j + \sum_{i=1}^{m} \beta_i w_i \in U$. Da $W \subseteq V$ ein linearer Unterraum ist folgt aus $w_i \in W$ dann auch $\sum_{i=1}^{m} \beta_i w_i \in W$ und in V/W gilt $\sum_{j=1}^{n} \alpha_j (v_j + W) = 0$. Da die $\{v_j + W \mid j \in J\}$

eine Basis von V/W bilden liefert dies $\alpha_j = 0$ für $j = 1, \dots n$. Wegen $w_i + U \in W/U$ ergibt sich jetzt in W/U die Identität

$$\sum_{i=1}^{m} \beta_i (w_i + U) = 0$$

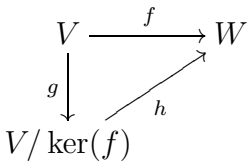
und da die $\{w_i + U\}$ eine Basis von W/U bilden gilt $\beta_i = 0$ für $i = 1, \dots m$; dies beweist die Behauptung.

(b): Folgt aus (a).

(c): Ist der Spezialfall $U = \{0\}$ von (b). □

Theorem 5.10. *(Homomorphiesatz) Seien V, W K-Vektorräume und sei $f \in Hom_K(V, W)$.*

(a) *Es gibt einen Epimorphismus $g : V \to V/\ker(f)$ und einen Monomorphismus $h : V/\ker(f) \to W$, sodass $f = h \circ g$ und $\mathrm{im}(f) = \mathrm{im}(h)$ ist, d.h. das folgende Diagramm kommutiert*



(b) *Ist $\dim_K V = n < \infty$, so gilt die Formel:*

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

• Es folgt: $h : V/\ker(f) \to \mathrm{im}(f)$ ist ein Isomorphismus.

Beweis. (a): Die Abbildung $g : V \to V/\ker(f)$ ist der evidente Epimorphismus $a \mapsto a + \ker(f)$. Die einzige Abbildung $h : V/\ker(f) \to W$, die die gewünschten Eigenschaften haben könnte ist definert durch

$$h : V/\ker(f) \to W,\ a + \ker(f) \mapsto f(a).$$

Zu zeigen ist: h ist ein wohldefinierter Monomorphismus. Sei $a_1 + \ker(f) = a_2 + \ker(f)$. Dann ist $a_1 - a_2 \in \ker(f)$ und es folgt

$$h(a_1 + \ker(f)) - h(a_2 + \ker(f)) = f(a_1) - f(a_2) = f(a_1 - a_2) = 0,$$

d.h. h ist wohldefiniert. Weiter ist h linear, da f linear ist; es ist

$$\begin{aligned} h(\alpha(a + \ker(f)) &= h(\alpha a + \ker(f)) = f(\alpha a) = \alpha f(a) = \\ &= \alpha h(a + \ker(f)); \end{aligned}$$

und ähnlich für die Addition. Nach Konstruktion gilt für jedes $a \in V$

$$(h \circ g)(a) = h(a + \ker(f)) = f(a),$$

also ist $f = h \circ g$ und $\mathrm{im}(f) = \mathrm{im}(h)$. Ist $a + \ker(f) \in \ker(h)$, so ist

$$0 = h(a + \ker(f)) = f(a),$$

d.h. $a + \ker(f) = \ker(f)$ und h ist ein Monomorphismus.
(b): Ist $\dim V = n < \infty$, so ist nach (a) $\mathrm{im}(f) \cong V/\ker(f)$, also $\dim \mathrm{im}(f) = \dim(V/\ker(f))$, und wegen Lemma 5.9(c) gilt

$$\dim \mathrm{im}(f) = \dim(V/\ker(f)) = \dim V - \dim \ker(f)$$

□

Lemma 5.11. *Seien V, W K-Vektorräume mit $\dim_K V = \dim_K W = n < \infty$ und sei $f \in Hom_K(V, W)$. Dann sind gleichwertig:*

(a) *f ist ein Isomorphismus,*
(b) *f ist ein Monomorphismus,*
(c) *f ist ein Epimorphismus.*

Beweis. (a) ⇒ (b): Trivial. (b)⇒ (c): Ist f ein Monomorphismus, so ist $\ker(f) = \{0\}$. Aus dem Homomorphiesatz 5.10 folgt $\dim \mathrm{im}(f) = \dim V = \dim W$, sodass nach Theorem 5.6 $\mathrm{im}(f) \cong W$ gilt, also ist f ein Epimorphismus. (c)⇒ (a): Ist f ein Epimorphismus, so ist $\dim \mathrm{im}(f) = \dim W = \dim V$, und der Homomorphiesatz 5.10 liefert $\dim \ker(f) = 0$, d.h. $\ker(f) = \{0\}$ und f ist ein Monomorphismus. □

Wir geben eine geometrische Interpretation von Faktorräumen.

Definition 5.12. Sei V ein K-Vektorraum, $U \subseteq V$ ein linearer Unterraum und $a \in V$. Ein affiner Unterraum $A \subseteq V$ ist eine Teilmenge der Form

$$A = a + U = \{a + u \mid u \in U\} \subseteq V.$$

NB. Jedes Element $a + U$ des Faktorraums V/U ist ein affiner Unterraum.

• Sei $V = \mathbb{R}^2$ und sei $U = \{(a', 0) \mid a' \in \mathbb{R}\} \subseteq V$, d.h. U ist die x-Achse. Dann ist $(1, 0) + U = (1, 1) + U$, und allgemein

$$\begin{aligned}(a, b) + U &= \{(a, b) + (a', 0) \mid a' \in \mathbb{R}\} = \{(a + a', b) \mid a' \in \mathbb{R}\} = \\ &= \{(a'', b) \mid a'' \in \mathbb{R}\} = U \times \{b\},\end{aligned}$$

d.h. die affinen Unterräume $(a, b) + U$ sind 'Parallelverschiebungen' des A definierenden Unterraums U.
• Ist $A = a + U \subseteq V$ ein affiner Unterraum, so ist U eindeutig durch A bestimmt: Sei $A = a + U = a' + U'$, wir zeigen $U = U'$. Nach Annahme ist $a - a' + U = U'$, also gibt es ein $u \in U$ mit $a - a' + u = 0$. Da U ein linearer Unterraum ist folgt $a - a' = -u \in U$, und damit $U = U'$.
• Da für $A = a + U$ der lineare Unterraum U eindeutig durch A bestimmt ist, lässt sich dem affinen Unterraum A eine Dimension zuordnen: $\dim_K A = \dim_K U$. Ein affiner Unterraum der Dimension 1 ist eine affine Gerade; im Fall $\dim_K V = n < \infty$ ist ein affiner Unterraum

der Dimension $\dim_K V - 1$ eine affine Hyperebene.

• Sei $f : V \to W$ eine lineare Abbildung. Das Urbild von $f(0) = 0$

$$f^{-1}(f(0)) = f^{-1}(0) = \ker(f) \subseteq V$$

ist ein linearer Unterraum. Ist $a \in V$ ein beliebiger Vektor, so ist

$$f^{-1}(f(a)) = \{a + u \mid u \in \ker(f)\} = a + \ker(f)$$

ein affiner Unterraum, dies ist die Faser von f über a.

NB. Ist $f : V \to W$ linear, so ist $f : V \to \mathrm{im}(f)$ surjektiv und zu jedem $b \in \mathrm{im}(f)$ gibt es ein $a \in V$ mit $f(a) = b$, d.h. über jedem $b \in \mathrm{im}(f)$ liegt genau eine Faser $f^{-1}(b) = a + \ker(f)$. Die Abbildung $b \mapsto f^{-1}(b)$ induziert eine Bijektion zwischen den Elementen von $\mathrm{im}(f)$ und den Elementen des Faktorraums $V/\ker(f)$. Die Aussage des Homomorphiesatzes ist, dass diese Bijektion einen Isomorphismus $V/\ker(f) \cong \mathrm{im}(f)$ von Vektorräumen liefert.

Lemma 5.13. *Sei V ein K-Vektorraum und $\emptyset \neq A \subseteq V$ eine Teilmenge. Dann sind gleichwertig:*

(a) *A ist affiner Unterraum, d.h. es gibt einen linearen Unterraum $U \subseteq V$ und ein $a \in V$ mit $A = a + U$,*

(b) *Es gibt eine lineare Abbildung $f : V \to W$, sodass A eine Faser von f ist, d.h. $A = f^{-1}(b)$ für ein $b \in W$,*

(c) *Seien $a_0, \ldots, a_k \in A$ und $\alpha_0, \ldots, \alpha_k \in K$ mit $\sum_{i=0}^k \alpha_i = 1$. Dann ist $\sum_{i=0}^k \alpha_i a_i \in A$.*

Beweis. $(a) \Rightarrow (b)$: Sei $A = a + U$. Für den Epimorphismus $f : V \to V/U,\ a \mapsto a + U$ gilt $f^{-1}(f(a)) = a + \ker(f) = a + U = A$.

$(b) \Rightarrow (c)$: Sei $A = f^{-1}(b)$ für ein $b \in W$. Seien $a_0, \ldots, a_k \in A$ und $\alpha_0, \ldots, \alpha_k \in K$ mit $\sum_{i=1}^k \alpha_i = 1$ gegeben. Die Linearität von f liefert

$$f(\sum_{i=0}^{k} \alpha_i a_i) = \sum_{i=0}^{k} \alpha_i f(a_i) = (\sum_{i=1}^{k} \alpha_i) b = 1 \cdot b = b,$$

d.h. $\sum_{i=0}^k \alpha_i a_i \in f^{-1}(b) = A$.

$(c) \Rightarrow (a)$: Wähle fest ein $a_0 \in A$ und betrachte die Menge $\Delta A = \{a - a_0 \mid a \in A\} \subseteq V$. Es ist $A = a_0 + \Delta A$; wir zeigen $\Delta A \subseteq V$ ist ein linearer Unterraum. Wegen $a_0 \in A$ ist $0 \in \Delta A$, also ist $\Delta A \neq \emptyset$. Für $a_1 - a_0, a_2 - a_0 \in \Delta A$ ist nach (c) $a_1 + (-1)a_0 + a_2 \in A$, sodass

$$(a_1 - a_0) + (a_2 - a_0) = (a_1 - a_0 + a_2) - a_0 \in \Delta A.$$

Für $\alpha \in K$ folgt aus (c) weiter $\alpha a_1 + (1 - \alpha)a_0 \in A$; somit gilt

$$\alpha(a_1 - a_0) = (\alpha a_1 + (1 - \alpha)a_0) - a_0 \in \Delta A.$$

□

Beispiel 5.14. Sei V ein K-Vektorraum und $a_0, \ldots, a_k \in V$. Dann ist der kleinste affine Unterraum der die Vektoren $a_0, \ldots, a_k$ enthält

$$A = \{a_0 + \sum_{i=1}^{k} \alpha_i(a_i - a_0) \mid \alpha_1, \ldots, \alpha_k \in K\} \subseteq V.$$

Nach Definition ist $A = a_0 + U$, wobei U der von den Vektoren $a_1 - a_0, \ldots, a_k - a_0$ erzeugte lineare Unterraum ist, d.h. A ist affiner Unterraum. Da $a_0 + \sum_{i=1}^{k} \alpha_i(a_i - a_0) = (1 - \sum_{i=1}^{k} \alpha_i)a_0 + \sum_{i=1}^{k} \alpha_i a_i$ folgt

$$A = \{\sum_{i=0}^{k} \alpha_i a_i \mid \alpha_0, \ldots, \alpha_k \in K \text{ mit } \sum_{i=0}^{k} \alpha_i = 1\}.$$

Nach Lemma 5.13(c) ist dies der kleinste affine Unterraum, der die Vektoren $a_0, \ldots, a_k$ enthält. Konkret: Sei $V = \mathbb{R}^2$ und seien $a_0, a_1 \in \mathbb{R}^2$ zwei Punkte. Der kleinste affine Unterraum der a_0 und a_1 enthält ist

$$A = \{a_0 + \alpha(a_1 - a_0) \mid \alpha \in \mathbb{R}\} = \{\alpha a_0 + \beta a_1 \mid \alpha, \beta \in \mathbb{R}, \alpha + \beta = 1\},$$

d.h. die affine Gerade durch die Punkte a_0 und a_1.

6. Lineare Abbildungen und Matrizen

Wir studieren lineare Abildungen und zeigen dazu zunächst, dass die Menge der K-linearen Abbildungen $Hom_K(V, W)$ selbst ein K-Vektorraum ist. Damit hat $Hom_K(V, W)$ eine Basis und jede lineare Abbildung $V \to W$ hat eine Darstellung als eine endliche Linearkombination von Basiselementen.

Lemma 6.1. *Seien V, W K-Vektorräume.*

(a) *Für $f, g \in Hom_K(V, W)$, $\alpha \in K$ und $a \in V$ setze*

$$(f + g)(a) = f(a) + g(a) \text{ und } (\alpha f)(a) = \alpha f(a);$$

mit diesen Operationen ist $Hom_K(V, W)$ ein K-Vektorraum.

(b) *Seien $\{a_1, \ldots, a_n\} \subseteq V$ und $\{b_1, \ldots, b_m\} \subseteq W$ Basen. Für $j = 1, \ldots, n$ und $i = 1, \ldots, m$ definiere $e_{ij} \in Hom_K(V, W)$ durch*

$$e_{ij}(a_k) = \begin{cases} 0 & j \neq k \\ b_i & j = k \end{cases}$$

Dann ist $\{e_{11}, \ldots, e_{mn}\}$ eine Basis von $Hom_K(V, W)$; insbesondere gilt $\dim_K Hom_K(V, W) = \dim_K V \cdot \dim_K W$.

Beweis. (a): Nachrechnen.
(b): Ist $f \in Hom_K(V,W)$ so gilt bezüglich der gegebenen Basen

$$f(a_j) = \sum_{i=1}^{m} \alpha_{ij} b_i,\ j = 1, \dots n.$$

Für diese Koeffizienten $\alpha_{ij}, i = 1, \dots m, j = 1, \dots n$ bilde

$$g = \sum_{i=1}^{m} \sum_{j=1}^{n} \alpha_{ij} e_{ij}.$$

Nach Definition hat die lineare Abbildung g die Eigenschaft, dass

$$g(a_j) = \sum_{i=1}^{m} \sum_{j=1}^{n} \alpha_{ij} e_{ij}(a_j) = \sum_{i=1}^{m} \alpha_{ij} b_i = f(a_j),$$

d.h. $f = \sum_{i=1}^{m} \sum_{j=1}^{n} \alpha_{ij} e_{ij}$ und die e_{ij} erzeugen $Hom_K(V,W)$. Sei

$$\sum_{i=1}^{m} \sum_{j=1}^{n} \beta_{ij} e_{ij} = 0,\ \beta_{ij} \in K.$$

Evaluierung dieser Abbildung auf a_j liefert für $j = 1, \dots n$ die Identität

$$0 = \sum_{i=1}^{m} \sum_{j=1}^{n} \beta_{ij} e_{ij}(a_j) = \sum_{i=1}^{m} \beta_{ij} b_i.$$

Da die b_i linear unabhängig sind folgt $\beta_{ij} = 0$ für alle i, j, also sind $\{e_{11}, \dots, e_{mn}\}$ linear unabhängig und bilden eine Basis. □

Sind $f : V_1 \to V_2$ und $g : V_2 \to V_3$ lineare Abbildungen, so schreibe $gf = g \circ f : V_1 \to V_3$ für die Komposition. Diese Komposition ist allgmein für Abbildungen definiert; wir zeigen, das die Verknüpfung von linearen Abbildungen wieder linear, mit der Addition verträglich ,und assoziativ ist.

Lemma 6.2. *Seien V_i K-Vektorräume, $i = 1, 2, 3, 4$.*

(a) *Sind $g \in Hom_K(V_2, V_3)$ und $f \in Hom_K(V_1, V_2)$ so definiert*

$$(gf)(a_1) = g(f(a_1)),\ a_1 \in V_1$$

eine lineare Abbildung $fg \in Hom_K(V_1, V_3)$.

(b) *Ist $g \in Hom_k(V_2, V_3)$ und sind $f_1, f_2 \in Hom_K(V_1, V_2)$, so gilt*

$$g(f_1 + f_2) = gf_1 + gf_2.$$

(c) *Sind $g_1, g_2 \in Hom_K(V_2, V_3)$ und $f \in Hom_K(V_1, V_2)$, so gilt*

$$(g_1 + g_2)f = g_1 f + g_2 f.$$

(d) *Sei* $h \in Hom_K(V_3, V_4)$, $g \in Hom_K(V_2, V_3)$, $f \in Hom_K(V_1, V_2)$. *Dann ist*

$$h(gf) = (hg)f.$$

Beweis. Nachrechnen. □

Wir betrachten Isomorphismen in $Hom_K(V, W)$. Ist $f : V \to W$ ein Isomorphismus, so ist f eine bijektive Abbildung und hat damit eine inverse bijektive Abbildung $g = f^{-1} : W \to V$. Wir zeigen, dass diese Abbildung $g = f^{-1}$ ebenfalls linear ist. Damit gelten für Isomorphismen diesselben Beziehungen wie für bijektive Abbildungen von Mengen.

Lemma 6.3. *Seien* V_i K*-Vektorräume,* $i = 1, 2, 3$.

(a) *Sei* $f \in Hom_K(V_1, V_2)$ *ein Isomorphismus. Dann gibt es genau ein* $g \in Hom_K(V_2, V_1)$ *mit* $gf = \mathrm{id}_{V_1}$ *und* $fg = \mathrm{id}_{V_2}$*; setze* $g = f^{-1}$.

(b) *Sind* $f \in Hom_K(V_1, V_2)$ *und* $g \in Hom_K(V_2, V_3)$ *Isomorphismen, so ist auch* $gf \in Hom_K(V_1, V_3)$ *ein Isomorphismus; es gilt:* $(gf)^{-1} = f^{-1}g^{-1}$.

Beweis. (a): Da $f : V_1 \to V_2$ eine Bijektion ist, gibt es nach Lemma 1.12 genau eine Bijektion $g : V_2 \to V_1$ mit $gf = \mathrm{id}_{V_1}$ und $fg = \mathrm{id}_{V_2}$. Wir zeigen g, dass linear ist. Für $a_2, a_2' \in V_2$ gilt

$$\begin{aligned} f(g(a_2 + a_2')) &= (fg)(a_2 + a_2') = \mathrm{id}_{V_2}(a_2 + a_2') = \mathrm{id}_{V_2}(a_2) + \mathrm{id}_{V_2}(a_2') \\ &= f(g(a_2)) + f(g(a_2')) = f(g(a_2) + g(a_2')). \end{aligned}$$

Da f injektiv ist, folgt damit $g(a_2 + a_2') = g(a_2) + g(a_2')$. Ähnlich zeigt man $\alpha g(a_2) = g(\alpha a_2)$.

(b): Folgt aus der Bemerkung nach Definition 1.13. □

Beispiel 6.4. Im Fall $V = W$ ist $Hom_K(V, W) = End_K(V)$. Nach Lemma 6.1(a) ist $End_K(V)$ ein K-Vektorraum. Die Verknüpfung von Endomorphismen $f : V \to V$ liefert eine 'Multiplikation' auf $End_K(V)$

$$f, g \in End_K(V) \Rightarrow fg = f \circ g \in End_K(V)$$

mit Einselement $\mathrm{id}_V : V \to V$, $\mathrm{id}_V(a) = a$. Für diese Multiplikation gelten die beiden Distributivgesetzen und das Assoziativgesetz. Weiter ist diese Multiplikation mit der Skalarmultiplikation verträglich, d.h.

$$\alpha(fg) = (\alpha f)g = f(\alpha g);\ f, g \in End_K(V),\ \alpha \in K.$$

Ein K-Vektorraum, zusammen mit einer Multiplikation, welche die obigen Verträglichkeitsbedingungen erfüllt ist eine K-Algebra.

Das Kroneckersymbol δ_{jk} ist definiert als $\delta_{jk} = 1$ falls $j = k$ und

$\delta_{jk} = 0$ falls $j \neq k$. Ist $\{a_1, \ldots, a_n\}$ eine Basis von V, so bilden nach Lemma 6.1(b) die Endomorphismen $e_{ij} \in End_K(V)$ mit

$$e_{ij}(a_k) = \delta_{jk} a_i$$

eine Basis $\{e_{11}, \ldots, e_{nn}\}$ von $End_K(V)$; es ist $\dim_K End_K(V) = n^2$.

Für die Basiselemente $\{e_{ij}\}$ von $End_K(V)$ gelten die Formeln

$$e_{ij} e_{kl} = \delta_{jk} e_{il} \quad \text{und} \quad \sum_{i=1}^{n} e_{ii} = \mathrm{id}_V \,.$$

Ist $\dim_K V > 1$, so ist die Multiplikation via Verknüpfung von Abbildungen in $End_K(V)$ *nicht* kommutativ: Die obige Formel liefert $e_{12}e_{22} = \delta_{22}e_{12} = e_{12} \neq 0$ und $e_{22}e_{12} = \delta_{21}e_{22} = 0$, d.h. $e_{12}e_{22} \neq e_{22}e_{12}$.

Definition 6.5. Sei V ein K-Vektorraum. Ist $f \in End_K(V)$ ein Isomorphismus, so ist f regulär (auch 'invertierbar' bzw. 'Automorphismus'); ist f nicht regulär, so ist f singulär. Die regulären Abbildungen aus $End_K(V)$ bilden bzgl. der Verknüpfung von Endomorphismen eine multiplikative Gruppe mit neutralem Element id_V (vgl. Lemma 6.3); diese Gruppe bezeichnen wir mit $GL(V)$ (General Linear group).

Beispiel 6.6. Sei $K = \mathbb{Z}/p\mathbb{Z}$ der Körper mit p Elementen und sei V ein K-Vektorraum der Dimension n, d.h. $V \cong (\mathbb{Z}/p\mathbb{Z})^n$. Für zwei (beliebige) endlich-dimensionale K-Vektorräume V, W und $f \in Hom_K(V, W)$ gilt: f ist ein Isomorphismus genau dann, wenn f jede Basis von V auf eine Basis von W abbildet. Also ist die Anzahl der Elemente von $GL(V)$ genau die Anzahl der verschiedenen Basen von V. Jede Basis $\{a_1, \ldots, a_n\}$ von V entsteht durch Wahl der a_i wie folgt:

$0 \neq a_1 \in V$	$p^n - 1$	Möglichkeiten,
$a_1 \in V \setminus \langle a_1 \rangle$	$p^n - p$	Möglichkeiten,
$\cdots$	$\cdots$	$\cdots$
$\cdots$	$\cdots$	$\cdots$
$a_n \in V \setminus \langle a_1, \ldots, a_{n-1} \rangle$	$p^n - p^{n-1}$	Möglichkeiten.

Damit ist $|GL(V)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$.

Definition 6.7. Seien V, W K-Vektorräume und sei $f \in Hom_K(V, W)$. Ist $\dim_K \mathrm{im}(f) < \infty$, so ist der Rang $r(f)$ von f definiert als

$$r(f) = \dim_K \mathrm{im}(f).$$

- Wegen $\mathrm{im}(f) \subseteq W$ ist stets $r(f) \leq \dim_K W$.
- Aus dem Homomorphiesatz 5.10 folgt:

$$r(f) = \dim_K \mathrm{im}(f) = \dim_K V - \dim_K \ker(f)$$

Definition 6.8. Sei K ein Körper. Eine Matrix vom Typ (m,n) über K ist ein Schema von Skalaren $\alpha_{ij} \in K$ der folgenden Form

$$A = (\alpha_{ij}) = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \alpha_{m1} & \alpha_{m2}, & \dots & \alpha_{mn} \end{pmatrix},$$

d.h. eine Matrix $A = (\alpha_{ij})$ vom Typ (m,n) besteht aus m Zeilen

$$z_i = (\alpha_{i1}, \alpha_{i2}, \dots, \alpha_{in}),\ i = 1, \dots, m$$

und n Spalten

$$s_j = \begin{pmatrix} \alpha_{1j} \\ \alpha_{2j} \\ \cdot \\ \cdot \\ \alpha_{mj} \end{pmatrix},\ j = 1, \dots n.$$

Sei $K^{m\times n}$ die Menge aller Matrizen vom Typ (m,n) über K.

Beispiel 6.9. Sei $K = \mathbb{R}$ und $m = 2 = n$. Seien $A = (\alpha_{ij}), B = (\beta_{ij})$ Matrizen vom Typ $(2,2)$ über $\mathbb{R}$ und sei $\alpha \in \mathbb{R}$ ein Skalar. Setze

$$\begin{aligned} A + B &= \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix} + \begin{pmatrix} \beta_{11} & \beta_{12} \\ \beta_{21} & \beta_{22} \end{pmatrix} = \begin{pmatrix} \alpha_{11} + \beta_{11} & \alpha_{12} + \beta_{12} \\ \alpha_{21} + \beta_{21} & \alpha_{22} + \beta_{22} \end{pmatrix}, \\ \alpha A &= \alpha \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix} = \begin{pmatrix} \alpha\alpha_{11} & \alpha\alpha_{12} \\ \alpha\alpha_{21} & \alpha\alpha_{22} \end{pmatrix} \end{aligned}$$

Die Menge $\mathbb{R}^{2\times 2}$ der $(2,2)$-Matrizen über $\mathbb{R}$ ist mittels dieser Addition und Skalarmultplikation ein K-Vektorraum. Die Abbildung

$$\Theta : \mathbb{R}^{2\times 2} \to \mathbb{R}^4 : \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix} \mapsto (\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22})$$

ist ein Isomorphismus, also ist $\dim_{\mathbb{R}} \mathbb{R}^{2\times 2} = 4$. Ist $\{e_1, \dots, e_4\}$ die Standardbasis von $\mathbb{R}^4$, so sind die Urbilder $\Theta^{-1}(e_1), \dots \Theta^{-1}(e_4)$ genau die Matrizen E_{ij} mit einer 1 in der Stelle (i,j) und 0 sonst. Da Θ ein Isomorphismus ist bilden die $\{E_{11}, E_{12}, E_{21}, E_{22}\}$ eine Basis von $\mathbb{R}^{2\times 2}$.

Das obige Beispiel hängt weder von $K = \mathbb{R}$ noch von $m = 2 = n$ ab, d.h. die Eigenschaften aus diesem Beispiel gelten allgemein für die Matrizen $K^{m\times n}$ vom Typ (m,n); genauer:

• Die Menge $K^{m\times n}$ aller Matrizen vom Typ (m,n) ist mittels

$$(\alpha_{ij}) + (\beta_{ij}) = (\alpha_{ij} + \beta_{ij}) \text{ und } \alpha(\alpha_{ij}) = (\alpha\alpha_{ij})$$

ein K-Vektorraum. Die Abbildung $\Theta : K^{m\times n} \to K^{mn}$

$$(\alpha_{ij}) \mapsto (\alpha_{11}, \cdots, \alpha_{1n}, \alpha_{21}, \cdots, \alpha_{2n}, \cdots, \alpha_{m1}, \ldots, \alpha_{mn})$$

definiert einen Isomorphismus von K-Vektorräumen $K^{m\times n} \cong K^{mn}$. Insbesondere ist $\dim_K K^{m\times n} = mn$.

• Sei $E_{ij} \in K^{m\times n}$ die Matrix mit 1 an der Stelle (i, j) und 0 sonst. Dann bilden die E_{ij} $(i = 1, \ldots, m; j = 1, \ldots, n)$ eine Basis von $K^{m\times n}$.

Seien V, W K-Vektorräume mid $\dim_K V = n$ und $\dim_K W = m$. Wir ordnen einer linearen Abbildung $f : V \to W$ eine Matrix in $K^{m\times n}$ zu (abhängig von der Wahl von Basen von V und W), um dann lineare Abbildungen mittels dieser zugeordneten Matrizen studieren.

Definition 6.10. Seien V und W K-Vektorräume, $X = \{v_1, \ldots, v_n\}$ eine Basis von V und $Y = \{w_1, \ldots, w_m\}$ eine Basis von W. Für eine lineare Abbildung $f \in Hom_K(V, W)$ haben die Werte $f(v_j)$ eine eindeutige Darstellung als endliche Linearkombiniation der w_i, d.h.

$$f(v_j) = \sum_{i=1}^{m} \alpha_{ij} w_i, \ j = 1, \ldots n.$$

Setze $A = A_{f,X,Y} = (\alpha_{ij}) \in K^{m\times n}$; die Matrix $A_{f,X,Y}$ ist die Matrix von f bezüglich der Basen X und Y. Ist $V = W$ und $X = Y$, so schreibe $A_{f,X}$ für $A_{f,X,Y}$.

NB. Die Matrix $A_{f,X,Y}$ hängt von den Basen X, Y und von der Anordnung der Vektoren in diesen Basen ab.

Proposition 6.11. *Seien U, V, W K-Vektorräume mit Basen $X = \{u_1, \ldots, u_k\}, Y = \{v_1, \ldots, v_n\}$ und $Z = \{w_1, \ldots, w_m\}$. Dann gilt:*

(a) *Die Abbildung $\kappa : Hom_K(U, V) \to K^{n\times k}$, $f \mapsto A_{f,X,Y}$ ist ein Isomorphismus.*

(b) *Seien $g \in Hom_K(U, V)$ und $f \in Hom_K(V, W)$. Sind $A_{g,X,Y} = (\alpha_{ij})$ und $A_{f,X,Y} = (\beta_{rs})$, so ist $A_{fg,X,Z} = (c_{is})$ mit*

$$c_{is} = \sum_{j=1}^{n} \alpha_{ij} b_{js}.$$

Beweis. (a): Da $Hom_K(U, V)$ und $K^{n\times k}$ die gleiche Dimension kn haben, genügt es nach Lemma 5.11 zu zeigen, dass κ linear und ein Monomorphismus ist. Dabei ist die zweite Aussage trivial: Nach Definition ist $A_{f,X,Y} = 0$ die Nullmatrix genau dann, wenn $f = 0$ ist. Wir zeigen

die Abbildung κ ist linear: Seien $f_1, f_2 \in Hom_K(U,V)$ gegeben durch

$$f_1(u_j) = \sum_{i=1}^{n} \alpha_{ij} v_i \text{ und } f_2(u_j) = \sum_{i=1}^{n} \alpha'_{ij} v_i,\ j = 1, \dots n,$$

d.h. f_1 und f_2 entsprechen bzgl. der Basen X und Y den Matrizen

$$A_{f_1,X,Y} = (\alpha_{ij}) \text{ und } A_{f_2,X,Y} = (\alpha'_{ij}).$$

Dann gilt

$$(f_1 + f_2)(u_j) = \sum_{i=1}^{n} (\alpha_{ij} + \alpha'_{ij}) v_i,\ j = 1, \dots, n$$

also hat die lineare Abbildung $f_1 + f_2$ bzgl. X und Y die Matrix

$$A_{f_1+f_2,X,Y} = (\alpha_{ij} + \alpha'_{ij}) = (\alpha_{ij}) + (\alpha'_{ij}) = A_{f_1,X,Y} + A_{f_2,X,Y}$$

und es gilt $\kappa(f_1+f_2) = \kappa(f_1)+\kappa(f_2)$. Der Beweis von $\kappa(\alpha f_1) = \alpha\kappa(f_1)$, d.h. $A_{\ \alpha f_1,X,Y} = \alpha(A_{f_1,X,Y})$, ist ähnlich einfach.
(b): Aus $f(v_j) = \sum_{i=1}^{m} \alpha_{ij} w_i$ und $g(u_s) = \sum_{j=1}^{n} \beta_{js} v_j$ folgt

$$(fg)(u_s) = \sum_{j=1}^{n} (f(v_j)) = \sum_{j=1}^{n} \sum_{i=1}^{m} \beta_{js} \alpha_{ij} w_i = \sum_{i=1}^{m} (\sum_{j=1}^{n} \alpha_{ij} \beta_{js}) w_i,$$

dies zeigt $A_{fg,X,Z} = (c_{is})$ mit $c_{is} = \sum_{j=1}^{n} \alpha_{ij} \beta_{js}$. □

Der Beweis von (b) zeigt, wie Matrizen (von kompatiblem Typ) zu multiplizieren sind, sodass das entsprechende Produkt der Komposiition der zugrundeliegenden linearen Abbildungen entspricht. Dies motiviert folgende Definition des allgemeinen Matrizenprodukts.

Definition 6.12. Sei K ein Körper und seien $A = (\alpha_{ij}) \in K^{m\times n}$, sowie $B = (\beta_{jl}) \in K^{n\times k}$. Definere das Produkt $AB \in K^{m\times k}$ als die Matrix

$$AB = (c_{il}) \text{ mit } c_{il} = \sum_{j=1}^{n} \alpha_{ij} \beta_{jl}$$

• Sind $A = (\alpha_{ij}), A' = (\alpha'_{ij}) \in K^{m\times n}$ und $B = (\beta_{jl}), B' = (\beta'_{jl}) \in K^{n\times k}$, so gelten für die Matrixmultiplikation die beiden Distributivgesetze

$$(A + A')B = AB + A'B \text{ und } A(B + B') = AB + AB'.$$

• Für $A = (\alpha_{ij}) \in K^{m\times n}, B = (\beta_{jl}) \in K^{n\times k}$ und $C = (\gamma_{lr}) \in K^{k\times s}$ ist

$$A(BC) = (AB)C.$$

Beispiele 6.13. (a) Rein formal gilt

$$\begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} -2 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ -1 & 5 \end{pmatrix}$$

oder

$$\begin{pmatrix} 3 & 0 \\ 2 & 0 \\ 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 3 & -3 \\ 2 & -2 \\ 9 & 7 \end{pmatrix}.$$

(b) Betrachte die linearen Abbildungen

$$g : \mathbb{R}^3 \to \mathbb{R}^2, \quad \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \mapsto \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \ \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \mapsto \begin{pmatrix} 0 \\ 2 \end{pmatrix}, \ \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} 2 \\ 2 \end{pmatrix},$$

$$f : \mathbb{R}^2 \to \mathbb{R}^3, \quad \begin{pmatrix} 1 \\ 0 \end{pmatrix} \mapsto \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \ \begin{pmatrix} 0 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

Bezüglich der Standardbasen sind die g und f zugeordneten Matrizen

$$A_g = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 2 & 2 \end{pmatrix} \text{ und } A_f = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Für das Kompositum $fg : \mathbb{R}^3 \to \mathbb{R}^3$ gilt nach Definition von f und g

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \mapsto \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \ \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \mapsto \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}, \ \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} 4 \\ 2 \\ 0 \end{pmatrix},$$

also ist

$$A_{fg} = \begin{pmatrix} 1 & 2 & 4 \\ 1 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 2 \\ 0 & 2 & 2 \end{pmatrix} = A_f \cdot A_g.$$

Ist $\dim_K V = n < \infty$, so besagen die obigen Verträglichkeitsaussagen für Matrizen, dass $K^{n\times n}$ nicht nur ein K-Vektorraum, sondern auch eine K-Algebra ist, vgl. Beispiel 6.4. Dabei ist das Einselement in $K^{n\times n}$

$$E_n = \begin{pmatrix} 1 & 0 & 0 & \cdot & \cdot & 0 \\ 0 & 1 & 0 & \cdot & \cdot & 0 \\ 0 & 0 & 1 & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & 0 \\ 0 & \cdot & \cdot & \cdot & 0 & 1 \end{pmatrix},$$

die Einheitsmatrix vom Typ (n, n). Ist X eine Basis von V, so ist der Isomorphismus von K-Vektorräumen von Proposition 6.11(a)

$$\kappa : End_K(V) \to K^{n\times n},\ f \mapsto A_{f,X}$$

in Fakt ein Isomorphismus von K-Algebren (d.h. mit Produkten verträglich, d.h. $\kappa(gf) = \kappa(g)\kappa(f)$). Im folgenden verwenden wir diesen Isomorphismus um Aussagen über Endomorphismen in Aussagen über Matrizen zu übersetzen.

Nach Lemma 6.3 ist $f \in End_K(V)$ ein Automorphismus genau dann, wenn es ein $g \in End_K(V)$ mit $gf = \mathrm{id}_V$ und $fg = \mathrm{id}_V$ gibt. Ist X eine Basis von V, so folgt aus $gf = \mathrm{id}_V$ und $fg = \mathrm{id}_V$ durch Anwendung des Isomorphismus $\kappa : End_K(V) \to K^{n\times n}$ wegen $\kappa(\mathrm{id}_V) = E_n$ dann

$$A_{f,X}A_{g,X} = E_n = A_{g,X}A_{f,X}.$$

Dies motiviert folgende Definition für Matrizen:

Definition 6.14. Sei $A \in K^{n\times n}$. Gibt es ein $B \in K^{n\times n}$ mit $AB = E_n = BA$, so ist B eindeutig durch A bestimmt; B ist die zu A inverse Matrix, schreibe $B = A^{-1}$. Hat A eine inverse Matrix, so ist A invertierbar (oder regulär).

• Gibt es ein B mit $AB = E_n$ oder $BA = E_n$, so ist $B = A^{-1}$.

Beispiel 6.15. Sei K ein Körper und sei $A \in K^{2\times 2}$, genauer

$$A = \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix}.$$

Setze $d = \alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21} \in K$. Ist $d \neq 0$, so rechnet man nach

$$\frac{1}{d}\begin{pmatrix} \alpha_{22} & -\alpha_{12} \\ -\alpha_{21} & \alpha_{11} \end{pmatrix}\begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E_2$$

d.h. A ist invertierbar. Sei $d = 0$. Ist $\alpha_{12} \neq 0$ oder $\alpha_{22} \neq 0$, so ist

$$\begin{pmatrix} \alpha_{22} & -\alpha_{12} \\ 0 & 0 \end{pmatrix} A = 0.$$

Wäre A invertierbar, so liefert Rechtsmultiplikation mit A^{-1} dann

$$\begin{pmatrix} \alpha_{22} & -\alpha_{12} \\ 0 & 0 \end{pmatrix} = 0;$$

dies ist ein Widerspruch, also ist A nicht invertierbar. In Fall $\alpha_{12} = 0 = \alpha_{23}$ folgt wegen

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

ähnlich wie vorher, dass A nicht invertierbar ist. Wir haben gezeigt:

$$A \text{ ist invertierbar } \Leftrightarrow d \neq 0.$$

Die Determinantentheorie wird uns ein ähnliches Kriterium für Matrizen in $K^{n\times n}$ liefern.

Sei $f \in End_K(V)$ und sei $A_{f,X}$ die Matrix von f bezüglich einer Basis X von V. Dann ist f ein Automorphismus genau dann, wenn $A_{f,X}$ für jede Wahl einer solchen Basis X invertierbar ist:

Lemma 6.16. *Sei V ein K-Vektorraum der Dimension $n < \infty$ und sei $f \in End_K(V)$ ein Endomorphismus. Dann sind gleichwertig:*

(a) *f ist Automorphismus,*

(b) *Für jede Basis X von V ist $A_{f,X}$ invertierbar; weiter gilt*

$$A_{f^{-1},X} = A_{f,X}^{-1},$$

(c) *Für wenigstens eine Basis X von V ist $A_{f,X}$ invertierbar.*

NB. Das Lemma impliziert die folgenden Ausagen: Sei $X = \{v_1, \ldots, v_n\}$ eine Basis von V und seien $\alpha_{ij} \in K$ $(i, j = 1, \ldots, n)$ Skalare. Setze

$$w_j = \sum_{i=1}^{n} \alpha_{ij} v_i,\ j = 1, \ldots, n.$$

1) Dann ist $\{w_1, \ldots, w_n\}$ genau dann eine Basis von V, wenn die Matrix (α_{ij}) invertierbar ist: Die Abbildung $f(v_j) = w_j$ ist ein Endomorphismus mit Basis $A_{f,X} = (\alpha_{ij})$. Dabei ist f genau dann ein Automorphismus, wenn $\{w_1, \ldots, w_n\}$ eine Basis ist; nach (b) gilt dies genau dann, wenn (α_{ij}) invertierbar ist.

2) Ist (α_{ij}) invertierbar und $(\beta_{ij}) = (\alpha_{ij})^{-1}$, so ist

$$v_j = \sum_{k=1}^{n} \beta_{kj} w_k,\ j = 1, \ldots, n$$

Folgt wegen

$$\begin{array}{rcl} v_j & = & \sum_{i=1}^n \delta_{ij} v_i = \sum_{i=1}^n (\sum_{k=1}^n \alpha_{ik}\beta_{kj}) v_i = \\ & = & \sum_{k=1}^n \beta_{kj} \sum_{i=1}^n \alpha_{ik} v_i = \sum_{k=1}^n \beta_{kj} w_k. \end{array}$$

Beweis. (a)⇒(b): Sei $f^{-1} \in End_K(V)$ die zu f inverse Abbildung, sodass $f^{-1}f = ff^{-1} = \mathrm{id}_V$. Ist X eine Basis von V, so liefert der Isomorphismus $f \mapsto A_{f,X}$ die Identitäten $A_{f^{-1},X}A_{f,X} = A_{f,X}A_{f^{-1},X} = E_n$, also ist die Matrix $A_{f,X}$ invertierbar und es gilt $A_{f^{-1},X} = A_{f,X}^{-1}$.

(b)⇒(c): Trivial.

(c)⇒(a): Sei $A_{f,X}$ invertierbar bzgl. X. Setze $g = \kappa^{-1}((A_{f,X})^{-1}) \in End_K(V)$. Da κ (und so κ^{-1}) ein Isomorphismus von K-Algebren ist, erhält die Abbildung κ^{-1} Produkte und Einselemente. Also ist

$$gf = \kappa^{-1}(A_{f,X}^{-1})\kappa^{-1}(A_{f,X}) = \kappa^{-1}(A_{f,X}^{-1}A_{f,X}) = \kappa^{-1}(E_n) = \mathrm{id}_V\,.$$

Genauso folgt $fg = \mathrm{id}_V$, d.h. f ist ein Automorphismus. □

Proposition 6.17. *(Basiswechsel) (a) Seien V, W K-Vektorräume. Ferner seien $X = \{v_1, \ldots, v_n\}$, $X' = \{v'_1, \ldots, v'_n\}$ Basen von V und $Y = \{w_1, \ldots, w_m\}$, $Y' = \{w'_1, \ldots, w'_m\}$ Basen von W, sodass*

$$\begin{aligned} v'_j &= \textstyle\sum_{i=1}^n \beta_{ij} v_i, \quad j = 1, \ldots, n, \\ w'_l &= \textstyle\sum_{k=1}^m \gamma_{kl} w_k, \quad l = 1, \ldots m. \end{aligned}$$

Dann sind (β_{ij}) und (γ_{kl}) invertierbar und für $f \in Hom_K(V, W)$ gilt

$$A_{f,X',Y'} = (\gamma_{kl})^{-1} A_{f,X,Y}(\beta_{ij}).$$

(b) Ist $V = W$, $X = Y$ und $X' = Y'$ so liefert dies die Identität

$$A_{f,X'} = (\beta_{ij})^{-1} A_{f,X}(\beta_{ij}).$$

Beweis. (a): Seien id_V und id_W die Identitäten auf V und V. Wegen

$$\mathrm{id}_V(v'_j) = v'_j = \sum_{i=1}^n \beta_{ij} v_i \text{ und } \mathrm{id}_W(w'_l) = w'_l = \sum_{k=1}^m \gamma_{kl} w_k$$

ist $A_{\mathrm{id}_V,X',X} = (\beta_{ij})$ und $A_{\mathrm{id}_W,Y,Y'} = (\gamma_{kl})^{-1}$. Nach Proposition 6.11(b) ist die zu einem Kompositum assoziierte Matrix das Produkt der zu den einzelnen Abbildungen assoziierten Matrizen, also folgt

$$\begin{aligned} A_{f,X',Y'} &= A_{(\mathrm{id}_W f \mathrm{id}_V),X',Y'} = A_{\mathrm{id}_W,Y,Y'} A_{f,X,Y} A_{\mathrm{id}_V,X',X} = \\ &= (\gamma_{kl})^{-1} A_{f,X,Y}(\beta_{ij}). \end{aligned}$$

(b): Ist ein Spezialfall von (a). □

Beispiel 6.18. Für ein konkretes Beispiel eines Basiswechsels wie in Proposition 6.17(a) betrachte die lineare Abbildung

$$f : \mathbb{R}^3 \to \mathbb{R}^2, \quad \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

Seien zunächst $X = \{(1,0,0), (0,1,0), (0,0,1)\}$ und $Y = \{(1,0), (0,1)\}$ die Standardbasen. Die Koeffizienten der Darstellungen der Bilder der Basisvektoren sind die Spalten der Matrix $A_{f,X,Y}$. Wegen

$$\begin{aligned} f(1,0,0) = (1,0) &= 1 \cdot (1,0) + 0 \cdot (0,1) \\ f(0,1,0) = (0,1) &= 0 \cdot (1,0) + 1 \cdot (0,1) \\ f(0,0,1) = (0,0) &= 0 \cdot (1,0) + 0 \cdot (0,1) \end{aligned}$$

ist somit die Matrix von f Byzgl. der Basen X, Y gegeben durch

$$A_{f,X,Y} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Die Wahl von anderen Basen X' von $\mathbb{R}^3$ bzw. Y' von $\mathbb{R}^2$ ergibt eine andere Matrix. Zum Beispiel, sind $X' = \{(1,0,0),(1,1,0),(1,1,1)\}$ und $Y' = \{(1,1),(0,1)\}$ diese Basen, so liefert die analoge Rechnung

$$\begin{array}{rcl} f(1,0,0) = (1,0) & = & 1\cdot(1,1) - 1\cdot(0,1) \\ f(1,1,0) = (1,1) & = & 1\cdot(1,1) + 0\cdot(0,1) \\ f(1,1,1) = (1,1) & = & 1\cdot(1,1) + 0\cdot(0,1) \end{array}$$

die Matrix

$$A_{f,X',Y'} = \begin{pmatrix} 1 & 1 & 1 \\ -1 & 0 & 0 \end{pmatrix}$$

Nach Proposition 6.17(a) lässt sich der Übergang von $A_{f,X,Y}$ nach $A_{f,X',Y'}$ durch invertierbare Matrizen beschreiben, die einem Basiswechsel entsprechen. Betrachte zunächst die Identitätsabbildung $\mathrm{id}_{\mathbb{R}^3}$ auf $\mathbb{R}^3$ bezüglich der Basen X' und X. Wegen

$$\begin{array}{rcl} (1,0,0) & = & 1\cdot(1,0,0) + 0\cdot(0,1,0) + 0\cdot(0,0,1) \\ (1,1,0) & = & 1\cdot(1,0,0) + 1\cdot(0,1,0) + 0\cdot(0,0,1) \\ (1,1,1) & = & 1\cdot(1,0,0) + 1\cdot(0,1,0) + 1\cdot(0,0,1) \end{array}$$

ist dann

$$A_{\mathrm{id}_{\mathbb{R}^3},X',X} = (\beta_{ij}) = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$

wobei die Matrix (β_{ij}) invertierbar ist, da die Identität ein offensichtlicher Isomorphismus ist. Genauso hat die Identität auf $\mathbb{R}^2$ bzgl. der Basen Y' und Y aufgrund von den Identitäten

$$\begin{array}{rl} (1,1) & = 1\cdot(1,0) + 1\cdot(0,1) \\ (0,1) & = 0\cdot(1,0) + 1\cdot(0,1) \end{array}$$

die Matrix

$$A_{\mathrm{id}_{\mathbb{R}^2},Y',Y} = (\gamma_{kl}) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Auch (γ_{kl}) ist invertierbar, und nach Beispiel 6.15 gilt

$$A_{\mathrm{id}_{\mathbb{R}^2},Y,Y'} = (\gamma_{kl})^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}.$$

Gleichwertig lässt sich $(\gamma_{kl})^{-1}$ als die Matrix der Identitätsabbildung $\mathrm{id}_{\mathbb{R}^2}$ bezüglich der Basen Y und Y' direkt bestimmen: Aufgrund von

$$\begin{array}{rl} (1,0) & = 1\cdot(1,1) - 1\cdot(0,1) \\ (0,1) & = 0\cdot(1,1) + 1\cdot(0,1) \end{array}$$

ist

$$A_{\mathrm{id}_{\mathbb{R}^2},Y,Y'} = (\gamma_{kl})^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}.$$

Nach Proposition 6.17(a) gilt dabei die Beziehung

$$A_{f,X',Y'} = (\gamma_{kl})^{-1} A_{f,X,Y}(\beta_{ij}),$$

d.h. das folgende Diagramm kommutiert

$$\begin{array}{ccc} \mathbb{R}^3 \text{ mit Basis } X' & \xrightarrow{A_{f,X',Y'}} & \mathbb{R}^2 \text{ mit Basis } Y' \\ {\scriptstyle A_{\mathrm{id},X',X}=(\beta_{ij})}\big\downarrow \cong & & \cong \big\uparrow {\scriptstyle A_{\mathrm{id},Y,Y'}=(\gamma_{kl})^{-1}} \\ \mathbb{R}^3 \text{ mit Basis } X & \xrightarrow{A_{f,X,Y}} & \mathbb{R}^2 \text{ mit Basis } Y \end{array}$$

d.h. wir haben

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

wie man durch direktes Nachrechnen bestätigt.

Definition 6.19. Sei K ein Körper und sei $A = (\alpha_{ij}) \in K^{m\times n}$ eine Matrix. Betrachte die Zeilenvektoren $z_i = (\alpha_{i1}, \ldots, \alpha_{in}), i = 1, \ldots m$ (bzw. die Spaltenvektoren $s_j = (\alpha_{1j}, \ldots, \alpha_{mj}), j = 1, \ldots, n$) von A als Elemente von K^n (bzw. K^m). Dann ist der Zeilenrang $r_z(A)$ (bzw. Spaltenrang $r_s(A)$) die Anzahl der linear unabhängigen Zeilenvektoren (bzw. Spaltenvektoren), d.h.

$$r_z(A) = \dim_K \langle z_1, \ldots, z_m \rangle \text{ und } r_s(A) = \dim_K \langle s_1, \ldots, s_n \rangle.$$

• Offensichtlich ist $r_z(A) \leq min\{m, n\}$ und $r_s(A) \leq min\{m, n\}$.

Sei $f \in Hom_K(V, W)$ eine lineare Abbildung mit assoziierter Matrix $A_{f,X,Y} \in K^{m\times n}$. Dann entspricht der Rang der linearen Abbildung f dem Spaltenrang von $A_{f,X,Y}$:

Lemma 6.20. *(a) Seien V, W K-Vektorräume, $X = \{v_1, \ldots, v_n\}$ eine Basis von V und $Y = \{w_1, \ldots, w_m\}$ eine Basis von W. Sei $f \in Hom_K(V, W)$ mit Matrix $A_{f,X,Y} = (\alpha_{ij})$, d.h. es gilt*

$$f(v_j) = \sum_{i=1}^{m} \alpha_{ij} w_i, \ j = 1, \ldots, n.$$

Dann ist $r(f) = r_s(A_{f,X,Y})$.
(b) Sei $A \in K^{m\times n}$ und seien $B \in K^{n\times n}$ und $C \in K^{m\times m}$ invertierbar. Dann ist $r_s(A) = r_s(CAB)$.
(c) Sei $A \in K^{m\times n}$ und $B \in K^{n\times r}$. Dann ist $r_s(AB) \leq min\{r_s(A), r_s(B)\}$.

Beweis. (a): Die lineare Abbildung $g : W \to K^m$

$$g(\sum_{i=1}^{m} \beta_i w_i) = \begin{pmatrix} \beta_1 \\ \cdot \\ \cdot \\ \beta_m \end{pmatrix}$$

ist ein Isomorphismus. Nach Übungblatt 8, Aufgabe 1 gilt somit

$$r(f) = r(gf) = \dim \operatorname{im}(gf),$$

wobei $\operatorname{im}(gf)$ genau das Erzeugnis der Spaltenvektoren

$$(gf)(v_j) = g(\sum_{i=1}^{m} \alpha_{ij} w_i) = \begin{pmatrix} \alpha_{1j} \\ \cdot \\ \cdot \\ \alpha_{mj} \end{pmatrix} = s_j, \ j = 1, \dots n$$

ist. Also ist $r(f) = \dim_K \langle s_1, \dots s_n \rangle = r_s(A_{f,X,Y})$.
(b), (c): Siehe Übungsblatt 8, Aufgabe 1. □

Definition 6.21. Sei K ein Körper. Für eine Matrix $A \in K^{m \times n}$

$$A = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdot & \cdot & \cdot & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdot & \cdot & \cdot & \alpha_{2n} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \alpha_{m1} & \alpha_{m2} & \cdot & \cdot & \cdot & \alpha_{mn} \end{pmatrix}$$

definiere die zu A transponierte Matrix $A^t \in K^{n \times m}$ durch

$$A^t = \begin{pmatrix} \alpha_{11} & \alpha_{21} & \cdot & \cdot & \cdot & \alpha_{m1} \\ \alpha_{12} & \alpha_{22} & \cdot & \cdot & \cdot & \alpha_{m2} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \alpha_{1n} & \alpha_{2n} & \cdot & \cdot & \cdot & \alpha_{nm} \end{pmatrix},$$

d.h. A^t entsteht aus A durch Vertauschen der Zeilen und Spalten.

- Die Abbildung $K^{m \times n} \to K^{n \times m}, \ A \mapsto A^t$ ist ein Isomorhismus.
- Für $A \in K^{m \times n}$ und $B \in K^{n \times r}$ gilt: $(AB)^t = B^t A^t$.
- Wir zeigen später: Jede lineare Abbildung $f \in Hom_K(V, W)$ induziert ein lineare Abbildung (die duale Abbildung) $f^* \in Hom_K(W^*, V^*)$, wobei $W^* = Hom_K(W, K)$ und $V^* = Hom_K(V, K)$ die entsprechenden Dualräume sind. Ist $A = A_{f,X,Y}$ die Matrix von f bgzl. der Basen X, Y, so ist $A^t = A_{f^*,Y^*,X^*}$ die Matrix von f^* bzgl. der dualen Basen X^*, Y^*.

Theorem 6.22. *Für jede Matrix $A \in K^{m\times n}$ gilt*

$$r_z(A) = r_s(A) \leq min\{m, n\} \text{ (d.h. Zeilenrang=Spaltenrang).}$$

• Schreibe $r(A) = r_z(A) = r_s(A)$; $r(A)$ ist der Rang der Matrix A.

Beweis. Sei $r = r_s(A)$. Nach Übungsblatt 9, Aufgabe 1 gibt es invertierbare Matrizen $B \in K^{m\times m}$ und $C \in K^{n\times n}$, sodass gilt

$$BAC = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix},$$

wobei E_r die Einheitsmatrix vom Typ r ist. Transponieren liefert

$$C^t A^t B^t = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}.$$

Wegen $E_m = (BB^{-1})^t = (B^{-1})^t B^t$ ist B^t invertierbar; ebenso ist C^t invertierbar. Mit Lemma 6.20(b) folgt aus den obigen Identitäten

$$r_s(A) = r_S(BAC) = r_s(C^t A^t B^t) = r_s(A^t) = r_z(A).$$

□

Proposition 6.23. *Für $A \in K^{n\times n}$ sind gleichwertig:*

(a) $r(A) = n$

(b) *A ist invertierbar, d.h. A^{-1} existiert.*

• Dies ist das Analogon von Lemma 5.11 (mit $V = W$) für Matrizen, d.h. für eine lineare Abbildung $f \in End_K(V)$ sind gleichwertig:

f ist Isomorphismus $\Leftrightarrow$ f ist Monomorphimus $\Leftrightarrow$ f ist Epimorphismus.

Beweis. Sei $A = (\alpha_{ij}) \in K^{n\times n}$ mit Zeilenvektoren $z_j = (\alpha_{j1}, \ldots, \alpha_{jn})$. Ist $B = (\beta_{ij}) \in K^{n\times n}$, so hat die Produktmatrix BA die Form

$$BA = \begin{pmatrix} \beta_{11} \cdots \beta_{1n} \\ \cdot \\ \cdot \\ \beta_{n1} \cdots \beta_{nn} \end{pmatrix} \cdot \begin{pmatrix} z_1 \\ \cdot \\ \cdot \\ z_n \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^n \beta_{1j} z_j \\ \cdot \\ \cdot \\ \sum_{j=1}^n \beta_{nj} z_j \end{pmatrix}.$$

(a)⇒ (b): Ist $r(A) = r_z(A) = \langle z_1, \ldots, z_n\rangle = n$, so ist $K^n = \langle z_1, \ldots, z_n\rangle$ und $\{z_1, \ldots, z_n\}$ bilden eine Basis (da $\dim_K K^n = n$ kann K^n nur von mindestens n Vektoren erzeugt werden, d.h. $\{z_1, \ldots, z_n\}$ bilden ein minimales Erzeugendensystem und damit eine Basis). Sei $\{e_1, \ldots, e_n\}$ die Standardbasis von K^n. Dann gibt es eindeutige $\beta_{ij} \in K$ mit

$$e_i = \sum_{j=1}^n \beta_{ij} z_j, \ i = 1, \ldots n.$$

Für die entsprechende Matrix $B = (\beta_{ij})$ gilt $E_n = BA$, d.h. A ist invertierbar und $B = A^{-1}$.

(b)⇒(a): Sei $A^{-1}A = E_n$. Lemma 6.20(b) (angewandt auf die Matrizen $C = A^{-1}$, $A = A$ und $B = E_n$, sodass $CAB = A^{-1}AE_n = E_n$) liefert

$$r(A) = r_s(A) = r_s(A^{-1}AE_n) = r_s(E_n) = n.$$

□

7. Elementare Umformungen und Lineare Gleichungssysteme

Für jede Matrix $A \in K^{m\times n}$ ist nach Theorem 6.22 der Zeilenrang gleich dem Spaltenrang, d.h. $r_z(A) = r_s(A)$. In einfachen Beispielen lässt sich der Rang einer Matrix sofort ablesen. Zum Beispiel ist

$$r\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix} = 2 \text{ und } r\begin{pmatrix}1 & 1\\ 2 & 2\end{pmatrix} = 1$$

Eine allgemeine Matrix lässt sich durch 'elementare Umformungen' wie Addition und Subtraktion von Vielfachen von Zeilen auf eine solche einfachere Form bringen. Zum Beispiel,

$$A = \begin{pmatrix}2 & 0 & 1\\ 1 & 2 & 0\\ 1 & 1 & 1\end{pmatrix} \overset{z_3-z_2}{\to} \begin{pmatrix}2 & 0 & 1\\ 1 & 2 & 0\\ 0 & -1 & 1\end{pmatrix} \overset{z_2-1/2z_1}{\to} \begin{pmatrix}2 & 0 & 1\\ 0 & 2 & -1/2\\ 0 & -1 & 1\end{pmatrix}$$
$$\overset{z_3+1/2z_2}{\to} \begin{pmatrix}2 & 0 & 1\\ 0 & 2 & -1/2\\ 0 & 0 & -3/4\end{pmatrix} = A'$$

Diese Umformungen lassen sich als Linksmultiplikation mit Matrizen beschreiben:

$$z_3-z_2 \leftrightarrow T_1 = \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & -1 & 1\end{pmatrix} : \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & -1 & 1\end{pmatrix}\begin{pmatrix}2 & 0 & 1\\ 1 & 2 & 0\\ 1 & 1 & 1\end{pmatrix} = \begin{pmatrix}2 & 0 & 1\\ 1 & 2 & 0\\ 0 & -1 & 1\end{pmatrix}$$

und genauso

$$z_2-1/2z_1 \leftrightarrow T_2 = \begin{pmatrix}1 & 0 & 0\\ -1/2 & 1 & 0\\ 0 & 0 & 1\end{pmatrix} \text{ und } z_3+1/2z_1 \leftrightarrow T_3 = \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 1/2 & 0 & 1\end{pmatrix}$$

Also führt Linksmultiplikation mit diesen 'Transformationsmatrizen' T_1, T_2, T_3 die gegebene Matrix A in die einfachere Form A' über, d.h.

$$T_3T_2T_1A = A',$$

wobei die T_i invertierbar sind (sie haben offensichtlich Rang 3). Nach Lemma 6.20(b) verändert die Multiplikation mit einer invertierbaren Matrix den Rang nicht, somit haben A und A' den gleichen Rang

$$r(A) = r(T_3T_2T_1A) = r(A') = 3.$$

Wir bestimmen allgemein 'Elementarmatrizen' mit der Eigenschaft, dass Multiplikation mit diesen Matrizen den Rang einer Matrix erhält und verallgemeinern das obige Beispiel zu einen Algorithmus, der es uns erlaubt den Rang einer Matrix zu berechnen.

Definition 7.1. Sei K ein Körper und $i \neq j$. Eine Elementarmatrix $T_{ij}(\alpha) = (\alpha_{ij}) \in K^{n\times n}$ hat die Form:

(a) $\alpha \in K$ an der Stelle (i, j) (wobei $i \neq j$ ist),
b) 1 auf der Diagonalen (d.h. $\alpha_{ii} = 1$ für alle i),
(c) 0 an allen anderen Stellen.

Für $\alpha = 1$ setze $T_{ij} = T_{ij}(1)$. Sei $\mathbb{E}_n \subseteq K^{n\times n}$ die Menge der Elementarmatrizen vom Typ (n, n).

• Offenbar gelten für Elementarmatrizen die Beziehungen

$$\begin{aligned} T_{ij}(\alpha) \cdot T_{ij}(\beta) &= T_{ij}(\alpha + \beta), \\ T_{ij}(\alpha)T_{ij}(-\alpha) &= E_n, \end{aligned}$$

insbesondere ist jede Elementarmatrix invertierbar, d.h. regulär.

Lemma 7.2. *Sei $A \in K^{m\times n}$ mit Zeilen $z_1, .., z_m$ und Spalten $s_1, .., s_n$.*

(a) *Ist $T_{ij}(\alpha) \in K^{m\times m}$ (d.h. das Produkt $T_{ij}(\alpha)A$ existiert), so ist*

$$T_{ij}(\alpha)A = \begin{pmatrix} z_1 \\ \cdot \\ \cdot \\ z_i + \alpha z_j \\ \cdot \\ \cdot \\ z_m \end{pmatrix}.$$

(b) *Ist $T_{ij}(\beta) \in K^{n\times n}$ (d.h. das Produkt $AT_{ij}(\beta)$ existiert), so gilt*

$$AT_{ij}(\beta) = (s_1, \cdots, s_j + \beta s_i, \ldots, s_n).$$

Beweis. Nachrechnen. □

Definition 7.3. Sei $A \in K^{m\times n}$. Eine elementare Umformung von A ist eine Operation, die durch Multiplikation von A durch eine Elementarmatrix von links oder von rechts ensteht. Explizit: Jede elementare Umformung ist von der Form:

(a) Ersetzen der Zeile z_i von A durch $z_i + \alpha z_j$, wobei $\alpha \in K$ und $i \neq j$; die Zeilen z_k für $k \neq i$ bleiben unverändert. Gleichwertig: Multiplikation mit $T_{ij}(\alpha) \in \mathbb{E}_m$ von links.

(b) Ersetzen der Spalte s_j von A durch $s_j + \beta s_i$, wobei $\beta \in K$ und $i \neq j$; die Spalten s_k für $k \neq i$ bleiben unverändert. Gleichwertig: Multiplikation mit $T_{ij}(\beta) \in \mathbb{E}_n$ von rechts.

NB. Ist $A \in K^{m\times n}$, so entspricht die Anwendung endlich vieler elementarer Umformungen $T_i \in \mathbb{E}_m$ und $S_j \in \mathbb{E}_n$ auf A einer Abbildung

$$A \quad \mapsto \quad T_k \cdots T_1 A S_1 \cdot S_l = A'.$$

Setze $C = T_k \cdots T_1$ und $B = S_1 \cdots S_l$. Dann sind C und B als Produkt von invertierbaren Matrizen invertierbar und nach Lemma 6.20(b) gilt

$$r(A) = r(CAB) = r(A').$$

Also verändert die Anwendung von (endlich viele) beliebigen elementare Umformungen auf A nicht den Rang von A; man kann somit eine gegebene Matrix A durch Links- bzw. Rechtsmutiplikation mit Elementarmatrizen in eine Matrix überführen, deren Rang leicht zu bestimmen ist. Dabei kann man entweder diese Operationen ad hoc auf eine gegebene Matrix anwenden, oder einen von diversen Algorithmen verwenden, die die gegebene Matrix in eine einfachere Form bringen.

Wir geben ein Beispiel eines solchen Algorithmus:

Theorem 7.4. *Sei $A = (\alpha_{ij}) \in K^{m\times n}$. Ist $A \neq 0$, so gibt es Elementarmatrizen $T_i \in \mathbb{E}_m$ $(i = 1, \ldots, k)$ und $S_j \in \mathbb{E}_n$ $(j = 1, \ldots, n)$, sodass die resultierende Matrix $A' = T_k \cdots T_1 A S_1 \cdots S_l$ die folgende Form hat*

$$A' = \begin{pmatrix} \alpha'_{11} & * & * & & & & \cdot & \cdot & * \\ 0 & \alpha'_{22} & * & & & & \cdot & \cdot & * \\ 0 & 0 & \alpha'_{33} & * & & & \cdot & \cdot & * \\ \cdot & & \cdot & & & & \cdot & \cdot & \cdot \\ \cdot & & & \cdot & & & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & \alpha'_{rr} & * & \cdot & \cdot & * \\ 0 & 0 & \cdot & 0 & 0 & 0 & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & & & & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & & & & \cdot & \cdot & \cdot \\ 0 & 0 & \cdot & & & & \cdot & \cdot & 0 \end{pmatrix},$$

wobei $\alpha'_{11} \cdots \alpha'_{rr} \neq 0$ ist. Offensichtlich ist $r(A) = r(A') = r$.

Beweis. Schritt 1: Ist $\alpha_{11} \neq 0$, so gehe zu Schritt 4.

Schritt 2: Sei $\alpha_{11} = 0$, aber sei z_1 nicht die Nullzeile. Dann gibt es in z_1 einen nicht-trivialen Eintrag α_{1j} mit $j > 1$. Rechtsmultipikation mit

der Elementarmatrix $T_{1j} \in \mathbb{E}_n$ ersetzt die erste Spalte s_1 durch $s_1 + s_j$, d.h. die Matrix AT_{1j} hat an der Stelle $(1,1)$ den Eintrag $\alpha_{j1} \neq 0$. Gehe jetzt zu Schritt 4.

Schritt 3: Sei $\alpha_{11} = 0$ und sei z_1 eine Nullzeile. Da $A \neq 0$ ist, gibt es eine Zeile $z_i,\ i > 1$ mit einem nicht-trivalen Eintrag. Linksmultiplikation mit der Elementarmatrix $T_{1i} \in \mathbb{E}_m$ ersetzt z_1 durch $z_1 + z_i$; also hat die erste Zeile von $T_{1i}A$ die Form $(\beta_{i1}, \ldots, \beta_{in})$ mit $\beta_{ij} \neq 0$ für ein j. Ist $\beta_{i1} \neq 0$, so gehe zu Schritt 4, ist $\beta_{i1} = 0$, so gehe zu Schritt 2.

Schritt 4: Wir haben eine Matrix A mit $\alpha_{11} \neq 0$. Also sind die Quotienten $\frac{\alpha_{i1}}{\alpha_{11}} \in K$ und damit die Matrizen $T_{i1}(\frac{\alpha_{i1}}{\alpha_{11}}) \in \mathbb{E}_m$ für $i = 2, \ldots, m$ definiert. Die Matrix $T_{m1}(-\frac{\alpha_{m1}}{\alpha_{11}}) \cdots T_{21}(-\frac{\alpha_{21}}{\alpha_{11}})A$ hat die Form

$$\begin{pmatrix} z_1 \\ z_1 - \frac{\alpha_{21}}{\alpha_{11}} z_1 \\ \cdot \\ \cdot \\ \cdot \\ z_m - \frac{\alpha_{m1}}{\alpha_{11}} z_1 \end{pmatrix} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdot & \cdot & \alpha_{1n} \\ 0 & & & & \\ \cdot & & & & \\ \cdot & & A_1 & & \\ \cdot & & & & \\ 0 & & & & \end{pmatrix}$$

Schritt 5: Ist die verbleibende $(m-1) \times (n-1)$-Matrix A_1 die Nullmatrix, so sind wir fertig. Falls $A_1 \neq 0$ ist, wende die Schritte 1-4 auf A' an (jede elementare Umformung von A_1 lässt sich als elementare Umformung von A interpretieren). Nach endlich vielen Schritten liefert dies eine Matrix der gewünschten Form. □

Beispiele 7.5. (a) Sei $A \in \mathbb{R}^{3\times 3}$ die Matrix

$$A = \begin{pmatrix} 1 & -1 & 2 \\ 4 & 4 & -2 \\ 2 & 0 & 2 \end{pmatrix}$$

Dem Algorithmus folgend beginnen wir mit Schritt 4. Dies liefert

$$\begin{pmatrix} 1 & -1 & 2 \\ 4 & 4 & -2 \\ 2 & 0 & 2 \end{pmatrix} \overset{T_{21}(-4)}{\to} \begin{pmatrix} 1 & -1 & 2 \\ 0 & 8 & -10 \\ 2 & 0 & 2 \end{pmatrix} \overset{T_{31}(-2)}{\to} \begin{pmatrix} 1 & -1 & 2 \\ 0 & 8 & -10 \\ 0 & 2 & -2 \end{pmatrix}$$

Iteration dieses Verfahrens auf die verbleibende Matrix $A_1 \in \mathbb{R}^{2\times 2}$ zeigt

$$\begin{pmatrix} 1 & -1 & 2 \\ 0 & 8 & 10 \\ 0 & 2 & -2 \end{pmatrix} \overset{T_{32}(-1/4)}{\to} \begin{pmatrix} 1 & -1 & 2 \\ 0 & 8 & 10 \\ 0 & 0 & 1/2 \end{pmatrix}$$

Also ist $r = 3$ und $r(A) = 3$.
(b) Betrachte die Matrix (mit reellen Koeffizienten)

$$A = \begin{pmatrix} 3 & 6 & 2 & 10 \\ 10 & 16 & 6 & 30 \\ 5 & 14 & 4 & 14 \end{pmatrix}$$

Elementare Umformungen (ohne Verwendung des Algorithmus) zeigen

$$\begin{pmatrix} 3 & 6 & 2 & 10 \\ 10 & 16 & 6 & 30 \\ 5 & 14 & 4 & 14 \end{pmatrix} \overset{z_2-3z_1}{\to} \begin{pmatrix} 3 & 6 & 2 & 10 \\ 1 & -2 & 0 & 0 \\ 5 & 14 & 4 & 14 \end{pmatrix}$$

$$\overset{z_3-2z_1}{\to} \begin{pmatrix} 3 & 6 & 2 & 10 \\ 1 & -2 & 0 & 0 \\ -1 & 2 & 0 & -6 \end{pmatrix}$$

$$\overset{z_3+z_2}{\to} \begin{pmatrix} 3 & 6 & 2 & 10 \\ 1 & -2 & 0 & 0 \\ 0 & 0 & 0 & -6 \end{pmatrix}$$

Die Zeilen z_1, z_2, z_3 in der letzten Matrix sind offensichtlich linear unabhängig, also ist $r(A) = 3$.

Wir wollen invertierbare Marizen mittels einfacher Matrizen beschreiben. Nicht jede invertierbare Matrix ist ein (endliches) Produkt von Elementarmatrizen. Eine einfache Rechnung zeigt, dass zum Beispiel

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \in \mathbb{R}^{2\times 2}$$

invertierbar, aber nicht Produkt von Elementarmatrizen ist: Da $d = d(A) = 2 \neq 0$ ist A invertierbar, siehe Beispiel 6.15. Jede Elementarmatrix vom Typ $(2, 2)$ ist eine Matrix der folgenden Form

$$T = \begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix} \text{ oder } S = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}$$

Es ist $d(T) = 1 = d(S)$. Wegen $T_{ij}(\alpha) \cdot T_{ij}(\beta) = T_{ij}(\alpha + \beta)$ gilt für eine endliches Produkt T' vn Matrizen vom Typ T (bzw. ein endliches Produkt S' von Matrizen vom Typ S) ebenfalls $d(T') = 1$ (bzw. $d(S') = 1$). Eine einfache direkte Rechnung zeigt, dass $d(ST) = 1 = d(TS)$. Also gilt für jedes endliche Produkt von Elementarmatrizen $d = 1$, und A kann keine Darstellung als ein solches Produkt haben.

Wir werden sehen: Invertierbare Diagonalmatrizen $D = (d_{ij})$ mit $d_{11} \cdots d_{nn} \neq 1$ sind nicht als Produkt von Elementarmatrizen darstellbar.

Definition 7.6. Eine elementare Diagonalmatrix $D_i(\alpha) \in K^{n\times n}$ ist eine Matrix $D_i(\alpha) = (\alpha_{ij})$ mit den Einträgen

(a) $\alpha_{ii} = \alpha$ für ein $\alpha \in K \setminus \{0\}$,
(b) $\alpha_{jj} = 1$ für $j \neq i$,
(c) $\alpha_{ij} = 0$ für $i \neq j$.

Sei $\mathbb{D}_n \subseteq K^{n\times n}$ die Menge der Matrizen von diesem Typ.

• $D_i(\alpha) \cdot D_i(\alpha^{-1}) = E_n$, d.h. $D_i(\alpha)$ ist invertierbar.

Lemma 7.7. *Jede invertierbare Matrix $A \in K^{n\times n}$ hat eine Darstellung als ein endliches Produkt von Elementen aus der Menge $\mathbb{E}_n^\times = \mathbb{E}_n \cup \mathbb{D}_n$.*

• Sei $GL_n(K)$ die Gruppe der invertierbaren Matrizen in $K^{n\times n}$ (bzgl. der Multiplikation von Matrizen). Das obige Lemma besagt, dass sich jedes Element von $GL_n(K)$ als ein endliches Produkt von Elementen von $\mathbb{E}_n^\times$ schreiben lässt; man sagt $GL_n(K)$ wird von $\mathbb{E}_n^\times$ erzeugt.
• Die Darstellung eines Elements von $GL_n(K)$ als ein endliches Produkt von Elementen aus $\mathbb{E}_n^\times$ ist nicht eindeutig. Zum Beispiel gilt in $GL_2(\mathbb{R})$:

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \text{ und } \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \cdot \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}.$$

Beweis. (Skizze) Sei $A \in K^{n\times n}$ invertierbar. Nach Lemma 6.23 ist $r(A) = n$, insbesondere hat A keine triviale Spalte. Ist $\alpha_{11} = 0$, so gibt es ein $i > 1$ mit $\alpha_{i1} \neq 0$ und $T_{1i}A$ hat α_{i1} an der Stelle $(1,1)$; wir können also annehmen, dass $\alpha_{11} \neq 0$ ist. Wie im Schritt 4 im Beweis von Theorem 7.4 lässt sich A durch Zeilenumformungen und Iteration (d.h. Anwendung auf A_1) in eine Matrix $B = T_k \cdots T_1 A$ der Form

$$B = \begin{pmatrix}\beta_{11} & * & * & * & *\\ 0 & \beta_{22} & * & * & *\\ 0 & 0 & \beta_{33} & * & *\\ \cdot & & \cdot & & \\ \cdot & & \cdot & \cdot & *\\ 0 & 0 & 0 & 0 & \beta_{nn}\end{pmatrix}$$

mit $\beta_{11} \cdots \beta_{nn} \neq 0$ überführen. Diese Matrix B lässt sich durch Linksmultiplikation mit Elementarmatrizen und Matrizen der Form $D_{ii}(\alpha)$ zu einer Einheitsmatrix machen: Man beseitigt die Einträge in der letzten Spalte $\beta_{1,n}, \beta_{2,n}, \cdots, \beta_{n-1,n}$ mit Hilfe der letzten Zeile, dann die Einträge in der vorletzten Spalte $\beta_{1,n-1}, \cdots, \beta_{n-2,n-1}$ mit Hilfe der vorletzten Zeile, etc. um so eine Diagonalmatrix mit nicht-trivalen Diagonaleinträgen zu erhalten. Multiplikation mit geeigneten Matrizen der Form $D_{ii}(\alpha)$ macht dann diese Diagonalmatrix zur Einheitsmatrix.

Also gibt es Elementarmatrizen $T_i \in \mathbb{E}_n$ $(i = 1, \ldots, k)$ sowie elementare Diagonalmatrizen $D_j \in \mathbb{D}_n$ $(j = 1, \ldots, l)$ mit $D_l \cdots D_1 T_k \cdots T_1 A = E_n$. Da A^{-1} eindeutig ist, folgt $A^{-1} = D_l \cdots D_1 T_k \cdots T_1$. □

Beispiele 7.8. Der Beweis von Lemma 7.7 ist konstruktiv und liefert ein Verfahren die inverse Matrix A^{-1} zu berechnen: Ist $A \in K^{n\times n}$ invertierbar und sind $D_i \in \mathbb{D}_n$ bzw. $T_j \in \mathbb{E}_n$ mit $D_l \cdots D_1 T_k \dots T_1 A = E_n$, so ist $A^{-1} = D_l \cdots D_1 T_k \cdots T_1 = D_l \cdots D_1 T_k \cdots T_1 E_n$. Um A^{-1} konkret zu berechnen schreibt man A und E_n nebeneinander, und formt A durch Linksmultiplikation mit Elementen aus $\mathbb{E}_n$ bzw. $\mathbb{D}_n$ zur Einheitsmatrix E_n um. Die analogen Umformungen angewandt auf E_n liefern die inverse Matrix A^{-1}.

(a) Wir betrachten $A \in \mathbb{R}^{3\times 3}$ und wenden das obige Verfahren zur Berechnung von A^{-1} an *ohne* vorher bestimmt zu haben, ob A^{-1} existiert.

$$
\begin{array}{rcc}
A & = & \begin{pmatrix} 1 & 1 & 2 \\ 1 & 2 & -1 \\ 0 & 1 & -4 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad = \quad E_3 \\
\overset{z_2-z_1}{\to} & \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & -3 \\ 0 & 1 & -4 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
\overset{z_3-z_2}{\to} & \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & -3 \\ 0 & 0 & -1 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 1 & -1 & 1 \end{pmatrix} \\
\overset{z_1-z_2}{\to} & \begin{pmatrix} 1 & 0 & 5 \\ 0 & -1 & -3 \\ 0 & 0 & -1 \end{pmatrix} & \begin{pmatrix} 2 & -1 & 0 \\ -1 & 1 & 0 \\ 1 & -1 & 1 \end{pmatrix} \\
\overset{z_2-3z_3}{\to} & \begin{pmatrix} 1 & 0 & 5 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} & \begin{pmatrix} 2 & -1 & 0 \\ -4 & 4 & -3 \\ 1 & -1 & 1 \end{pmatrix} \\
\overset{z_1+5z_3}{\to} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} & \begin{pmatrix} 7 & -6 & 5 \\ -4 & 4 & -3 \\ 1 & -1 & 1 \end{pmatrix} \\
\overset{D_3(-1)}{\to} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 7 & -6 & 5 \\ -4 & 4 & -3 \\ -1 & 1 & -1 \end{pmatrix} \quad = \quad A^{-1}
\end{array}
$$

Zur Kontrolle rechnet man nach:

$$
A^{-1} \cdot A = \begin{pmatrix} 7 & -6 & 5 \\ -4 & 4 & -3 \\ -1 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 2 \\ 1 & 2 & -1 \\ 0 & 1 & -4 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} = E_3
$$

(b) Wendet man dieses Verfahren auf eine Matrix A an, die nicht invertierbar ist, so zeigt sich das unterwegs:

$$\begin{array}{rcccc} A & = & \begin{pmatrix} 1 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 1 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} & = E_3 \\ & \overset{z_3-z_1}{\rightarrow} & \begin{pmatrix} 1 & 0 & 1 \\ 0 & -1 & 0 \\ 0 & 1 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix} & \end{array}$$

Der Rang der letzten Matrix auf der A-Seite ist 2 und gleich dem Rang von A, d.h. $r(A) = 2 < 3$ und die Matrix A ist nicht invertierbar.

Sei $A \in K^{m\times n}$ mit $r(A) = r$. Nach Übungszettel 9, Aufgabe 1 gibt es invertierbare Matrizen $C \in K^{m\times m}$ und $B \in K^{n\times n}$, sodass gilt

$$CAB = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} \in K^{m\times n}$$

Wir zeigen, wie sich mit Hilfe von Elementarmatrizen diese Matrizen C und B explizit berechnen lassen.

Wir benötigen dazu die folgende Definition.

Definition 7.9. Eine Matrix $A = (\alpha_{ij}) \in K^{m\times n}$ hat Zeilenstufenform, falls gilt:

(a) Es gibt ein r mit $0 \leq r \leq m$, sodass in den Zeilen mit Index 1 bis r jeweils nicht nur Nullen stehen, und in den Zeilen mit Index $r+1$ bis m nur Nullen stehen,

(b) Für jedes i mit $1 \leq i \leq r$ sei j_i der kleinste Index der Spalte, in der ein Eintrag ungleich Null steht, d.h. $j_i = \min\{j \mid \alpha_{ij} \neq 0\}$; hier ist $j_1 < j_2 < \cdots < j_r$.

Dabei ist $r = 0$ zulässig, in diesem Fall sind alle Einträge von A Null. Die ersten nichttrivialen Einträge in den nichttrivialen Zeilen $\alpha_{1j_1}, \ldots, \alpha_{rj_r}$ sind die Pivots (oder auch Angelpunkte) von A.

Beispiele 7.10. (a) Die Matrix

$$A = \begin{pmatrix} 0 & 2 & 0 & 4 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 2 \end{pmatrix}$$

ist in Zeilenstufenform. Hier $m = 3, n = 4, r = 3$; weiter ist $j_1 = 2, j_2 = 3, j_3 = 4$, die Pivots sind die Einträge $\alpha_{12} = 2, \alpha_{23} = 1$ und $\alpha_{34} = 2$.

(b) Die folgende Matrix ist in Zeilenstufenform

$$A = \begin{pmatrix} 1 & 3 & 0 & 5 & 6 & 0 & 5 \\ 0 & 0 & 1 & 3 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Das Rechenverfahren zur Bestimmung von C und B basiert auf folgende Beobachtung: Jede Matrix $A \in K^{m\times n}$ lässt sich durch geeigenete Zeilenumformungen (d.h. Linksmultiplikation mit Elementarmatrizen) in Zeilenstufenform überführen. Also gibt es $T_1, \dots T_k \in \mathbb{E}_m$, sodass

$$T_k \cdots T_1 A$$

in Zeilenstufenform ist. Weiter lässt sich jede Matrix in Zeilenstufenform (mit entsprechendem r) durch Spaltenumformungen (d.h. Rechtsmultiplikation mit Elementarmatrizen) in eine Matrix der Form

$$\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$$

überführen. Für geeigente Elementarmatrizen $S_1, \dots, S_l \in \mathbb{E}_n$ ist also

$$T_k \cdots T_1 A S_1 \dots S_l = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}.$$

Damit ist $C = T_k \cdots T_1$ und $B = S_1 \cdots S_l$.

Beispiel 7.11. Betrachte die folgende Matrix mit reellen Einträgen

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

Offensichtlich hat A den Rang 2, d.h. es gibt invertierbare Matrizen C und B mit

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

Umd B und C zu bestimmen, schreiben wir im ersten Schritt E_2 und A nebeneinander und formen diese Matrizen durch Zeilenumformungen parallel so um, dass A in Zeilenstufenform übergeführt wird:

$$\begin{array}{rcll} E_2 & = & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 0 \\ 2 & 2 & 1 \end{pmatrix} = A \\ & \overset{z_2-2z_1}{\to} & \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 2 & 0 \\ 0 & -2 & 1 \end{pmatrix} = T_1 A \end{array}$$

Im zweiten Schritt schreiben wir T_1A und E_3 nebeneinander und bringen T_1A durch Spaltenumformungen auf die gewünschte Form:

$$\begin{array}{rcll} T_1A & = & \begin{pmatrix}1&2&0\\0&-2&1\end{pmatrix} & \begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix} = E_3 \\ & \overset{s_2-2s_1}{\to} & \begin{pmatrix}1&0&0\\0&-2&1\end{pmatrix} & \begin{pmatrix}1&-2&0\\0&1&0\\0&0&1\end{pmatrix} = E_3S_1 \\ & \overset{s_2+3s_3}{\to} & \begin{pmatrix}1&0&0\\0&1&1\end{pmatrix} & \begin{pmatrix}1&-2&0\\0&1&0\\0&3&1\end{pmatrix} = E_3S_1S_2 \\ & \overset{s_3-s_2}{\to} & \begin{pmatrix}1&0&0\\0&1&0\end{pmatrix} & \begin{pmatrix}1&-2&2\\0&1&-1\\0&3&-2\end{pmatrix} = E_3S_1S_2S_3 \end{array}$$

Also ist $C = T_1 = \begin{pmatrix}1&0\\-2&1\end{pmatrix}$ und $B = S_1S_2S_3 = \begin{pmatrix}1&-2&2\\0&1&-1\\0&3&-2\end{pmatrix}$.

8. Lineare Gleichungssysteme

Wir betrachten Systeme von m linearen Gleichungen in n Variablen mit Koeffizienten in einem Körper K, d.h. ein System von Gleichungen

$$\begin{array}{ccccccccc} \alpha_{11}x_1 & + & \alpha_{12}x_2 & \cdot & \cdot & \alpha_{1n}x_n & = & \beta_1 \\ \alpha_{21}x_1 & + & \alpha_{22}x_2 & \cdot & \cdot & \alpha_{2n}x_n & = & \beta_2 \\ \cdot & & \cdot & & & & & \cdot \\ \cdot & & \cdot & & & & & \cdot \\ \alpha_{m1}x_1 & + & \alpha_{m2}x_2 & \cdot & \cdot & \alpha_{mn}x_n & = & \beta_m, \end{array}$$

mit Variablen x_j und Skalaren $\alpha_{ij}, \beta_i \in K$; dafür schreiben wir auch

$$\text{(L)} \quad \sum_{j=1}^{n} \alpha_{ij}x_j = \beta_i, \ i = 1, \ldots, m.$$

Eine Lösung von (L) ist eine gemeinsame Lösung der m Gleichungen.

Das System (L) lässt sich als ein Matrizenprodukt auffassen

$$Ax = \begin{pmatrix}\alpha_{11} & \cdot & \cdot & \cdot & \alpha_{1n}\\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \alpha_{m1} & \cdot & \cdot & \cdot & \alpha_{mn}\end{pmatrix} \cdot \begin{pmatrix}x_1\\x_2\\\cdot\\\cdot\\x_n\end{pmatrix} = \begin{pmatrix}\beta_1\\\beta_2\\\cdot\\\cdot\\\beta_m\end{pmatrix} = b$$

Der Matrix $A = (\alpha_{ij})$ definiert eine lineare Abbildung $A : K^n \to K^m$ durch $x \mapsto Ax$. Damit lässt sich das System (L) wie folgt interpretieren: Ist $b \in K^m$ fest gewählt, so gilt $A^{-1}(b) = \{x \in K^n \mid Ax = b\}$, d.h. die Elemente von $A^{-1}(b)$ sind genau die Lösungen von (L).

Die wesentlichen Fragestellungen nach der Existenz und Eindeutigkeit von Lösungen von (L) lassen sich somit wie folgt formulieren:

(1) Ist $A^{-1}(b) \neq \emptyset$, d.h. gibt es eine Lösung?

(2) Ist $|A^{-1}(b)| = 1$, d.h. gibt es eine eindeutige Lösung?

Das System (L) lässt sich wie folgt umschreiben

$$\begin{pmatrix} \alpha_{11} \\ \alpha_{21} \\ \cdot \\ \cdot \\ \alpha_{m1} \end{pmatrix} \cdot x_1 + \begin{pmatrix} \alpha_{12} \\ \alpha_{22} \\ \cdot \\ \cdot \\ \alpha_{m2} \end{pmatrix} \cdot x_2 + \cdots + \begin{pmatrix} \alpha_{1n} \\ \alpha_{2n} \\ \cdot \\ \cdot \\ \alpha_{mn} \end{pmatrix} \cdot x_n = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \cdot \\ \cdot \\ \beta_m \end{pmatrix}$$

Dabei sind die auf der linken Seite auftretenden Vektoren genau die Spalten $s_1, \ldots, s_n$ der Matrix A, und falls eine Lösung x exisitiert, dann muss b eine Linearkombination der s_i sein und es gilt

$$x_1 s_1 + \cdots x_n s_n = b.$$

Die Fragen nach Existenz und Eindeutgkeit von Lösungen lassen sich somit auch wie folgt ausdrücken:

(1') Ist $b \in \langle s_1, \ldots, s_n \rangle$?

(2') Falls $b \in \langle s_1, \ldots, s_n \rangle$, sind $s_1, \ldots, s_n$ linear unabhängig?

Wir formalisieren diese Überlegungen und geben zunächst einfach zu berechnende Existenz- und Eindeutigkeitskriterien für die Lösbarkeit eines solchen Systems von linearen Gleichungen.

Definition 8.1. Sei $A = (\alpha_{ij}) \in K^{m \times n}$ eine Matrix und $b = (\beta_i) \in K^m$ ein Spaltenvektor. Ein lineares Gleichungssystem (L) ist ein System von Gleichungen der Form $Ax = b,\ x = (x_j) \in K^n$, d.h. die m Gleichungen

$$(\mathrm{L}): \quad \sum_{j=1}^{n} \alpha_{ij} x_j = \beta_i,\ i = 1, \ldots, m.$$

Ist $b = 0$, so ist (L) homogen; ist $b \neq 0$, so ist (L) inhomogen. Die erweiterte Koeffizientenmatrix des linearen Gleichungssystems (L) ist

$$B = [A, b] = \begin{pmatrix} \alpha_{11} & \cdot & \cdot & \cdot & \alpha_{1n} & \beta_1 \\ \cdot & \cdot & & & & \cdot \\ \cdot & \cdot & & & & \cdot \\ \cdot & \cdot & & & & \cdot \\ \alpha_{m1} & \cdot & & & \alpha_{mn} & \beta_n \end{pmatrix}$$

Lemma 8.2. *Sei $A \in K^{m\times n}$ eine Matrix.*

(a) *Die Lösungen des homogenen Systems $Ax = 0$ ist genau* $\ker(A)$*; insbesondere bilden die Lösungen von $Ax = 0$ einen linearen Unterraum von K^n der Dimension $n - r(A)$.*

(b) *Ist x_0 eine Lösung von $Ax = b$, so ist $x_0 + \ker(A)$ die Menge aller Lösungen von $Ax = b$.*

• Nach (b) bilden die Lösungen von $Ax = b$ einen affinen Unterraum von K^n; nach (a) hat dieser affine Unterraum Dimension $n - r(A)$.

• Aus (a) folgt: Ist $n > m$, so hat $Ax = 0$ nicht-triviale Lösungen $x \neq 0$.

Beweis. (a): Sei $A : K^n \to K^m, x \mapsto Ax$ die durch die Matrix A definierte lineare Abbildung. Die Menge der Lösungen von $Ax = 0$ ist $A^{-1}(0) = \ker(A) \subseteq K^n$ und damit ein linearer Unterraum. Da $\dim \operatorname{im}(A) = r(A)$ ergibt sich mit dem Homomorphiesatzes 5.10(b) $\dim \ker(A) = \dim K^n - \dim \operatorname{im}(A) = n - r(A)$.

(b): Sei x_0 eine Lösung von $Ax = b$. Ist $y \in K^n$ mit $Ay = 0$, so folgt $A(x_0 + y) = b$, sodass $x_0 + \ker(A) \subseteq A^{-1}(b)$. Ist umgekehrt $x \in A^{-1}(b)$ eine Lösung von $Ax = b$, so setze $y = x - x_0$. Dann ist $Ay = 0$ und $x = x_0 + y \in x_0 + \ker(A)$; dies zeigt $A^{-1}(b) \subseteq x_0 + \ker(A)$. □

Proposition 8.3. *(Existenz) Sei $A \in K^{m\times n}$ und sei $b \in K^m$. Betrachte das System (L): $Ax = b$ mit erweiterter Koeffizientenmatrix $B = [A, b]$. Dann gilt: (L) ist lösbar genau dann, wenn $r(A) = r(B)$ ist.*

Beweis. Sei $b = (\beta_i)$ und seien $s_1, \dots s_n$ die Spalten von A. Dann ist (L) genau dann lösbar, wenn $b \in \langle s_1, \dots, s_n\rangle$ ist. Dies gilt wegen

$$r(A) = \dim\langle s_1, \dots, s_n\rangle \leq \dim\langle s_1, \dots, s_k, b\rangle = r(B)$$

genau dann, wenn $r(A) = r(B)$ ist. □

Proposition 8.4. *(Eindeutigkeit) Sei $A \in K^{m\times n}$ und $b \in K^m$ mit $A^{-1}(b) \neq \emptyset$ (d.h. (L): $Ax = b$ hat eine Lösung). Dann hat (L) genau dann eine eindeutige Lösung, wenn $Ax = 0$ nur die triviale Lösung $x = 0$ hat; dies gilt genau dann, wenn $r(A) = n$ ist.*

• Sei $A \in K^{m\times n}$, sodass $Ax = b$ für alle $b \in K^m$ lösbar ist. Nach Proposition 8.3 ist dann $r(A) = m$. Sind diese Lösungen eindeutig, so folgt mit Proposition 8.4 $r(A) = n$. Also ist in diesem Fall A vom Typ (n, n) und wegen $r(A) = n$ invertierbar. Ist A^{-1} die inverse Matrix, so sind die eindeutigen Lösungen von $Ax = b$ genau die $x = A^{-1}b$.

Beweis. Ist $x_0 \in A^{-1}(b)$, so sind nach Lemma 8.2(b) die Lösungen von $Ax = b$ genau die Elemente von $x_0 + \ker(A)$ und x_0 ist die einzige

Lösung genau dann, wenn $\ker(A) = \{0\}$ ist. Da $\dim \ker(A) = n - r(A)$ gilt $\ker(A) = \{0\}$ genau dann, wenn $r(A) = n$ ist. □

Beispiel 8.5. Betrachte das lineare Gleichungssystem mit reellen Koeffizienten

$$\begin{array}{rcrcrcl} x_1 & + & x_2 & + & 2x_3 & = & 0 \\ 2x_1 & + & 3x_2 & & & = & 9 \\ & & 2x_2 & + & x_3 & = & -1 \end{array}$$

Wir haben die Matrizen

$$A = \begin{pmatrix} 1 & 1 & 2 \\ 2 & 3 & 0 \\ 0 & 2 & 1 \end{pmatrix} \text{ und } B = [A, b] = \begin{pmatrix} 1 & 1 & 2 & 0 \\ 2 & 3 & 0 & 9 \\ 0 & 2 & 1 & -1 \end{pmatrix}$$

Für A berechnet man $r(A)$ mittels der elementaren Zeilenumformungen

$$\begin{pmatrix} 1 & 1 & 2 \\ 2 & 3 & 0 \\ 0 & 2 & 1 \end{pmatrix} \overset{z_2-2z_1}{\to} \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & -4 \\ 0 & 2 & 1 \end{pmatrix} \overset{z_3-2z_1}{\to} \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & -4 \\ 0 & 0 & 9 \end{pmatrix}$$

Es ist $r(A) = 3$. Aus $3 = r(A) \leq r(B) \leq 3$ folgt $r(A) = r(B) = 3$ und nach Proposition 8.3 hat $Ax = b$ eine Lösung. Da $r(A) = 3$ ist nach Proposition 8.4 diese Lösung eindeutig; es ist $x = A^{-1}b$.

Die Bestimmung von $r(A)$ und $r(B)$ kann durch elementare Umformungen durchgeführt werden und liefert nach den obigen Kriterien Existenz- und Eindeutigkeitsaussagen. Eine Variante solcher Umformungen liefert einen Lösungsalgorithmus für ein Gleichungssystem (L): $Ax = b$ mit $B = [A, b]$. Die zulässige Umformungen von (L) sind:

(a) Vertauschen der Zeilen von B (Permutation der Gleichungen),

(b) Vertauschen der Spalten von A (Permutation der $x_1, \ldots x_n$),

(c) Zeilenübergänge in B der Form $z_i \to z_i + \alpha z_j, i \neq j, \alpha \in K$.

Diese Operationen ändern die Lösungsmenge von (L) nicht (abgesehen von einer eventuellen Umnumerierung der x_i).

Gauss-Algorithmus. Wir können annehmen, dass A keine Nullspalte hat (d.h. jede Variable x_j kommt in dem System (L) nicht-trivial vor).

1. Nach Anwendung von (a) und (b) ist $A = (\alpha_{ij})$ mit $\alpha_{11} \neq 0$.

2. Mittels $z_i \to z_i - \alpha_{i1}/\alpha_{11} z_1$ für $i \geq 2$ ergibt sich ein System der Form

$$\begin{array}{rcl} \alpha_{11}x_1 + \sum_{k=2}^n \alpha_{1k}x_k & = & \beta_1 \\ \sum_{k=2}^n \alpha'_{jk}x_k & = & \beta'_j, j = 2, \ldots n. \end{array}$$

3. Betrachte das reduzierte System von $m-1$ Gleichungen

$$\sum_{k=2}^{n} \alpha'_{jk} x_k = \beta'_j,\ j = 2, \dots n.$$

Ist $(\alpha'_{ij}) = 0$ ist, so sind wir fertig. Ist $(\alpha'_{ij}) \neq 0$, so liefert Anwendung von **1.** und **2.** auf dieses System und dann weitere Iteration ein Gleichungsssystem von m Gleichungen in n Variablen y_i der Form

$$\begin{array}{rrcl} & \beta_{11}y_1 + \beta_{12}y_2 + \cdots + \beta_{1k}y_k + \cdots + \beta_{1n}y_n &=& \beta'_1 \\ & \beta_{22}y_2 + \cdots + \beta_{2k}y_k + \cdots + \beta_{2n}y_n &=& \beta'_2 \\ & & \cdot & \cdot \\ & & \cdot & \cdot \\ \text{(L')}: & \beta_{kk}y_k + \cdots + \beta_{kn}y_n &=& \beta'_k \\ & 0 &=& \beta'_{k+1} \\ & & \cdot & \\ & & \cdot & \\ & 0 &=& \beta'_m \end{array}$$

mit $\beta_{rr} \neq 0$ für $r = 1, \dots k$ (d.h. die Matrix (β_{ij}) ist in Zeilenstufenform mit Pivots $\beta_{11}, \dots \beta_{kk}$). Für das System (L') gilt:

- Ist $\beta'_r \neq 0$ für ein $r = k+1, \dots m$, so ist (L) nicht lösbar.
- Ist $\beta'_{k+1} = \cdots = \beta'_m = 0$ so ist (L') lösbar (und die $y_{k+1}, \dots, y_n$ können beliebig gewählt werden). Wegen $\beta'_{jj} \neq 0$ für $j = 1, \dots k$ lässt sich (L') sukzessive nach $y_k, y_{k-1}, \dots, y_1$ auslösen; eine eindeutige Lösung von (L') liegt dabei nur dann vor, wenn $k = n$ ist.

Beispiele 8.6. (a) Betrachte das System (mit reellen Koeffizenten)

$$\text{(L)}:\ B = [A, b] = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 2 & 0 & 2 & 2 \end{pmatrix}$$

Es ist $\alpha_{11} \neq 0$. Die Operation $z_3 - 2z_1$ liefert ein neues System

$$\text{(L')}:\ B' = [A', b'] = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & -2 & 0 & 0 \end{pmatrix}$$

Das reduzierte System hat $\alpha'_{22} = 0$. Vertauschen der 2. und 3. Spalte von A' ergibt eine Matrix A'' mit $\alpha''_{22} \neq 0$ und demselben b, d.h.

$$\text{(L")}:\ B'' = [A'', b'] = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & -2 & 0 \end{pmatrix}$$

Aus dieser Darstellung lässt sich durch sukzessive Auflösung die eindeutige Lösung $y = (0, 1, 0)$ bestimmen. Da wir die 2. und 3. Spalte vertauscht haben, ist die eindeutige Lösung von $B = [A, b]$ dann $x = (0, 0, 1)$.

(b) Die erweitere Koeffizientenmatrix

$$B = [A, b] = \begin{pmatrix} 4 & 0 & 0 & 0 & 4 \\ 0 & 2 & 2 & 4 & 2 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

ist bereits in Zeilenstufenform. Für die Lösungen ergibt sich

$$x_4 = 1,\ 2x_2 + 2x_3 + 4 = 2,\ x_1 = 1.$$

Auflösen der 2. Gleichung nach x_2 liefert $x_2 = -x_3 - 1$. Also lässt sich jede Lösung x von $Ax = b$ in folgender Form schreiben

$$x = \begin{pmatrix} 1 \\ -x_3 - 1 \\ x_3 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \\ 0 \\ 1 \end{pmatrix} + x_3 \begin{pmatrix} 0 \\ -1 \\ 1 \\ 0 \end{pmatrix}.$$

Dabei ist $x_0 = (1, -1, 0, 1)^t$ eine spezielle Lösung von $Ax = b$. Weiter liegt $(0, -1, 1, 0)^t \in \ker(A)$; wegen $r(A) = 3$ folgt $\dim \ker(A) = 4 - 3 = 1$, d.h. $(0, -1, -1, 0)$ ist eine Basis von $\ker(A)$. Die obige Beschreibung der Lösungsmenge von $Ax = b$ entspricht damit genau der Darstellung $x_0 + \ker(A)$ von Lemma 8.2(b).

(c) Hat die erweiterte Koeffizientenmatrix die Form

$$B = [A, b] = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

so folgt aus der letzten Gleichung $0x_3 = 1$; das diese Gleichung keine Lösung hat ist das System $Ax = b$ nicht lösbar.

(d) Betrachte die folgende Matrix mit reellen Koeffizienten

$$A = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 7 \\ 0 & 2 & 5 \end{pmatrix}$$

Es ist $r(A) = 3$: Dies folgt, zum Beispiel, da allgemein gilt

$$\begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix} \begin{pmatrix} B_1 & 0 \\ 0 & B_2 \end{pmatrix} = \begin{pmatrix} A_1 B_1 & 0 \\ 0 & A_2 B_2 \end{pmatrix}$$

und in diesem Beispiel für die entsprechende 2×2-Matrix A_2

$$d(A_2) = 3 \cdot 5 - 2 \cdot 7 = 1 \neq 0$$

ist, d.h. $r(A_2) = 2$ und damit $r(A) = 3$. Damit hat $Ax = b$ für *jedes* $b \in \mathbb{R}^3$ die eindeutige Lösung $x = A^{-1}b$. Wegen $d = 1$ folgt weiter

$$A_2^{-1} = \begin{pmatrix} 5 & -7 \\ -2 & 3 \end{pmatrix} \text{ und } A^{-1} = \begin{pmatrix} 1/2 & 0 & 0 \\ 0 & 5 & -7 \\ 0 & -2 & 3 \end{pmatrix}$$

Konkret ist zum Beispiel für $b = (1, 1, 1)^t$ die Lösung von $Ax = b$ somit

$$x = \begin{pmatrix} 1/2 & 0 & 0 \\ 0 & 5 & -7 \\ 0 & -2 & 3 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1/2 \\ -2 \\ 1 \end{pmatrix}$$

wie man durch direktes Nachrechnen leicht bestätigt.

9. Gruppen II

Um Determinanten von Matrizen definieren zu können benötigen wir einige elementare Aussagen der Gruppentheorie:

Definition 9.1. Seien G und H (multiplikativ geschriebene) Gruppen.

(1) Ein Homomorphismus (oder Gruppenhomomorphismus) ist eine Abbildung $f : G \to H$, die mit den Gruppenstrukturen verträglich ist, d.h. für $g_1, g_2 \in G$ gilt

$$f(g_1 g_2) = f(g_1) f(g_2).$$

(2) Ist $f : G \to H$ ein Gruppenhomomorphismus, so der Kern von f (bzw. das Bild von f) $\ker(f) = \{g \in G \mid f(g) = 1\}$ (bzw. $\mathrm{im}(f) = \{f(g) \mid g \in G\}$).

(3) Ein Homomorphismus $f : G \to H$ heisst Epimorphismus (bzw. Monomorphismus, Isomorphismus) falls f surjektiv (bzw. injektiv, bijektiv) ist. Gibt es einen Isomorphismus $f : G \to H$, so sind G und H isomorph, $G \cong H$. Die Isomorphismen $G \to G$ sind die Automorphismen von G.

• Für einen Gruppenhomomorphismus f gilt stets: $f(1) = 1$ und $f(g^{-1}) = f(g)^{-1}$.

• Ein Homomorphismus $f : G \to H$ ist genau dann ein Monomorphismus, wenn $\ker(f) = \{1\}$ ist.

• Ein Homomorphismus $f : G \to H$ ist genau dann ein Isomorphismus, wenn es einen Homomorphismus $g : H \to G$ mit $g \circ f = \mathrm{id}_G$ und $f \circ g = \mathrm{id}_H$ gibt. In diesem Fall ist $g = f^{-1}$.

Beispiele 9.2. (a) Sei G eine Gruppen und $a \in G$. Dann ist die Abbildung 'Konjugation mit a', d.h. $f_a : G \to G,\ g \mapsto a^{-1}ga$ ein Automorphismus: f_a ist Homomorphismus, da für $g_1, g_2 \in G$ gilt

$$f_a(g_1)f_a(g_2) = a^{-1}g_1aa^{-1}g_2a = a^{-1}g_1g_2a = f_a(g_1g_2).$$

Ist $f_a(g) = a^{-1}ga = 1$, so folgt $ga = a$ und $g = 1$, also ist $\ker(f_a) = \{1\}$ und f_a ist ein Monomorphismus. Für $g \in G$ ist $f_a(aga^{-1}) = g$, somit ist f_a auch surjektiv.

(b) Seien V, W K-Vektorräume und sei $f \in Hom_K(V, W)$. Dann besagt

$$f(v + v') = f(v) + f(v') \text{ für alle } v, v' \in V,$$

dass f ein Homomorphismus zwischen den V und W zugrundeliegenden additiven Gruppen $(V, +)$ und $(W, +)$ ist. In diesem Fall sind die abelschen Gruppen $\ker(f) \subseteq V$ und $\mathrm{im}(f) \subseteq W$ die den entsprechenden linearen Unterräumen zugrundeliegenden abelschen Gruppen.

(c) Sei K ein Körper und $A = (\alpha_{ij}) \in K^{2\times 2}$. Setze

$$\det(A) = \alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21} \in K.$$

Nach Beispiel 6.15 ist A invertierbar genau dann, wenn $\det(A) \neq 0$ ist. Sind $A, B \in K^{2\times 2}$, so zeigt eine einfache direkte Rechnung $\det(AB) = \det(A)\det(B)$. Also definiert det einen Homomorphismus

$$\det : GL_2(K) \to K^\times.$$

Ist $\alpha \in K^\times$, so ist

$$\det \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} = \alpha \in K^\times,$$

d.h. der Homomorphismus det ist ein Epimorphismus.

Definition 9.3. Sei G eine Gruppe. Eine Untergruppe $U \leq G$ ist ein Normalteiler (oder eine normale Untergruppe), $U \trianglelefteq G$, falls gilt

$$u \in U,\ g \in G \Rightarrow g^{-1}ug \in U.$$

Ist $U < G$ (d.h. $U \neq G$), so schreibe $U \lhd G$.

Beispiele 9.4. (a) Die trivialen Untergruppen $\{1\} < G$ und $G \leq G$ einer jeden Gruppe G sind Normalteiler, die trivialen Normalteiler.

(b) Ist G abelsch, so folgt aus $g^{-1}ug = g^{-1}gu = 1u = u \in U$, dass jede Untergruppe ein Normalteiler ist.

(c) Sei $G = S_3$ die Gruppe der bijektiven Abbildungen von $\{1, 2, 3\}$. Für verschiedene Ziffern $i, j, k \in \{1, 2, 3\}$ sei (i, j) die bijektive Abbildung $i \mapsto j, j \mapsto i, k \mapsto k$. Wegen $(i, j)(i, j) = \mathrm{id}$ definiert jede solche

Transposition (i,j) eine Untergruppe $\{\mathrm{id},(i,j)\} < G$ der Ordnung 2. Sei nun $U = \{\mathrm{id},(1,2)\} < G$, $u = (1,2)$ und $g = (1,3) \in G$. Dann ist

$$g^{-1}ug = (13)(12)(13) = (23) \notin U,$$

d.h. die Untergruppe $U = \{\mathrm{id},(1,2)\} < S_3$ ist kein Normalteiler.

Lemma 9.5. *Sei $f : G \to H$ ein Gruppenhomomorphismus. Dann gilt:*

(a) $\mathrm{im}(f) \subseteq H$ *ist eine Untergruppe,*

(b) $\ker(f) \subseteq G$ *ist ein Normalteiler.*

Beweis. (a): Einfaches Nachrechnen.

(b): Wegen $f(1) = 1$ ist $1 \in \ker(f)$. Für $g, g' \in \ker(f)$ folgt $f(gg') = f(g)f(g') = 1$, also ist $gg' \in \ker(f)$. Ist $g \in \ker(f)$, so ist $f(g^{-1}) = f(g)^{-1} = 1^{-1} = 1$ und $g^{-1} \in \ker(f)$, d.h. $\ker(f) \subseteq G$ ist eine Untergruppe. Sei $g \in G$ und $u \in \ker(f)$. Dann ist

$$f(g^{-1}ug) = f(g)^{-1}f(u)f(g) = f(g)^{-1} \cdot 1 \cdot f(g) = f(g)^{-1}f(g) = 1,$$

also ist $g^{-1}ug \in \ker(f)$ und $\ker(f) \trianglelefteq G$. □

Ist V ein K-Vektorraum und $W \subseteq V$ ein linearer Unterraum, so ist auf dem Faktorraum $V/W = \{a + W \mid a \in V\}$ die Verküpfung $(a_1 + W) + (a_2 + W) = a_1 + a_2 + W$ wohldefiniert. Der naive Versuch analog für eine Gruppe G und eine Untergruppe $U \leq G$ eine Faktorgruppe zu definieren scheitert: In multiplikativer Notation ist die entsprechende Menge $G/U = \{gU \mid g \in G\}$ und die 'evidente' Mutiplikation

$$g_1U \cdot g_2U = g_1g_2U$$

ist im allgemeinen *nicht* wohl-definiert. Ist $g_1U = g_1'U$ und $g_2U = g_2'U$, so ist $g_1' = g_1u_1$ und $g_2' = g_2u_2$ für geeignete $u_1, u_2 \in U$. Es folgt

$$g_1'g_2' = g_1u_1g_2u_2 = g_1(g_2g_2^{-1})u_1g_2u_2 = g_1g_2(g_2^{-1}u_1g_2)u_2,$$

d.h. $g_1g_2U = g_1'g_2'U$ gilt nur dann, wenn $g_2^{-1}u_1g_2 \in U$ ist; dies ist gerade die Normalteilerbedingung an U. Insbesondere induziert die Multiplikation auf G nur dann eine wohl-definierte Multiplikation auf G/U, wenn $U \subseteq G$ nicht nur eine Untergruppe, sondern ein Normalteiler ist.

Lemma 9.6. *Sei $N \trianglelefteq G$ ein Normalteiler und $G/N = \{gN \mid g \in G\}$.*

(a) *Die Menge G/N ist mittels der Verknüpfung*

$$g_1N \cdot g_2N = g_1g_2N, \quad g_1, g_2 \in G$$

eine Gruppe mit neutralem Element N

(b) *Die Abbildung $\pi : G \to G/N$, $g \mapsto gN$ ist ein Epimorphismus mit* $\ker(\pi) = N$.

Beweis. (a): Da $N \trianglelefteq G$ ist, ist die Gruppenoperation auf G/N wohldefiniert, siehe oben; wegen $N = 1N$ und $1N \cdot gN = 1gN = gN$ ist N das neutrale Element.
(b): Die Abbildung π ist offensichtlich surjektiv und nach Definition der Gruppenoperation auf G/N ein Homomorphismus. Die letzte Aussage $N = \ker(\pi)$ gilt da $g \in \ker(\pi) \Leftrightarrow gN = N \Leftrightarrow g \in N$. □

Theorem 9.7. *(Homomorphiesatz) Sei $f : G \to H$ ein Gruppenhomomorphismus. Dann gibt es einen Epimorphismus $\pi : G \to G/\ker(f)$ und einen Monomorphismus $h : G/\ker(f) \to H$ mit $f = h \circ \pi$ und* $\mathrm{im}(f) = \mathrm{im}(h)$.

• Der Monomorphismus $h : G/\ker(f) \to H$ induziert einen Isomorphismus $h : G/\ker(f) \xrightarrow{\cong} \mathrm{im}(f)$.

Beweis. Da $\ker(f) \trianglelefteq G$ ein Normalteiler ist hat $G/\ker(f)$ eine Gruppenstruktur. Die Abbildungen π und h sind die evidenten Abbildungen

$$\begin{aligned} \pi: &\quad G \to G/\ker(f), \quad g \mapsto g\ker(f), \\ h: &\quad G/\ker(f) \to H, \quad g\ker(f) \mapsto f(g) \end{aligned}$$

Dabei ist π nach Konstruktion ein Epimorphismus. Man rechnet nach, dass h wohl-definiert ist; die restlichen Eigenschaften sind dann klar. □

Wir betrachten nun die symmetrische Gruppe S_n der bijektiven Abbildungen der Menge $\{1, \ldots, n\}$ aus Beipiel 2.2(d). Die Gruppenoperation auf S_n ist die Verknüpfung von Abildungen, S_n ist eine endliche Gruppe mit $|S_n| = n!$. Für $n \geq 3$ ist die Gruppe S_n *nicht* abelsch.

Die Elemente von S_n heissen Permutationen und wir bezeichnen diese mit kleinen griechischen Buchstaben; dabei sei ι das neutrale Element von S_n, d.h. die Identitätsabbildung. Für $\tau \in S_n$ schreibe

$$\tau = \begin{pmatrix} 1 & 2 & \cdot & \cdot & \cdot & n \\ \tau(1) & \tau(2) & \cdot & \cdot & \cdot & \tau(n) \end{pmatrix}$$

Bei feststehendem n lassen wir zur Vereinfachung der Notation oft die Ziffern mit $\tau(j) = j$ weg, zum Beispiel schreiben wir für $n = 6$ so

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

Definition 9.8. Seien $a_1, \cdots, a_k$ paarweise verschiedene Ziffern aus der Menge $\{1, .., n\}$. Ein k-Zykel in S_n ist eine Permutation der Form

$$\psi = \begin{pmatrix} a_1 & a_2 & \cdot & \cdot & a_{k-1} & a_k \\ a_2 & a_3 & \cdot & \cdot & a_k & a_1 \end{pmatrix};$$

wir verwenden für einen solchen k-Zykel auch die Notation

$$\psi = (a_1, a_2, \cdots, a_{k-1}, a_k) = (a_2, a_3, \cdots, a_k, a_1).$$

Zwei Zyklen $(a_1, a_2, \cdots, a_k)$ und $(b_1, b_2, \cdots, b_l)$ heissen disjunkt, falls $\{a_1, \ldots a_k\} \cap \{b_1, \ldots b_l\} = \emptyset$ ist. Eine Transposition ist ein 2-Zykel (i, j) (nach Definition ist dabei $i \neq j$).

Lemma 9.9. *Sei S_n die symmetrische Gruppe mit $n > 1$.*

(a) *Jede Permutation $\tau \in S_n$ hat eine Darstellung als ein Produkt von disjunkten Zyklen.*

(b) *Es gilt $(a_1, a_2, \cdots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \cdots (a_1, a_2)$, d.h. jede Permutation lässt sich als ein Produkt von Transpositionen schreiben.*

• Ist $n = 5$, so gilt nach (b) $(1, 2, 3) = (1, 3)(1, 2)$. Wegen $(1, 2, 3) = (1, 3)(1, 2) = (1, 3)(1, 2)(4, 5)(4, 5)$ ist die Darstellung einer Permutation als ein Produkt von Transpositionen *nicht* eindeutig.

Beweis. (a): Jede Permutation lässt sich sukzessive in disjunkte Zyklen aufteilen, zum Beispiel ist

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix} = (1, 2)(4, 5, 6)$$

Der Beweis von (a) ist eine Formalisierung dieses Prozesses und eine einfache Übung.

(b): Die erste Aussage folgt durch Nachrechnen (Permutationen sind von rechts zu lesen), die zweite aus (a). □

Theorem 9.10. *Sei $n > 1$ und sei $\{-1, 1\}$ die multiplikative Gruppe.*

(a) *Es gibt einen Epimorphismus*

$$\operatorname{sgn} : S_n \to \{-1, +1\}$$

mit $\operatorname{sgn}(\tau) = -1$ für alle Transpositonen $\tau \in S_n$.

(b) *Sei K ein Körper und $f : S_n \to K^\times$ ein Homomorphismus. Dann ist entweder $f(\rho) = 1$ für alle $\rho \in S_n$, oder es ist $char(K) \neq 2$ und $f = \operatorname{sgn}$.*

• Ist $\pi \in S_n$ und $\pi = \tau_1 \cdots \tau_k$ eine Zerlegung in Transpositionen, so gilt nach (a) sgn ein Homomorphismus mit $\operatorname{sgn}(\tau_i) = -1$ für alle i, also ist $\operatorname{sgn}(\pi) = (-1)^k$. Die Zerlegung von π in ein Produkt vonTranspositionen ist nicht eindeutig, aber für jede solche Zerlegung gilt, dass die Parität (gerade oder ungerade) der Anzahl der Faktoren eindeutig ist.

Beweis. (a): Sei $T = \{i, j\} \subseteq \{1, \ldots, n\}$ mit $i \neq j$. Für $\tau \in S_n$ setze

$$Z_\tau(T) = \begin{cases} 1 & \text{falls } \tau(i) \leq \tau(j), \\ -1 & \text{falls } \tau(i) > \tau(j) \end{cases}$$

und definiere

$$\operatorname{sgn}(\tau) = \prod_T Z_\tau(T) \in \{-1, 1\},$$

wobei das Produkt über alle $T = \{i, j\} \subseteq \{1, \ldots n\}$ mit $i \neq j$ läuft. Für $\rho \in S_n$ und $T = \{i, j\}$ setze $\rho T = \{\rho(i), \rho(j)\}$. Wir zeigen

$$(\#) \qquad Z_{\tau\rho}(T) = Z_\tau(\rho T) Z_\rho(T).$$

Gilt dies, so folgt

$$\operatorname{sgn}(\tau\rho) = \prod_T Z_{\tau\rho}(T) = \prod_T Z_\tau(\rho T) \prod_T Z_\rho(T) = \operatorname{sgn}(\tau) \operatorname{sgn}(\rho),$$

da mit T auch ρT alle 2-elementigen Teilmengen von $\{1, \ldots n\}$ durchläuft; insbesondere definiert sgn einen Homomorphismus. Die Behauptung (#) ergibt sich aus der folgenden Tabelle, die die $Z_*(T)$ bzgl. der relative Lage von $\{\rho(i), \rho(j)\}$ und $\{\tau(\rho(i)), \tau(\rho(j))\}$ beschreibt. Für $T = \{i, j\}$ ist

	$Z_\rho(T)$	$Z_\tau(\rho T)$	$Z_{\tau\rho}(T)$
$\rho(i) \leq \rho(j)$ und $\tau(\rho(i)) \leq \tau(\rho(j))$	1	1	1
$\rho(i) \leq \rho(j)$ und $\tau(\rho(i)) > \tau(\rho(j))$	1	-1	-1
$\rho(i) > \rho(j)$ und $\tau(\rho(i)) \leq \tau(\rho(j))$	-1	-1	1
$\rho(i) > \rho(j)$ und $\tau(\rho(i)) > \tau(\rho(j))$	-1	1	-1

Es bleibt zu zeigen: $\operatorname{sgn}(\tau) = -1$ für jede Transposition $\tau \in S_n$. Ist $\tau = (1, 2)$, so ist $Z_\tau(T) = -1$ für $T = \{1, 2\}$ und $Z_\tau(T) = 1$ sonst, d.h. $\operatorname{sgn}(\tau) = -1$. Ist $\tau' = (i, j)$ beliebig, so gibt es ein

$$\rho = \begin{pmatrix} 1 & 2 & \cdots \\ i & j & \cdots \end{pmatrix} \in S_n$$

mit $\rho(1) = i$ und $\rho(2) = j$. Dann ist $\tau' = \rho\tau\rho^{-1}$, und es folgt

$$\operatorname{sgn}(\tau') = \operatorname{sgn}(\rho\tau\rho^{-1}) = \operatorname{sgn}(\rho) \operatorname{sgn}(\tau) \operatorname{sgn}(\rho)^{-1} = -1,$$

da $\operatorname{sgn}(\rho)^{-1} = -1$ falls $\operatorname{sgn}(\rho) = -1$ und $\operatorname{sgn}(\rho)^{-1} = 1$ sonst.

(b): Sei $f : S_n \to K^\times$ ein Homomorphismus. Ist τ eine Transposition, so ist $\tau^2 = \iota$ und $1 = f(\tau^2) = f(\tau)^2$, also $f(\tau) \in \{-1, 1\}$. Da sich jede Permutation nach Lemma 9.9(b) als Produkt von Transpositonen schreiben lässt, folgt $f(\tau) \in \{-1, 1\}$ für jedes $\tau \in S_n$. Ist $\tau = (1, 2)$ und

ist $\tau' = (i, j)$ eine beliebige Transposition, so liefert der Beweis von (a) ein $\rho \in S_n$ mit $\tau' = \rho\tau\rho^{-1}$. Also ist (die Gruppe $\{-1, 1\}$ ist abelsch)

$$f(\tau') = f(\rho\tau\rho^{-1}) = f(\rho)f(\tau)f(\rho)^{-1} = f(\tau)$$

d.h. für jede Transposition τ' gilt $f(\tau') = 1$ falls $f(\tau) = 1$ und $f(\tau') = -1$ falls $f(\tau) = -1$ ist. Ist $\rho \in S_n$ und ist $\rho = \tau_1 \cdots \tau_k$ eine Darstellung als ein Produkt von Transpositionen, so gilt nach Teil (a)

$$\operatorname{sgn}(\rho) = \prod_{j=1}^{k} \operatorname{sgn}(\tau_j) = (-1)^k.$$

Andererseits ist

$$f(\rho) = \prod_{j=1}^{k} f(\tau_j) = \begin{cases} (-1)^k & \text{falls } f(\tau) = -1 \\ 1 & \text{falls } f(\tau) = 1 \end{cases}$$

Dies zeigt die Behauptung: Ist $f(\rho) \neq 1$ für ein $\rho \in S_n$, so ist $char(K) \neq 2$ (sonst ist $-1 = 1$). Weiter gibt es eine Transposition τ_j mit $f(\tau_j) = -1$ und damit gilt auch $f(\tau) = -1$, sodass $f = \operatorname{sgn}$. □

Definition 9.11. Für $n \geq 2$ ist $A_n = \ker\{\operatorname{sgn} : S_n \to \{-1, 1\}\}$ die alternierende Gruppe auf n Ziffern.

- Es ist $A_n \trianglelefteq S_n$ und $|S_n : A_n| = 2$.
- Für jedes $\tau \in S_n$ mit $\tau(\pi) = -1$ ist $S_n = A_n \cup \tau A_n = \tau A_n \cup A_n$, wobei die Vereinigung jeweils disjunkt ist.

Beispiel 9.12. Sei $U < S_n$ eine Untergruppe mit $|S_n : U| = 2$. Dann ist $U = A_n$: Betrachte die Abbildung

$$f : S_n \to \{-1, 1\},\ f(\tau) = \begin{cases} 1 & \text{falls } \tau \in U, \\ -1 & \text{falls } \tau \notin U. \end{cases}$$

Man rechnet nach, dass f ein Homormorphismus ist; die Behauptung folgt dann mit Theorem 9.10(b).

Bemerkung 9.13. Für $n = 3$ und $n \geq 5$ sind $\{1\}, A_n$ und S_n die einzigen Normalteiler von S_n, und A_n besitzt nur die trivialen Normalteiler $\{1\}$ und A_n (man sagt A_n ist eine *einfache* Gruppe). Für $n = 4$ ist A_4 nicht-einfach, da $V = \{\iota, (12)(34), (13)(24), (14)(23)\}$ einen Normalteiler mit $|V| = 4$ definiert. Die Existenz dieser Untergruppe ist der Grund dafür, dass Lösungen von Polynomgleichungen der Form

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0,\ a_i \in \mathbb{C},$$

für $n \leq 4$ stets durch Wurzeln ausgedrückt werden können (der Fall $n = 2$ ist die 'Mitternachtsformel'), dies für $n \geq 5$ aber nicht gilt.

Die systematische Analyse der Lösungen solcher Polynomgleichungen erfolgt im Rahmen der Galoistheorie und ist ein Thema der Vorlesung 'Algebra'.

10. Determinanten

Nach Beispiel 6.15 gilt lässt sich für eine Matrix $A = (\alpha_{ij}) \in K^{2\times 2}$ aus den Koeffizienten α_{ij} bestimmen, ob A invertierbar ist, genauer

$$A^{-1} \text{ existiert } \Leftrightarrow d = \alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21} \neq 0.$$

Ist A invertierbar, so ist die inverse Matrix A^{-1} durch die Formel

$$A^{-1} = \frac{1}{d}\begin{pmatrix} \alpha_{22} & -\alpha_{12} \\ -\alpha_{21} & \alpha_{11} \end{pmatrix}$$

gegeben, die ebenfalls d involviert. Der Ausdruck $d \in K$ ist ein Spezialfall einer sogenannten Determinante. Wir ordnen im folgenden jeder Matrix $A \in K^{n\times n}$ eine Determinante $\det(A) \in K$ zu. Diese Invariante enkodiert Information über die Invertierbarkeit von A, lässt sich zur Berechnung von A^{-1} benüzten, und hat geometrische Bedeutung.

Wir definieren die Determinante einer quadratischen Matrix allgemeiner für Matrizen $A = (\alpha_{ij})$, deren Einträge α_{ij} nicht Elemente eines Körpers, sondern allgemeiner Elemente eines kommutativen Rings sind. Ein kommutativer Ring ist dabei eine Menge mit zwei Verknüpfungen, die alle Bedingungen an einen Körper erfüllt, mit Ausnahme der Existenz von mutiplikativ inversen Elementen, genauer:

Definition 10.1. Ein Ring R ist eine Menge, zusammen mit zwei Verknüpfungen $+$ und $\cdot$, sodass gilt:

(1) R ist bzgl. $+$ eine abelsche Gruppe (mit neutralem Element 0),
(2) Es gibt ein $1 \in R$ mit $1r = r = r1$ für $r \in R$; es gilt das Assoziativgesetz $r_1(r_2r_3) = (r_1r_2)r_3$ für $r_1, r_2, r_3 \in R$.
(3) Es gelten die Distributivgesetze, d.h. für $r_1, r_2, r_3 \in R$ ist

$$r_1(r_2 + r_3) = r_1r_2 + r_1r_3 \text{ und } (r_1 + r_2)r_3 = r_1r_3 + r_2r_3.$$

Ein Ring R ist kommutativ, falls zusätzlich gilt

(4) $r_1r_2 = r_2r_1$ für $r_1, r_2 \in R$.

• Die Definition besagt nicht, dass wie in einem Körper $0 \neq 1$ sein muss, inbesondere ist der Nullring $R = \{0\}$ definiert.

Beispiele 10.2. (a) Die ganzen Zahlen $\mathbb{Z}$ formen bzgl. der üblichen Addition und Multiplikation einen kommutativen Ring.

(b) Ist R ein (kommutativer) Ring, so bildet die Menge der n-Tupel

$$R^n = \{(r_1, \ldots, r_n) \mid r_i \in R\}$$

bzgl. der komponentenweisen Addition und Multiplikation wieder einen (kommutativen) Ring.

(c) Die Menge der Polynome $K[x]$ (bzw. $R[x]$) über einem Körper (bzw. einem kommutativen Ring R) bilden bzgl. der Addition und Mutiplikation von Polynomen einen kommutativen Ring.

(d) Sei $R^{n\times n}$ die Menge der quadratischen Matrizen $A = (\alpha_{ij})$ vom Typ (n, n) mit Einträgen α_{ij} aus einem kommutativen Ring R. Dann ist $R^{n\times n}$ bzgl. der Addition und Multipliaktion von Matrizen ein Ring. Der Ring $R^{n\times n}$ ist für $n \geq 2$ in der Regel (z.B. falls $0 \neq 1$ in R) nicht kommutativ.

Definition 10.3. Sei R ein kommutativer Ring und $A = (\alpha_{ij}) \in R^{n\times n}$ eine quadratische Matrix vom Typ (n, n). Die Determinante von A ist

$$\det(A) = \sum_{\tau\in S_n} \operatorname{sgn}(\tau)\alpha_{1\tau(1)}\alpha_{2\tau(2)}\cdots\alpha_{n\tau(n)} \in R$$

• Ist $n = 6$, so hat die die Determinante definierende Formel 720 Terme, d.h. obige Definition liefert ein Ringelement, welches a priori nur schwer berechenbar ist.

Beispiele 10.4. (a) Sei $A = (\alpha_{ij}) \in R^{n\times n}$ eine Dreiecksmatrix mit $\alpha_{ij} = 0$ für $j > i$. Dann sind die in der Determinante $\det(A)$ auftretenden Summanden $\alpha_{1\tau(1)}\alpha_{2\tau(2)}\cdots\alpha_{n\tau(n)}$ nur dann nicht-trivial, wenn $\tau(1) \leq 1, \tau(2) \leq 2, \cdots, \tau(n) \leq n$ ist. Dies gilt nur für die Identitätsabbildung ι, sodass $\det(A)$ das Produkt der Diagonaleinträge ist

$$\det(A) = \alpha_{11}\alpha_{22}\cdots\alpha_{nn}.$$

(b) Sei $A = (\alpha_{ij}) \in R^{2\times 2}$. Es gilt $S_2 = \{\iota, \tau\}$, wobei $\tau = (1, 2)$ ist. Nach Definition ist die Determinante von A dann (vgl. Beispiel 6.15)

$$\begin{aligned}\det(A) &= \operatorname{sgn}(\iota)\alpha_{1\iota(1)}\alpha_{2\iota(2)} + \operatorname{sgn}(1,2)\alpha_{1\tau(1)}\alpha_{2\tau(2)}\\ &= 1\cdot\alpha_{11}\alpha_{22} + (-1)\cdot\alpha_{12}\alpha_{21}\\ &= \alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21} \in R.\end{aligned}$$

(c) In $\mathbb{R}^2$ seien Vektoren $s_1 = (x_1, y_1)^t$ und $s_2 = (x_2, y_2)^t$ gegeben. Wir schreiben diese Vektoren in Polarkoordinaten, d.h. in der Form

$$x_j = r_j\cos(\alpha_j) \text{ und } y_j = r_j\sin(\alpha_j),$$

wobei $0 \leq \alpha_1 \leq \alpha_2 \leq \pi/2$ sei. Sei $\gamma = \alpha_2 - \alpha_1$ der Winkel zwischen (x_2, y_2) und (x_1, y_1). Elementar-Geometrische Überlegungen zeigen, dass die Fläche F des von den Spaltenvektoren s_1 und s_2 aufgespannten Parallelogramms durch die folgende Formel gegeben ist

$$F = r_1 r_2\sin(\gamma).$$

Betrachte den Winkel α_1 zwischen s_1 und der x-Achse. Die Matrix

$$D = \begin{pmatrix} \cos(-\alpha_1) & -\sin(-\alpha_1) \\ \sin(-\alpha_1) & \cos(-\alpha_1) \end{pmatrix}$$

beschreibt die Drehung um den Winkel $-\alpha_1$. Es gilt $\det(D) = 1$. Für

$$A = (s_1, s_2) = \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix}$$

gilt also

$$DA = \begin{pmatrix} r_1 & * \\ 0 & r_2 \sin(\gamma) \end{pmatrix}$$

wobei (siehe Übung) $\det(A) = \det(D)\det(A) = \det(DA) = r_1 r_2 \sin(\gamma)$. Es folgt $F = \det(A)$, d.h. die Determinante entspricht genau dem Volumen des durch die Vektoren aufgespannten Parallelogramms.

Das obige Beispiel (c) suggeriert, dass die Determinante allgemein eine 'Volumenfunktion' ist. Wir zeigen im folgenden, dass jede 'abstrakte Volumenfunktion' bis auf eine Konstante durch die Determinanten gegeben ist. Wir beginnen mit elementaren Eigenschaften.

Für $A \in R^{n\times n}$ mit Zeilen $z_1, \dots z_n$ und Spalten $s_1, \dots, s_n$ betrachten wir im folgenden $\det(A)$ als eine Funktion der Zeilen bzw. Spalten

$$\det(A) = f_{\det}(z_1, \dots, z_n) = g_{\det}(s_1, \dots, s_n).$$

Lemma 10.5. *Sei $A \in R^{n\times n}$. Dann gilt*

(a) $\det(A) = \det(A^t)$,

(b) *Für $r, r' \in R$ und $z_j, z_j' \in R^n$ gilt die Formel*

$$f_{\det}(*, rz_j + r'z_j', *) = r f_{\det}(*, z_j, *) + r' f_{\det}(*, z_j', *)$$

(d.h. für $R = K$ ein Körper und j fest ist die Abbildung $z_j \mapsto f_{\det}(z_1, \dots, z_{j-1}, z_j, z_{j+1}, \dots, z_n)$ linear).

(c) *Ist $z_i = z_j$ für ein $i \neq j$, so ist $f_{\det}(z_1, \dots, z_n) = 0$.*

(d) *Die zu (b) und (c) analogen Aussagen für $g_{\det}(s_1, \dots, s_n)$ gelten.*

Beweis. (a): Sei $A^t = (\beta_{ij})$ mit $\beta_{ij} = \alpha_{ji}$. Nach Definition von A^t ist

$$\begin{aligned} \det(A^t) &= \textstyle\sum_{\tau\in S_n} \operatorname{sgn}(\tau)\beta_{1\tau(1)} \cdots \beta_{n\tau(n)} \\ &= \textstyle\sum_{\tau\in S_n} \operatorname{sgn}(\tau)\alpha_{\tau(1)1} \cdots \alpha_{\tau(n)n} \end{aligned}$$

Wegen $\operatorname{sgn}(\tau)^2 = 1$ ist $\operatorname{sgn}(\tau) = \operatorname{sgn}(\tau)^{-1} = \operatorname{sgn}(\tau^{-1})$. Da τ eine Bijektion ist gilt $\tau(i) = j$ genau dann, wenn $i = \tau^{-1}(j)$ ist. Umordnung der Faktoren (dies verwendet, dass der Ring R kommutativ ist) liefert

$$\alpha_{\tau(1)1} \cdots \alpha_{\tau(n)n} = \alpha_{1\tau^{-1}(1)} \cdots \alpha_{n\tau^{-1}(n)}.$$

Also ist

$$\det(A^t) = \sum_{\tau\in S_n} \operatorname{sgn}(\tau^{-1})\alpha_{1\tau^{-1}(1)}\cdots\alpha_{n\tau^{-1}(n)} = \det(A).$$

(b): Sei $z_j = (\alpha_{j1},\ldots,\alpha_{jn})$ und $z'_j = (\alpha'_{j1},\ldots,\alpha'_{jn})$. Dann gilt wegen

$$\begin{aligned}\textstyle\sum_{\tau\in S_n} \operatorname{sgn}(\tau)\alpha_{1\tau(1)}\ldots(r\alpha_{j\tau(j)} + r'\alpha'_{j\tau(j)})\ldots\alpha_{n\tau(n)} = \\ = r\textstyle\sum_{\tau\in S_n} \operatorname{sgn}(\tau)\alpha_{1\tau(1)}\ldots\alpha_{j\tau(j)}\ldots\alpha_{n\tau(n)} \\ + r'\textstyle\sum_{\tau\in S_n} \operatorname{sgn}(\tau)\alpha_{1\tau(1)}\ldots\alpha'_{j\tau(j)}\ldots\alpha_{n\tau(n)}\end{aligned}$$

die Formel $f_{\det}(*, rz_j + r'z'_j, *) = rf_{\det}(*, z_j, *) + r'f_{\det}(*, z'_j, *)$.
(c): Sei $z_i = z_j$ mit $i < j$ und sei $\sigma = (i, j)$. Dann ist $S_n = A_n \cup A_n\sigma$ eine disjunkte Zerlegung und $\sum_{\tau\in S_n} = \sum_{\pi\in A_n} + \sum_{\pi\sigma\in A_n\sigma}$. Es folgt

$$\begin{aligned} & \operatorname{sgn}(\pi)(\alpha_{1\pi(1)}\ldots\alpha_{n\pi(n)}) + \operatorname{sgn}(\pi\sigma)(\alpha_{1\pi\sigma(1)}\ldots\alpha_{n\pi\sigma(n)}) \\ = \; & \operatorname{sgn}(\pi)(\alpha_{1\pi(1)}\ldots\alpha_{n\pi(n)}) - \operatorname{sgn}(\pi)(\alpha_{1\pi\sigma(1)}\ldots\alpha_{n\pi\sigma(n)}) \\ = \; & \operatorname{sgn}(\pi)(\alpha_{1\pi(1)}\ldots\alpha_{n\pi(n)} - \alpha_{1\pi\sigma(1)}\ldots\alpha_{n\pi\sigma(n)} = 0\end{aligned}$$

da wegen $z_i = z_j$ auch $\alpha_{i\pi\sigma(i)} = \alpha_{i\pi(j)} = \alpha_{j\pi(j)}$.
(d): Folgt mit (a) aus (b) und (c). □

Definition 10.6. Sei R ein kommutativer Ring. Eine Abbildung

$$V : (R^n)^n \to R$$

ist eine abstrakte Volumenfunktion auf R^n falls gilt:

(1) Für $r, r' \in R$ und $z_j, z'_j \in R^n$ ist

$$V(*, rz_j + r'z'_j, *) = rV(*, z_j, *) + r'V(*, z'_j, *)$$

(2) Ist $z_i = z_j \in R^n$, $i \neq j$, so ist $V(z_1,\ldots,z_n) = 0$.

• Nach Lemma 10.5(b)(c) definiert die Determinante eine abstrakte Volumenfunktion $f_{\det} : (R^n)^n \to R,\ (z_1,\ldots,z_n) \mapsto f_{\det}(z_1,\ldots,z_n)$.

Proposition 10.7. *Für eine abstrakte Volumenfunktion V auf R^n gilt*

(a) *Für $i \neq j$ und $r \in R$ ist*

$$V(z_1,\ldots,z_i + rz_j,\ldots,z_n) = V(z_1,\ldots,z_i,\ldots,z_n)$$

(b) *Für $\tau \in S_n$ ist*

$$V(z_{\tau(1)},\ldots,z_{\tau(n)}) = \operatorname{sgn}(\tau)V(z_1,\ldots z_n).$$

(c) *Ist $z_i = (\alpha_{i1},\ldots,\alpha_{in})$ und sind $e_1,\ldots,e_n$ die Vektoren in R^n mit 1 an der Stelle i und 0 sonst, so ist*

$$V(z_1,\ldots,z_n) = \det(\alpha_{ij})V(e_1,\ldots e_n).$$

NB. Die letzte der obigen Aussagen besagt, dass jede abstrakte Volumenfunktion auf R^n bis auf eine Konstante die Determinante ist:

$$V(z_1, \ldots, z_n) = f_{det}(z_1, \ldots, z_n) \cdot V(e_1, \ldots, e_n) = f_{det}(z_1, \ldots, z_n) \cdot c,$$

wobei $c = V(e_1, \ldots, e_n) \in R$ eine Konstante ist.

Beweis. (a): Folgt direkt aus den Eigenschaften (1) und (2) von V.
(b): Sei $\tau = (i, j)$ mit $i < j$. Da V linear in jeder Komponente ist folgt

$$V(*, z_i, *, z_j, *) + V(*, z_j, *, z_i, *) = V(*, z_i + z_j, *, z_j + z_i, *) = 0$$

und die Behauptung gilt für eine Transposition. Eine beliebige Permutation $\tau \in S_n$ lässt sich τ nach Lemma 9.9(b) als ein Produkt geeigneter Transpositionen $\tau = \tau_1 \cdots \tau_k$ schrieben. Setze $\rho = \tau_2 \cdots \tau_k$. Induktion (nach der Anzahl der Faktoren in einer solchen Zerlegung) liefert

$$\begin{aligned} V(z_{\tau(1)}, \ldots, z_{\tau(n)}) &= V(z_{\tau_1\rho(1)}, \ldots, z_{\tau_1\rho(n)}) \\ &= \operatorname{sgn}(\tau_1) V(z_{\rho(1)}, \ldots, z_{\rho(n)}) \\ &= \operatorname{sgn}(\tau_1)\operatorname{sgn}(\rho) V(z_1, \ldots, z_n) \\ &= \operatorname{sgn}(\tau) V(z_1, \ldots, z_n) \end{aligned}$$

(c): Sei $z_i = \sum_{j=1}^n \alpha_{ij} e_j$ für $i = 1, \ldots, n$. Da nach (1) V in jeder Komponente linear ist folgt

$$V(z_1, \ldots, z_n) = \sum_{(j_1, \ldots, j_n)} \alpha_{1j_1} \ldots \alpha_{nj_n} V(e_{j_1}, \ldots, e_{j_n}).$$

Taucht in einem solchen n-Tupel $(j_1, \ldots, j_n)$ eine Zahl wiederholt auf, so gilt nach (2) $V(e_{j_1}, \ldots, e_{j_n}) = 0$. Damit sind die nicht-trivialen Summanden in der obigen Summe genau diejenigen mit $\{j_1, \ldots, j_n\} = \{1, \ldots, n\}$, und zu jedem solchen Summanden gibt es genau eine Permutation $\tau \in S_n$ mit $j_i = \tau(i)$. Mit (b) folgt so

$$\begin{aligned} V(z_1, \ldots, z_n) &= \textstyle\sum_{\tau \in S_n} \alpha_{1\tau(1)} \ldots \alpha_{n\tau(n)} \operatorname{sgn}(\tau) V(e_1, \ldots, e_n) \\ &= \det(\alpha_{ij}) V(e_1, \ldots, e_n) \end{aligned}$$

□

Lemma 10.8. *Für $A, B \in R^{n\times n}$ gilt* $\det(AB) = \det(A)\det(B)$.

• Sei K ein Körper und $A \in K^{n\times n}$. Dann ist A genau dann invertierbar, wenn die Spaltenvektoren von A linear unabhängig sind, also genau dann, wenn $\det(A) \neq 0$ ist. Insbesondere definiert det eine Abbildung $\det : GL_n(K) \to K^\times$; dies ist ein Epimorphismus.

• Seien $z_1, \ldots, z_n \in R^n$ und V eine beliebige abstrakte Volumenfunktion. Dann gibt es eine Konstante $c \in R$, sodass

$$V(z_1, \ldots, z_n) = c \cdot f_{det}(z_1, \ldots, z_n).$$

Ist $A \in R^{n\times n}$ mit Zeilen $z_1, \ldots, z_n$, und ist $B \in R^{n\times n}$ eine weitere Matrix, so hat AB die Zeilen $z_1B, \ldots, z_nB$ und das obige Lemma besagt

$$V(z_1B, \ldots, z_nB) = c\cdot\det(AB) = c\cdot\det(A)\det(B) = V(z_1, \ldots z_n)\det(B),$$

d.h. $\det(B)$ ist der 'Verzerrungsfaktor' der Volumenfunktion V bei Anwendung von B.

Beweis. Seien $z_1, \ldots, z_n$ die Zeilen von A. Betrachte die Abbildung

$$f_B : (R^n)^n \to R,\ (z_1, \ldots, z_n) \mapsto f_{\det}(z_1B, \ldots, z_nB) = \det(AB).$$

Wir zeigen, dass f_B eine abstrakte Volumenfunktion auf R^n definiert. Gilt dies, so gibt es nach Proposition 10.7 eine Konstante $c(B)$ mit

$$f_B(z_1, \ldots, z_n) = f_{\det}(z_1, \ldots, z_n)c(B) = \det(A)c(B).$$

Ist speziell $A = E_n$ die Einheitsmatrix mit den Zeilen $e_1, \ldots, e_n$, so ist

$$\det(B) = \det(E_nB) = f_B(e_1, \ldots, e_n) = \det(E_n)c(B) = c(B),$$

also ist $c(B) = \det(B)$ und $\det(AB) = f_B(z_1, \ldots, z_n) = \det(A)\det(B)$.

Wir verifizieren die Eigenschaften einer Volumenfunktion: Sei $z_i = z_j$ für ein $i \neq j$. Dann stimmen in AB die Zeilen z_iB und z_jB überein, und nach Lemma 10.5(c) ist $\det(AB) = 0$, also gilt

$$f_B(z_1, \ldots, z_n) = \det(AB) = 0.$$

Sei $A = (\alpha_{ij}) \in R^{n\times n}$ mit Zeilen $z_1, \ldots, z_n$, und sei $z'_j = (\alpha'_{j1}, \ldots, \alpha'_{jn})$. Nach Lemma 10.5(b) gilt für $B \in R^{n\times n}$ und $r, r' \in R$ die Formel

$$\det\begin{pmatrix} z_1B \\ \cdot \\ \cdot \\ (rz_j + r'z'_j)B \\ \cdot \\ \cdot \\ z_nB \end{pmatrix} = r\det\begin{pmatrix} z_1B \\ \cdot \\ \cdot \\ z_jB \\ \cdot \\ \cdot \\ z_nB \end{pmatrix} + r'\det\begin{pmatrix} z_1B \\ \cdot \\ \cdot \\ z'_jB \\ \cdot \\ \cdot \\ z_nB, \end{pmatrix}$$

also ist

$$f_B(*, rz_j + r'z'_j, *) = rf_B(*, z_j, *) + r'f_B(*, z'_j, *)$$

und f_B definiert eine abstrakte Volumenfunktion. □

Wir kommen zur Berechnung von Determinanten.

Lemma 10.9. *(Kästchensatz) Seien $B \in R^{m\times m}$, $C \in R^{n\times n}$ und weiter $D \in R^{n\times m}$. Setze $k = m + n$ und betrachte die $k \times k$-Matrix*

$$A = \begin{pmatrix} B & 0 \\ D & C \end{pmatrix}.$$

Dann gilt: $\det(A) = \det(B)\det(C)$.

Beweis. Sei $E_l \in R^{l\times l}$ die Einheitsmatrix. Aufgrund der Darstellung

$$\begin{pmatrix} B & 0 \\ D & C \end{pmatrix} = \begin{pmatrix} B & 0 \\ D & E_n \end{pmatrix} \begin{pmatrix} E_m & 0 \\ 0 & C \end{pmatrix},$$

genügt es nach Lemma 10.8 die folgenden Identitäten zu beweisen

$$\det \begin{pmatrix} B & 0 \\ D & E_n \end{pmatrix} = \det(B) \text{ und } \det \begin{pmatrix} E_m & 0 \\ 0 & C \end{pmatrix} = \det(C)$$

Seien $z_1, \ldots, z_n \in R^n$ und sei $C(z_i) \in R^{n\times n}$ die durch die Zeilen $z_1, \ldots, z_n$ definierte Matrix. Dann definiert die Abbildung

$$h : (R^n)^n \to R,\ (z_1, \ldots, z_n) \mapsto \det \begin{pmatrix} E_m & 0 \\ 0 & C(z_i) \end{pmatrix}$$

eine abstrakte Volumenfunktion auf R^n. Nach Lemma 10.7(b) unterscheidet sich h von der Determinatenfunktion nur um eine Konstante, d.h. es gibt ein $c \in R$, sodass für jede Matrix $C(z_i)$ gilt

$$h(z_1, \ldots, z_n) = c \cdot f_{\det}(z_1, \ldots, z_n).$$

Ist $C(z_i) = E_n$ die Einheitsmatrix mit den Zeilen $e_1, \ldots, e_n$, so folgt

$$1 = \det(E_k) = h(e_1, \ldots, e_n) = c \cdot f_{\det}(e_1, \ldots, e_n) = c$$

und somit $h(z_1, \ldots, z_n) = f_{\det}(z_1, \ldots, z_n)$. Dies zeigt

$$\det \begin{pmatrix} E_m & 0 \\ 0 & C \end{pmatrix} = \det(C).$$

Die verbleibende Behauptung folgt analog: Für $z_1, \ldots, z_m \in R^m$ und $B(z_i) \in R^{m\times m}$ die Matrix mit Zeilen $z_1, \ldots, z_m$ definiert die Abbildung

$$k : (R^m)^m \to R,\ (z_1, \ldots, z_m) \mapsto \det \begin{pmatrix} B & 0 \\ D & E_n \end{pmatrix}$$

eine abstrakte Volumenfunktion. Also gibt es ein $c \in R$, sodass

$$k(z_1, \ldots, z_m) = c \cdot f_{\det}(z_1, \ldots, z_m).$$

Der Fall $B(z_i) = E_m$ liefert $c = 1$ und es folgt

$$\det \begin{pmatrix} B & 0 \\ D & E_n \end{pmatrix} = \det(B).$$

□

Beispiele 10.10. (a) Sei K ein Körper und $A, B, C, D \in K^{n\times n}$ mit $AC = CA$. Wegen $AC = CA$ gilt dann die Identiät

$$\begin{pmatrix} E_n & 0 \\ -C & A \end{pmatrix} \cdot \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} A & B \\ 0 & AD - CB \end{pmatrix}.$$

Mit Lemma 10.9 folgt

$$\det(A)\det\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det(A)\det(AD - CB)$$

Gilt weiter $\det(A) \neq 0$, so kann man durch $\det(A)$ teilen und erhält

$$\det\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det(AD - CB),$$

d.h. die Determinante der $2n \times 2n$-Matrix auf der linken Seite dieser Gleichung ist gleich der Determinante der $n \times n$-Matrix auf der rechten Seite.

(b) Seien $A, B, C, D \in K^{n\times n}$ wie in (a). Gilt $AC = CA$, so kann man zeigen

$$\det\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det(AD - CB),$$

auch wenn $\det(A) = 0$ ist. Für $AC \neq CA$ gilt dies nicht: Betrachte

$$A = D = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ und } B = -C = \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix}.$$

Es gilt $\det(A) = 1$ und $AC \neq CA$. Direktes Nachrechnen zeigt weiter

$$\det\begin{pmatrix} A & -C \\ C & A \end{pmatrix} = 2 \neq 1 = \det(A^2 + C^2).$$

Wir geben abschliessend zwei allgemeine Methoden zur Berechnung von Determinaten an.

I. Zeilenstufenform. Sei $R = K$ ein Körper und $A \in K^{n\times n}$. Nach Theorem 7.4 gibt es Elementarmatrizen $T_1, \ldots, T_k, S_1, \ldots, S_l \in K^{n\times n}$, sodass $A' = T_k \cdots T_1 A S_1 \cdots S_l$ eine obere Dreiecksmatrix ist. Nach Definition haben alle Elementarmatrizen die Determinante 1 und Lemma 10.8 besagt, dass $\det(A') = \det(A)$ ist. Da A' eine obere Dreiecksmatrix ist, ist $\det(A')$ das Produkt der Diagonaleinträge und leicht berechenbar.

Beispiel 10.11. Sei $A \in \mathbb{R}^{3\times 3}$ die Matrix

$$A = \begin{pmatrix} 1 & -1 & 2 \\ 4 & 4 & -2 \\ 2 & 0 & 2 \end{pmatrix}$$

Wie in Beispiel 7.5(a) lässt sich A mittels elementarer Umformungen in die Matrix

$$A' = \begin{pmatrix} 1 & -1 & 2 \\ 0 & 8 & 10 \\ 0 & 0 & 1/2 \end{pmatrix}$$

überführen. Es folgt $\det(A) = 8 \cdot (1/2) = 4$.

II. Laplace Entwicklung. Betrachte $A = (\alpha_{ij}) \in R^{3\times 3}$. Sei $A_{ij} \in R$ die Determinante der Matrix, die aus A durch ersetzen der i-ten Zeile durch die Zeile e_j (mit 1 an der Stelle j und 0 sonst) entsteht, z.B.

$$A_{12} = \det \begin{pmatrix} 0 & 1 & 0 \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{pmatrix}.$$

Dies liefert n^2 Elemente A_{ij} von R. Sei $\widetilde{A} = (A_{ij})^t \in R^{3\times 3}$. Dann ist

$$A \cdot \widetilde{A} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{pmatrix} \cdot \begin{pmatrix} A_{11} & A_{21} & A_{31} \\ A_{12} & A_{22} & A_{32} \\ A_{13} & A_{23} & A_{33} \end{pmatrix}$$

Dieses Produkt hat an der Stelle $(1,1)$ den Ausdruck

$$\alpha_{11} \cdot \det \begin{pmatrix} 1 & 0 & 0 \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{pmatrix} + \alpha_{12} \cdot \det \begin{pmatrix} 0 & 1 & 0 \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{pmatrix} + \\ + \alpha_{13} \cdot \det \begin{pmatrix} 0 & 0 & 1 \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{pmatrix}$$

Da die Determinante in einer Zeile linear ist, ist dies genau $\det(A)$. Analog steht in dem Produkt $A \cdot \widetilde{A}$ an den Stellen $(2,2)$ und $(3,3)$ das Ringelement $\det(A)$. An den Stellen (i,j) mit $i \neq j$ ist der Eintrag 0, da nach Definition von $\widetilde{A}$ in diesem Fall der Eintrag die Determinante einer Matrix mit zwei identischen Zeilen ist. Also ist $A \cdot \widetilde{A} = \det(A) \cdot E_3$. Insbesondere ist im Fall $R = K$ ein Körper die Matrix A invertierbar genau dann, wenn $\det(A) \neq 0$, und in diesem Fall ist $A^{-1} = \det(A)^{-1}\widetilde{A}$. Weiter ergibt sich eine explizite Möglichkeit für die Berechnung von $\det(A)$: Die in der obigen Summe auftretenden Determinanten lassen sich nach einer Vertauschung von Spalten mittels dem Kästchensatz 10.9 leicht berechnen. Da eine solche Vertauschung τ nach Lemma 10.7(c) die Determinante nur um $\operatorname{sgn}(\tau)$ ändert, folgt

$$\det(A) = \alpha_{11} \det \begin{pmatrix} \alpha_{22} & \alpha_{23} \\ \alpha_{32} & \alpha_{33} \end{pmatrix} - \alpha_{12} \det \begin{pmatrix} \alpha_{21} & \alpha_{23} \\ \alpha_{31} & \alpha_{33} \end{pmatrix} + \alpha_{13} \det \begin{pmatrix} \alpha_{21} & \alpha_{22} \\ \alpha_{31} & \alpha_{32} \end{pmatrix}$$

Dies ist die Berechnung von $\det(A)$ mittels 'Entwicklung nach der 1.Zeile'. Analog lässt sich die Determinante mittels Entwicklung nach einer beliebigen Zeile oder Spalte berechnen.

Allgemein gilt:

Definition 10.12. Sei $A = (\alpha_{ij}) \in R^{n\times n}$, und sei $A_{ij} \in R$ die Determinante der Matrix, die aus A durch Ersetzen der i-ten Zeile durch $e_j = (0, \ldots, 0, 1, 0, \ldots, 0)$ mit 1 an der Stelle j entsteht, d.h.

$$A_{ij} = \det \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1j} & \cdots & \alpha_{1n} \\ \cdot & \cdots & \cdot & \cdots & \cdot \\ 0 & \cdots & 1 & \cdots & 0 \\ \cdot & \cdots & \cdot & \cdots & \cdot \\ \alpha_{n1} & \cdots & \alpha_{nj} & \cdots & \alpha_{nn} \end{pmatrix}$$

Die Adjunkte $\widetilde{A}$ von A ist die Matrix $(A_{ij})^t$.

• Die explizite Berechnung von $\widetilde{A}$ für $A \in R^{n\times n}$ erfordert die Berechnung von n^2 Determinanten.

• Sei $A \setminus \{ij\}$ die Matrix, die aus A durch Streichen der i-ten Zeile und der j-ten Spalte entsteht. Aus Lemma 10.7(b) und Lemma 10.9 folgt

$$A_{ij} = (-1)^{i+j} \det(A \setminus \{ij\}).$$

• Die Einträge A_{ij} lassen sich gleichwertig als die Determinante derjenigen Matrix definieren, die aus A durch Ersetzen der j-ten Spalte durch $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ mit 1 an der Stelle i entsteht.

Theorem 10.13. *Sei $A = (\alpha_{ij}) \in R^{n\times n}$. Dann gilt:*

(a) *$A\widetilde{A} = det(A)E_n$, d.h. $\sum_{j=1}^n \alpha_{ij}A_{kj} = \delta_{ik}\det(A)$; ist $k = i$, so ist $\sum_{j=1}^n \alpha_{ij}A_{ij} = det(A)$ (Entwicklung nach der i-ten Zeile).*

(b) *$\widetilde{A}A = det(A)E_n$, d.h. $\sum_{j=1}^n A_{ji}\alpha_{jk} = \delta_{ik}\det(A)$; ist $k = i$, so ist $\sum_{j=1}^n A_{ji}\alpha_{ji} = det(A)$ (Entwicklung nach der i-ten Spalte).*

(c) *Ist $R = K$ ein Körper, so ist A genau dann invertierbar, wenn $det(A) \neq 0$ ist. In diesem Fall ist $A^{-1} = det(A)^{-1}\widetilde{A}$.*

Beweis. (a): Das Produkt $A\widetilde{A}$ hat an der Stelle (i, k) den Eintrag

$$\sum_{j=1}^{n} \alpha_{ij}A_{kj} = \delta_{ik}\det(A).$$

Somit sind die einizgen nicht-trivialen Einträge von $A\widetilde{A}$ die Einträge $\det(A)$ auf der Diagonalen ($i = k$), und $A\widetilde{A} = \det(A)E_n$.

(b): Analog mittels A_{ij} als Determinante nach Spaltenvertauschung.

(c): Existiert A^{-1}, so ist $AA^{-1} = E_n$, und $\det(A) \neq 0$ folgt aus

$$1 = \det(E_n) = \det(AA^{-1}) = \det(A)\det(A^{-1}).$$

Ist umgekehrt $\det(A) \neq 0$, so gilt nach (a) $A^{-1} = \det(A)^{-1}\widetilde{A}$. □

Beispiele 10.14. (a): Betrachte die Matrix mit reellen Einträgen

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 1 \\ 2 & 1 & 1 \end{pmatrix}.$$

Nach Theorem 10.13(a) ist $\det(A) = \sum_{j=1}^{3} \alpha_{ij} A_{ij}$. Im Fall $i = 1$ (Entwicklung nach der 1. Zeile) ergibt sich die Formel

$$\det(A) = \alpha_{11} A_{11} + \alpha_{12} A_{12} + \alpha_{13} A_{13}.$$

Wegen $\alpha_{11} = 1$ folgt mit dem Kästchensatz 10.9

$$A_{11} = \det(1) \cdot \det \begin{pmatrix} 4 & 1 \\ 1 & 1 \end{pmatrix} = 1 \cdot (4 - 1) = 3,$$

also ist $\alpha_{11} A_{11} = 1 \cdot 3 = 3$. Nachrechnen liefert $\alpha_{12} A_{12} = 2 \cdot 2 = 4$ und $\alpha_{13} A_{13} = 3 \cdot (-8) = -24$. Also ist $\det(A) = 3 + 4 - 24 = -17$.

Effizienter ist hier die Entwicklung nach der 1. Spalte (da der Eintrag $\alpha_{21} = 0$ ist). Explizit:

$$\det(A) = 1 \cdot \det \begin{pmatrix} 4 & 1 \\ 1 & 1 \end{pmatrix} + 2 \cdot \det \begin{pmatrix} 2 & 3 \\ 4 & 1 \end{pmatrix} = 1 \cdot (4-1) + 2 \cdot (2-12) = -17.$$

(b): Für die Matrix

$$A = \begin{pmatrix} 5 & 0 & 3 & -1 \\ 3 & 0 & 0 & 4 \\ -1 & 2 & 4 & -2 \\ 1 & 0 & 0 & 5 \end{pmatrix} \in \mathbb{R}^{4 \times 4}$$

liefert Entwicklung nach den jeweiligen Spalten mit vielen Nullen

$$\det(A) = -2 \cdot \det \begin{pmatrix} 5 & 3 & -1 \\ 3 & 0 & 4 \\ 1 & 0 & 5 \end{pmatrix} = -2 \cdot (-3) \det \begin{pmatrix} 3 & 4 \\ 1 & 5 \end{pmatrix} = 6 \cdot 11 = 66.$$