Lineare Algebra
HS 2010
Mannheim

Claus Hertling

02.12.2010

Inhaltsverzeichnis

hertling@math.uni-mannheim.de

0 Einige grundlegende Begriffe und Notationen

Mengen: Georg Cantor (Begründer der Mengenlehre):
"Eine Menge ist eine Zusammenfassung bestimmter wohlunterschiedener Objekte unserer Anschauung oder unseres Denkens – welche die Elemente der Menge genannt werden – zu einem Ganzen."

$\mathbb{N}$ = Menge der natürlichen Zahlen = $\{1, 2, 3, ...\}$;
$\mathbb{Z}$ = Menge der ganzen Zahlen = $\{0, 1, -1, 2, -2, ...\}$;
$\mathbb{Q}$ = Menge der rationalen Zahlen;
$\mathbb{R}$ = Menge der reellen Zahlen;
$\emptyset$ = die leere Menge;
$\{1\},\ \{1, 2, 3\},\ \{\{1\}, 2, 3\}, ...$

"$a \in M$" heißt: a ist Element der Menge M;
$1 \in \{1, 2, 3\},\ 4 \notin \{1, 2, 3\}$.

Seien M_1 und M_2 zwei Mengen;
$M_1 \cup M_2$ ist die Vereinigungsmenge von M_1 und M_2,
$M_1 \cup M_2 = \{a \mid a \in M_1$ oder $a \in M_2\}$,
"die Menge der a, für die gilt: a in M_1 oder a in M_2";
$M_1 \cap M_2$ ist die Schnittmenge von M_1 und M_2,
$M_1 \cap M_2 = \{a \mid a \in M_1$ und $a \in M_2\}$;
$M_1 - M_2 = M_1 \setminus M_2 = \{a \in M_1 \mid a \notin M_2\}$ = die Differenzmenge
("M_1 ohne M_2");
$M_1 \times M_2 = \{(a, b) \mid a \in M_1, b \in M_2\}$
= Produkt der Mengen M_1 und M_2;
(a, b) "geordnetes Paar" aus a und b;
$\mathbb{R} \times \mathbb{R} = \mathbb{R}^2 = \{(x_1, x_2) \mid x_1 \in \mathbb{R}, x_2 \in \mathbb{R}\}$ = die reelle Ebene;
sei $n \in \mathbb{N}$, $\mathbb{R}^n = \{(x_1, ..., x_n) \mid x_i \in \mathbb{R}$ für alle $i = 1, ..., n\}$;
$(x_1, ..., x_n)$ "geordnetes n-Tupel".

$\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\};\ \mathbb{R}_0^+ = \{x \in \mathbb{R} \mid x \geq 0\} = \mathbb{R}^+ \cup \{0\}$.
$\mathbb{R}^- = \{x \in \mathbb{R} \mid x < 0\};\ \mathbb{R}_0^- = \mathbb{R}^- \cup \{0\}$;
analog für $\mathbb{Q}$ und $\mathbb{Z}$;
$\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

Zwei Mengen M_1 und M_2 heißen disjunkt, falls $M_1 \cap M_2 = \emptyset$.
Eine Menge M_1 ist die *disjunkte Vereinigung* von zwei Mengen M_2 und M_3 falls $M_1 = M_2 \cup M_3$ und $M_2 \cap M_3 = \emptyset$.
$M_1 \subset M_2$ heißt, daß M_1 eine Teilmenge von M_2 ist, d.h. alle Elemente von M_1 sind auch Elemente von M_2.

Ist M eine Menge mit unendlich vielen Elementen, so ist $|M| = \infty$; hat eine Menge M nur endlich viele Elemente, so ist $|M|$ die Anzahl dieser Elemente. In beiden Fällen heißt $|M|$ die *Ordnung* von M.
Die Potenzmenge $\mathcal{P}(M)$ einer Menge M ist die Menge aller Teilmengen von M. Ist M endlich, so auch $\mathcal{P}(M)$, und dann ist $|\mathcal{P}(M)| = 2^{|M|}$.

Abbildungen: Eine Abbildung f von einer Menge X in eine Menge Y ist eine Vorschrift, die jedem Element von X ein Element von Y zuordnet.
Notation: $f : X \to Y, \quad x \mapsto f(x)$;
hier ist $x \in X$, und $f(x) \in Y$ ist das zugeordnete Element.
X ist der *Definitionsbereich*, und Y ist der *Wertebereich* der Abbildung f.

Ist $f : M_1 \to M_2$ eine Abbildung und $M_3 \subset M_1$, so ist $f(M_3) = \{f(x) \mid x \in M_3\}$ *das Bild von* M_3 *unter* f; es ist $f(M_3) \subset M_2$.

Beispiele:

$$
\begin{aligned}
&f_1 : \mathbb{R} \to \mathbb{R}, \quad x \mapsto x^2;\\
&f_2 : \mathbb{R} \to \mathbb{R}, \quad x \mapsto x^3;\\
&f_3 : \mathbb{R}_0^+ \to \mathbb{R}_0^+, \quad x \mapsto \sqrt{x};\\
&f_4 : \{3,4\} \to \{1\}, \quad 3 \mapsto 1,\ 4 \mapsto 1;\\
&f_5 : \{g \mid g : \mathbb{R} \to \mathbb{R} \text{ Abbildung}\} \to \mathbb{R}, \quad g \mapsto g(7);\\
&f_6 : \mathbb{R} \to \{g \mid g : \mathbb{R} \to \mathbb{R} \text{ Abbildung}\},\\
&\quad x \mapsto (\text{die konstante Abbildung mit Wert } x);\\
&f_7 : \mathbb{R} \to \mathbb{R}_0^+, \quad x \to x^2;\\
&f_8 : \mathbb{R}_0^+ \to \mathbb{R}_0^+, \quad x \to x^2.
\end{aligned}
$$

Definition 0.1 Eine Abbildung $f : X \to Y$ ist
injektiv, falls aus $x_1, x_2 \in X,\ x_1 \neq x_2$ auch $f(x_1) \neq f(x_2)$ folgt, d.h. falls verschiedene Elemente von X unter f verschiedene Bilder in Y haben;
surjektiv, falls zu jedem $y \in Y$ ein $x \in X$ existiert mit $f(x) = y$, d.h. falls das Bild der Menge X unter f die ganze Menge Y ist;
bijektiv, falls f injektiv und surjektiv ist, d.h. falls zu jedem $y \in Y$ *genau ein* $x \in X$ mit $f(x) = y$ existiert.

Ist $f : X \to Y$ bijektiv, so bezeichnet $f^{-1} : Y \to X$ die Abbildung mit

$$f^{-1}(y) = (\text{das eindeutige } x \text{ mit } f(x) = y).$$

f^{-1} ist die *Umkehrabbildung* von f.

Beispiel	injektiv	surjektiv	bijektiv
f_1	nein	nein	nein
f_2	ja	ja	ja
f_3	ja	ja	ja
f_4	nein	ja	nein
f_5	nein	ja	nein
f_6	ja	nein	nein
f_7	nein	ja	nein
f_8	ja	ja	ja

Definition 0.2 Die *Komposition* zweier Abbildungen $f : X \to Y$ und $g : Y \to Z$ ist die Abbildung $g \circ f : X \to Z$, $x \mapsto g(f(x))$.

Lemma 0.3 *a) Die Komposition zweier Abbildungen ist* assoziativ*, d.h. wenn $f : X \to Y$, $g : Y \to Z$ und $h : Z \to W$ Abbildungen sind, so ist*

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

b) Ist $f : X \to Y$ bijektiv und $f^{-1} : Y \to X$ die Umkehrabbildung, so ist

$$f^{-1} \circ f = \mathrm{id}_X : X \to X,\ x \mapsto x,$$

die identische Abbildung auf X, und

$$f \circ f^{-1} = \mathrm{id}_Y : Y \to Y,\ y \mapsto y;$$

und natürlich ist

$$f \circ \mathrm{id}_X = f = \mathrm{id}_Y \circ f.$$

Beweis: a)

$$\begin{aligned}(h \circ (g \circ f))(x) &= h((g \circ f)(x)) = h(g(f(x))) \\ &= (h \circ g)(f(x)) = ((h \circ g) \circ f)(x).\end{aligned}$$

b) Die ersten beiden Formelzeilen folgen aus der Definition von f^{-1}, die dritte ist klar. □

"□" bezeichet das Ende eines Beweises (ebenso q.e.d.= quod erat demonstrandum).

1 Gruppen

Eine Verknüpfung $*$ auf einer Menge G ist eine Abbildung

$$* : G \times G \to G, \quad (a, b) \mapsto *(a, b).$$

Wir schreiben $a * b$ statt $*(a, b)$.

Definition 1.1 a) Eine *Gruppe* ist ein Paar $(G, *)$, wobei G eine Menge und $*$ eine Verknüpfung auf G ist, so daß folgende Eigenschaften erfüllt sind:

(G1) *Assoziativität*: für alle $a, b, c \in G$ gilt

$$a * (b * c) = (a * b) * c.$$

(G2) Existenz eines *neutralen Elements*: es gibt ein $e \in G$ mit

$$a * e = e * a = a \text{ für alle } a \in G.$$

(G3) Existenz von *inversen Elementen*: zu jedem $a \in G$ gibt es ein $a' \in G$ mit

$$a * a' = a' * a = e.$$

b) Eine Gruppe heißt *abelsch* (oder *kommutativ*), falls zusätzlich gilt:

(G4) *Kommutativität*: für alle $a, b \in G$ gilt $a * b = b * a$.

Beispiele 1.2 i) $(\mathbb{R}, +)$ ist eine abelsche Gruppe mit $e = 0$, $a' = -a$, ebenso $(\mathbb{Q}, +)$ und $(\mathbb{Z}, +)$.
ii) $(\mathbb{Q} - \{0\}, \cdot)$ mit $\cdot =$ *Multiplikation* ist eine abelsche Gruppe mit $e = 1$, $a' = a^{-1}$, ebenso $(\mathbb{Q}^+, \cdot)$, $(\mathbb{R} - \{0\}, \cdot)$ und $(\mathbb{R}^+, \cdot)$.
iii) Dagegen ist $(\mathbb{R}_0^+, +)$ keine Gruppe: zwar ist die Addition eine Verknüpfung auf $\mathbb{R}_0^+$ (sie schickt $\mathbb{R}_0^+ \times \mathbb{R}_0^+$ auf $\mathbb{R}_0^+$, denn $a \geq 0, b \geq 0 \Rightarrow a+b \geq 0$), und $e = 0$ ist ein neutrales Element, aber zu $x > 0$ gibt es kein inverses Element in $\mathbb{R}_0^+$.
iv) $(\mathbb{Q}, \cdot)$ ist keine Gruppe, denn 0 hat kein inverses Element in $\mathbb{Q}$ bezüglich der Multiplikation.
Ebenso ist $(\mathbb{Z} - \{0\}, \cdot)$ keine Gruppe, denn alle Elemente in $\mathbb{Z} - \{-1, 0, 1\}$ haben keine inversen Elemente in $\mathbb{Z} - \{0\}$ bezüglich der Multiplikation.
v) Auf $G = \mathbb{R}$ definiere

$$*_{am} : G \times G \to G \quad (x, y) \mapsto \frac{x + y}{2},$$

das arithmetische Mittel.

$(G, *_{am})$ ist keine Gruppe: $*_{am}$ ist nicht assoziativ, z.B.

$$\begin{aligned}(1 *_{am} 1) *_{am} 2 &= \frac{\frac{1+1}{2}+2}{2} = \frac{3}{2}\\ \neq \quad 1 *_{am} (1 *_{am} 2) &= \frac{1+\frac{1+2}{2}}{2} = \frac{5}{4},\end{aligned}$$

und überdies existiert kein neutrales Element: aus $x = x *_{am} e = \frac{x+e}{2}$ würde folgen, daß $e = x$ ist; aber man braucht ein gemeinsames e für alle x.

Lemma 1.3 *Sei $(G, *)$ eine Gruppe.*
a) Es gibt nur ein neutrales Element.
b) Es gibt zu jedem $a \in G$ nur ein inverses Element.
c) Kürzungsregel: erfüllen $a, b, c \in G$ die Gleichung $a * b = a * c$ so ist $b = c$.

Beweis: a) Sind e und $\widetilde{e}$ neutrale Elemente, so ist $e = e * \widetilde{e} = \widetilde{e}$.
b) Sind a' und $\widetilde{a}'$ inverse Elemente von a, so ist

$$a' = a' * e = a' * (a * \widetilde{a}') = (a' * a) * \widetilde{a}' = e * \widetilde{a}' = \widetilde{a}'.$$

c)

$$b = e * b = (a' * a) * b = a' * (a * b) = a' * (a * c) = (a' * a) * c = e * c = c.$$

□

Notationen 1.4 i) Oft wird bei einer Gruppe $(G, *)$ das Verknüpfungssymbol $*$ weggelassen: man schreibt ab oder $a \cdot b$ statt $a * b$; man sagt, man schreibt die Verknüpfung multiplikativ. Das eindeutige neutrale Element heißt e oder 1_G (oder 1), das eindeutige inverse Element zu a heißt a^{-1}.
Man schreibt $a^2 = a \cdot a$, $a^3 = a \cdot a \cdot a$, $a^n = a \cdot ... \cdot a$ (n Faktoren) bei $n \geq 1$, $a^0 = e$, $a^{-n} = a^{-1} \cdot ... \cdot a^{-1}$ (n Faktoren) bei $n \geq 1$. Dann ist $a^{n_1} a^{n_2} = a^{n_1+n_2}$ für $n_1, n_2 \in \mathbb{Z}$.
ii) Manchmal, aber nur wenn die Gruppe abelsch ist, schreibt man die Verknüpfung als Addition, also $a+b$ statt $a*b$. Dann heißt das neutrale Element 0, und das inverse Element zu a heißt $-a$. Dann schreibt man

$n \cdot a = a + ... + a$	(n Summanden)	bei $n \geq 1$,
$n \cdot a = 0$		bei $n = 0$,
$n \cdot a = (-a) + ... + (-a)$	(n Summanden)	bei $n \leq -1$,

und $a - b = a + (-b)$.
iii) Oft ergibt sich aus dem Kontext, welche Verknüpfung gemeint ist. Dann spricht man von der Gruppe G.

Satz 1.5 *Sei X eine nichtleere Menge und $Bij(X, X) := \{f : X \to X \mid f$ ist bijektiv$\}$.*
$(\mathrm{Bij}(X, X), \circ)$ ist eine Gruppe mit $e = \mathrm{id}_X$.

Beweis: Lemma 0.3. □

Bemerkung 1.6 Sei X eine Menge mit mindestens zwei Elementen (d.h. $|X| \geq 2$). Sei $\mathrm{Abb}(X, X)$ die Menge aller Abbildungen von X nach X. Trotz Lemma 0.3 ist $(\mathrm{Abb}(X, X), \circ)$ keine Gruppe. Denn die Menge $\mathrm{Abb}(X, X) - \mathrm{Bij}(X, X)$ ist nicht leer wegen $|X| \geq 2$; und die Elemente in dieser Menge haben keine inversen Elemente: um das zweite einzusehen, muß man zeigen, daß die Gleichungen

$$f' \circ f = \mathrm{id}_X = f \circ f'$$

implizieren, daß f bijektiv ist. Übung ...., mit Hilfe von Blatt 1, Übung 2.

Definition 1.7 Im Fall $X = \{1, ..., n\}$ für ein $n \in \mathbb{N}$ heißt $(\mathrm{Bij}(X, X), \circ)$ die *symmetrische Gruppe* S_n. Ihre Elemente heißen *Permutationen*.
Eine Notation für ein Element $\sigma \in S_n$: $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$.
Später wird das Verknüpfungssymbol $\circ$ oft weggelassen.

Lemma 1.8 *Für $n \geq 3$ ist die symmetrische Gruppe S_n nicht abelsch. Die Gruppen S_1 und S_2 sind abelsch.*

Beweis: $S_1 = \{\mathrm{id}_{\{1\}}\}$, $S_2 = \{\mathrm{id}_{\{1,2\}}, \varphi\}$ mit $\varphi : 1 \mapsto 2,\ 2 \mapsto 1$.
Sei $n \geq 3$.

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 3 & 1 & 4 & \dots & n \end{pmatrix}, \qquad \tau := \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 2 & 1 & 3 & 4 & \dots & n \end{pmatrix},$$

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 3 & 2 & 1 & 4 & \dots & n \end{pmatrix}, \qquad \tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 1 & 3 & 2 & 4 & \dots & n \end{pmatrix}.$$

Es ist $\sigma \circ \tau \neq \tau \circ \sigma$. □

Lemma 1.9 *Die symmetrische Gruppe S_n hat*

$$n! = n(n-1) \cdot ... \cdot 2 \cdot 1 \quad (\text{“}n \textit{ Fakultät}''\text{)}$$

Elemente.

Beweis: Wieviel Freiheit hat man bei der Wahl eines Elementes $\sigma \in S_n$?
Der Wert $\sigma(1)$ kann beliebig in $\{1, 2, ..., n\}$ gewählt werden; also n Möglichkeiten.
Der Wert $\sigma(2)$ kann beliebig in $\{1, 2, ..., n\} - \{\sigma(1)\}$ gewählt werden; also $n - 1$ Möglichkeiten.
....
Der Wert $\sigma(n)$ ist das einzige Element von $\{1, 2, ..., n\} - \{\sigma(1), ..., \sigma(n-1)\}$, also 1 Möglichkeit.
Insgesamt hat man $n \cdot (n-1) \cdot ... \cdot 1$ Möglichkeiten. □

Definition 1.10 a) Eine Permutation $\sigma \in S_n$ heißt *zyklisch*, falls es ein Tupel $(a_1, a_2, ..., a_k)$ gibt mit $2 \leq k \leq n$, $a_1, ..., a_k \in \{1, ..., n\}$, $a_i \neq a_j$ für $i \neq j$, und so, daß

$$\begin{aligned} \sigma(a_i) &= a_{i+1} \text{ für } i = 1, ..., k-1, \\ \sigma(a_k) &= a_1, \\ \sigma(b) &= b \text{ für } b \in \{1, ..., n\} - \{a_1, ..., a_k\} \end{aligned}$$

ist. Notation: Dann schreibt man für σ auch $(a_1 a_2 ... a_k)$.
Skizze mit a_1,...,a_k auf einem Kreis,
Pfeilen von a_i nach a_{i+1}
und σ an diesen Pfeilen
b) Eine zyklische Permutation mit $k = 2$ heißt Transposition.

Beispiele 1.11 i) Im Beweis von Lemma 1.8 waren σ, τ, $\sigma \circ \tau$ und $\tau \circ \sigma \in S_n$ im Fall $n = 3$ zyklisch:

$$\begin{aligned} &\sigma = (123) = (231) = (312), \\ &\tau = (12) = (21) \text{ eine Transposition,} \\ &\text{ebenso } \sigma \circ \tau = (13) = (31),\ \tau \circ \sigma = (23) = (32). \end{aligned}$$

ii) Wegen $k \geq 2$ in Definition 1.10 ist $e = \mathrm{id} \in S_n$ nicht zyklisch.
iii) In S_5 ist

$$(1\ 2\ 3\ 4\ 5)(1\ 3\ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix} = (1\ 4\ 5\ 2\ 3).$$

Vorsicht: Jeden Zykel von links nach rechts durchlaufen, aber die Zykel von rechts nach links abarbeiten (wichtig in Klausuren!).

Satz 1.12 *a) Ist $\sigma = (a_1 a_2 ... a_k) \in S_n$ eine zyklische Permutation, so ist die Menge $\{a_1, a_2, ..., a_k\}$ eindeutig bestimmt. Sie heißt Träger von σ,* $\mathrm{Tr}(\sigma)$.
b) Jede Permutation $\sigma \in S_n - \{\mathrm{id}\}$ ist ein Produkt von eindeutig bestimmten zyklischen Permutationen mit paarweise disjunkten Trägern (d.h. je zwei Träger haben leere Schnittmenge). Diese zyklischen Permutationen kommutieren. Daher kommt es bei der Darstellung von σ als Produkt von ihnen nicht auf die Reihenfolge an.

Beispiel 1.13 Sei

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 6 & 4 & 2 & 1 \end{pmatrix} \in S_6$$

Dann ist

$$1 \mapsto 3 \mapsto 6 \mapsto 1, \quad 2 \mapsto 5 \mapsto 2, \quad 4 \mapsto 4,$$

also

$$\sigma = (136)(25) = (25)(136) = (52)(361) = (613)(52) = ...$$

Beweis von Satz 1.12: Man betrachtet die Folge der Zahlen $1, \sigma(1), \sigma^2(1), \sigma^3(1), \ldots$. Weil die Menge $\{1, 2, ..., n\}$ endlich ist, taucht irgendwann eine Zahl zum zweitenmal auf. Es gibt ein $k_0 \in \mathbb{N} \cup \{0\}$ und ein $k_1 > k_0$ mit $\sigma^{k_0}(1) = \sigma^{k_1}(1)$ und k_1 minimal.
Wäre $k_0 > 0$, so wäre $\sigma^{k_0}(1)$ Bild von $\sigma^{k_0-1}(1)$ und von $\sigma^{k_1-1}(1)$ unter σ, und diese wären verschieden (k_1 war minimal), also wäre σ keine Bijektion.
Skizze dazu in der Vorlesung
Also ist $k_0 = 0$ und $\sigma^{k_1}(1) = 1$. Die Einschränkung von σ auf $\{1, \sigma(1), ..., \sigma^{k_1-1}(1)\}$ ist zyklisch.
Weil σ eine Bijektion ist, operiert σ bijektiv auf $\{1, ..., n\} - \{1, \sigma(1), ..., \sigma^{k_1-1}(1)\}$. Man wiederholt das Argument mit einem Element dieser Menge (z.B. mit dem kleinsten) anstelle von 1. Man wiederholt das Argument solange, bis man alle Elemente von $\{1, ..., n\}$ erfaßt hat. □

Lemma 1.14 *Sei $n \geq 2$. Zu jeder Permutation $\sigma \in S_n$ gibt es Transpositionen $\tau_1, ..., \tau_k$ (k geeignet) mit*

$$\sigma = \tau_1 \circ ... \circ \tau_k$$

(k und $\tau_1, ..., \tau_k$ sind nicht eindeutig bestimmt; die Träger der τ_j sind im allgemeinen nicht disjunkt).

Beweis: $\mathrm{id} = (12)(12)$.
Sei $\sigma \in S_n - \{\mathrm{id}\}$. Wegen Satz 1.12 können wir annehmen, daß σ zyklisch ist, $\sigma = (a_1 ... a_l)$. Dann ist

$$\sigma = (a_1 a_l)(a_1 a_{l-1})...(a_1 a_3)(a_1 a_2).$$

Beispiel: $(1\ 4\ 5\ 2\ 3) = (1\ 3)(1\ 2)(1\ 5)(1\ 4)$. □

Definition/Beispiel 1.15 *a) (Definition) Sei $n \geq 2$, $\sigma \in S_n$.*
Ein Paar $(i, j) \in \{1, ..., n\} \times \{1, ..., n\}$ heißt Fehlstand von σ, falls $i < j$ und $\sigma(i) > \sigma(j)$ ist.
Das Signum von σ ist definiert als

$$\mathrm{sign}(\sigma) := (-1)^{|\{\textit{Fehlstände}\}|}.$$

Eine Permutation heißt gerade, falls $\mathrm{sign}(\sigma) = +1$ *ist, und ungerade, falls* $\mathrm{sign}(\sigma) = -1$ *ist.*
b) (Beispiel)

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \in S_4$$

hat 5 Fehlstände, also ist $\mathrm{sign}(\sigma) = (-1)^5 = -1$*:*

(i,j)	$(\sigma(i),\sigma(j))$	*Fehlstand*
(1,2)	(4,3)	*ja*
(1,3)	(4,1)	*ja*
(1,4)	(4,2)	*ja*
(2,3)	(3,1)	*ja*
(2,4)	(3,2)	*ja*
(3,4)	(1,2)	*nein*

c) Warnung: Diese Definition ist gut, um Aussagen über das Signum zu beweisen. Zum Ausrechnen in Beispielen sollte man aber nie die Fehlstände bestimmen, sondern immer Eigenschaften in Satz 1.16 benutzen.

Satz 1.16 *Sei $n \geq 2$. Es gilt:*

(i) $\text{sign}(\text{id}) = 1$.

(ii) $\text{sign}(\widetilde{\sigma} \circ \sigma) = \text{sign}(\widetilde{\sigma}) \cdot \text{sign}(\sigma)$ *für* $\widetilde{\sigma}, \sigma \in S_n$.

(iii) Falls τ eine Transposition ist, ist $\text{sign}(\tau) = -1$.

(iv) Falls $\tau_1, ..., \tau_k$ Transpositionen sind, ist $\text{sign}(\tau_1 \circ ... \circ \tau_k) = (-1)^k$.

(v) Ein Zykel $(a_1...a_l)$ erfüllt $\text{sign}((a_1...a_l)) = (-1)^{l-1}$.

(vi) $k - l$ ist gerade bei

$$\tau_1 \circ ... \circ \tau_k = \widetilde{\tau}_1 \circ ... \circ \widetilde{\tau}_l \quad \textit{mit } \tau_i, \widetilde{\tau}_j \textit{ Transpositionen.}$$

Beweis: (i) gilt, denn id hat keine Fehlstände.
(iv) folgt aus (ii) und (iii).
(v) folgt aus (iv) und $(a_1...a_l) = (a_1a_l)(a_1a_{l-1})...(a_1a_3)(a_1a_2)$.
(vi) folgt aus (iv).
Der Beweis von (ii) und (iii) ergibt sich aus den folgenden zwei Definitionen und zwei Behauptungen. 1. Definition:

$$\text{Fehlst}(\sigma) := \{(i,j) \mid (i,j) \text{ ist ein Fehlstand von } \sigma\}.$$

2. Definition: Eine Transposition heißt *Nachbartransposition*, falls sie eine der Transpositionen $(12), (23), ..., (n-1\,n)$ ist.

1. Behauptung: Jede Permutation läßt sich als Produkt von Nachbartranspositionen schreiben. Eine Transposition ist Produkt einer ungeraden Anzahl von Nachbartranspositionen.

2. Behauptung: Ist $\sigma \in S_n$ beliebig und $\tau \in S_n$ eine Nachbartransposition, so ist $|Fehlst(\tau \circ \sigma)| = |\,\text{Fehlst}(\sigma)| \pm 1$. Insbesondere ist $|Fehlst(\tau)| = 1$. Daher ist $\text{sign}(\tau \circ \sigma) = (-1) \cdot \text{sign}(\sigma) = \text{sign}(\tau) \cdot \text{sign}(\sigma)$.

Nach der zweiten Behauptung ist $\text{sign}(\tau_1 \circ ... \circ \tau_k) = (-1)^k$, falls $\tau_1, ..., \tau_k$ Nachbartranspositionen sind. Zusammen mit der 1. Behauptung, erster Teil, gibt das $\text{sign}(\widetilde{\sigma} \circ \sigma) = \text{sign}(\widetilde{\sigma}) \cdot \text{sign}(\sigma)$ für beliebige Permutationen $\widetilde{\sigma}$ und σ. Der zweite Teil der 1. Behauptung zeigt $\text{sign}(\tau) = -1$ für beliebige Transpositionen.

Beweis der 1. Behauptung: Wegen Lemma 1.14 reicht es, eine Transposition (ij) als Produkt von Nachbartranspositionen zu schreiben. Sei $1 \leq i < j \leq n$.

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

Beispiel: $(1\ 5) = (1\ 2)(2\ 3)(3\ 4)(4\ 5)(3\ 4)(2\ 3)(1\ 2)$.
Die Anzahl rechts ist $2(j-i-1)+1$, also ungerade.

Beweis der 2. Behauptung: Sei $\tau = (i\,i+1)$ und $\sigma(a) = i, \sigma(b) = i+1$. Ist $a < b$, so ist $(a\,b) \notin \text{Fehlst}(\sigma)$ und $\text{Fehlst}(\tau \circ \sigma) = \text{Fehlst}(\sigma) \cup \{(a\,b)\}$. Ist $a > b$, so ist $(a\,b) \in \text{Fehlst}(\sigma)$ und $\text{Fehlst}(\tau \circ \sigma) = \text{Fehlst}(\sigma) - \{(a\,b)\}$.
Skizze in der Vorlesung □

Definition 1.17 Sei $(G, \cdot)$ eine Gruppe und $U \subset G$ eine nichtleere Teilmenge. U heißt Untergruppe von G, falls gilt:

$$\begin{aligned} a, b \in U &\Rightarrow a \cdot b \in U, \\ a \in U &\Rightarrow a^{-1} \in U. \end{aligned}$$

Bemerkung 1.18 Dann ist $e \in U$ wegen $a \cdot a^{-1} = e$, und U ist eine Gruppe.

Beispiele 1.19 i) Für jedes $m \in \mathbb{N}$ sei

$$m\mathbb{Z} := \{mk \mid k \in \mathbb{Z}\} = \{ \text{ die durch } m \text{ teilbaren ganzen Zahlen}\}.$$

Folgende Inklusionen geben Untergruppen:

$$(\{0\}, +) \subset (m\mathbb{Z}, +) \subset (\mathbb{Z}, +) \subset (\mathbb{Q}, +) \subset (\mathbb{R}, +).$$

ii) Ebenso die Inklusionen

$$\begin{aligned} (\{1\}, \cdot) \quad &\subset \quad (\mathbb{Q}^+, \cdot) \subset (\mathbb{Q} - \{0\}, \cdot) \subset (\mathbb{R} - \{0\}, \cdot) \\ \text{und} \quad &\quad (\mathbb{Q}^+, \cdot) \subset (\mathbb{R}^+, \cdot) \subset (\mathbb{R} - \{0\}, \cdot). \end{aligned}$$

iii) Die Gruppe $S_3 = \{\text{id}, (123), (132), (12), (13), (23)\}$ hat 6 Untergruppen:

$$\begin{aligned} &S_3, \\ &A_3 := \{\text{id}, (123), (132)\}, \\ &Z_1 := \{\text{id}, (12)\}, \quad Z_2 := \{\text{id}, (13)\}, \quad Z_3 := \{\text{id}, (23)\}, \\ &\{\text{id}\}. \end{aligned}$$

Definition 1.20 Es seien $(G, \cdot)$ und $(H, \cdot)$ Gruppen.
Eine Abbildung $f : G \to H$ heißt *Gruppenhomomorphismus* (oder einfach *Homomorphismus*), falls

$$f(a \cdot b) = f(a) \cdot f(b) \quad \text{für alle } a, b \in G \text{ gilt.}$$

Falls f darüber hinaus auch bijektiv ist, so heißt f ein *Gruppenisomorphismus*. Dann sind G und H *isomorphe Gruppen*.
Notation: $G \cong H$, "G isomorph H".

Beispiele 1.21 i) Die Abbildung sign : $S_n \to \{1, -1\}$, $\sigma \mapsto \text{sign}(\sigma)$, ist ein Gruppenhomomorphismus von S_n in die Gruppe $(\{1, -1\}, \cdot)$, wegen Satz 1.16: $\text{sign}(\widetilde{\sigma} \circ \sigma) = \text{sign}(\widetilde{\sigma}) \cdot \text{sign}(\sigma)$.
ii) Ist U eine Untergruppe einer Gruppe G, so ist die kanonische Inklusion $U \to G$ ein injektiver Gruppenhomomorphismus.
iii) Die Abbildung

$$\exp : \mathbb{R} \to \mathbb{R}^+, \quad x \mapsto e^x,$$

ist ein Isomorphismus von $(\mathbb{R}, +)$ nach $(\mathbb{R}^+, \cdot)$, denn $e^{x+y} = e^x \cdot e^y$.
iv) Die Gruppe S_3 ist isomorph zur Symmetriegruppe eines gleichseitigen Dreiecks: Die Ecken werden mit 1,2,3 bezeichnet, der Mittelpunkt mit 0.
Skizze in der Vorlesung.

S_3	$\to$	Symmetriegruppe des gleichseitigen Dreiecks
id	$\mapsto$	id
(123)	$\mapsto$	Drehung um $\frac{2\pi}{3}$ mit Fixpunkt 0
(132)	$\mapsto$	Drehung um $\frac{4\pi}{3}$ mit Fixpunkt 0
(12)	$\mapsto$	Spiegelung an der Geraden durch 3 und 0
(13)	$\mapsto$	Spiegelung an der Geraden durch 2 und 0
(23)	$\mapsto$	Spiegelung an der Geraden durch 1 und 0

v) Zahlreiche Gruppen kann man so interpretieren, als Symmetriegruppen von geometrischen Objekten, oder allgemeiner als Gruppen von Selbstabbildungen (*"Automorphismen"*) von Objekten mit Struktur.

Lemma 1.22 *Sei $f : G \to H$ ein Gruppenhomomorphismus von Gruppen $(G, \cdot)$ und $(H, \cdot)$.*
Dann ist $f(e_G) = e_H$ und $f(a^{-1}) = f(a)^{-1}$ für $a \in G$.
Ist $U \subset G$ eine Untergruppe von G, so ist $f(U) \subset H$ eine Untergruppe von H. Insbesondere ist $f(G)$ eine Untergruppe von H.
Ist $V \subset H$ eine Untergruppe von H, so ist $f^{-1}(V) \subset G$ eine Untergruppe von G. Insbesondere ist die Menge

$$\ker(f) := \{a \in G \mid f(a) = e_H\} = f^{-1}(e_H)$$

eine Untergruppe von G (es gilt mehr: sie ist ein Normalteiler).
Ist $f : G \to H$ ein Isomorphismus von Gruppen, so ist auch $f^{-1} : H \to G$ ein Isomorphismus von Gruppen.

Beweis: Die Rechnung $f(e_G) \cdot f(e_G) = f(e_G \cdot e_G) = f(e_G) = f(e_G) \cdot e_H$ und die Kürzungsregel (Lemma 1.3) zeigen $f(e_G) = e_H$.
Aus $f(a^{-1}) \cdot f(a) = f(a^{-1} \cdot a) = f(e_G) = e_H$ und analog $f(a) \cdot f(a^{-1}) = e_H$ folgt $f(a^{-1}) = f(a)^{-1}$.
$f(U)$ Untergruppe von H: zu zeigen ist, daß $f(U)$ abgeschlossen ist unter dem Produkt und der Inversen-Bildung. Das ist es wegen $f(a)^{-1} = f(a^{-1})$ und wegen $f(a) \cdot f(b) = f(a \cdot b)$
$f^{-1}(V)$ Untergruppe von G: zu zeigen ist, daß $f^{-1}(V)$ abgeschlossen unter dem Produkt und der Inversen-Bildung. Das ist es wegen

$$\begin{aligned} f(a) \in V, \quad f(b) \in V &\Rightarrow f(ab) = f(a)f(b) \in V, \\ f(a) \in V &\Rightarrow f(a^{-1}) = f(a)^{-1} \in V. \end{aligned}$$

f Isomorphismus $\Rightarrow f^{-1}$ Isomorphismus: sei $f(a) = c, f(b) = d$, also $f^{-1}(c) = a, f^{-1}(d) = b$; es ist

$$f^{-1}(c)f^{-1}(d) = ab = f^{-1}(f(ab)) = f^{-1}(f(a)f(b)) = f^{-1}(cd).$$

□

Beispiel 1.23 Sei $n \geq 2$. Die Teilmenge A_n von S_n,

$$\begin{aligned} A_n &:= \ker(\text{sign} : S_n \to \{1, -1\}) \\ &= \{\sigma \in S_n \mid \text{sign}(\sigma) = 1\} = \{\text{die geraden Permutationen}\}, \end{aligned}$$

ist eine Untergruppe von S_n.
Die Gruppen A_n für $n \geq 2$ heißen *alternierende Gruppen.*

$$S_n = A_n \ \cup \ \{\text{die ungeraden Permutationen}\};$$

die Abbildung $A_n \to \{\text{die ungeraden Permutationen}\}$, $a \mapsto (12)a$, ist eine Bijektion; also ist $|A_n| = \frac{n!}{2}$.

Satz 1.24 *a) Die einzigen Untergruppen von $(\mathbb{Z}, +)$ sind die Untergruppen $m\mathbb{Z}$ für $m \in \mathbb{N}_0$ von Beispiel 1.19 (i).*
b) Division mit Rest in $\mathbb{Z}$: Zu $a \in \mathbb{Z}$ und $b \in \mathbb{N}$ gibt es eindeutige $q \in \mathbb{Z}$ und $r \in \{0, 1, ..., b-1\}$ mit

$$a = qb + r.$$

Beweis: b) bekannt oder klar.
a) Ist $U = \{0\}$, so ist $U = m\mathbb{Z}$ für $m := 0$. Sei nun $U \subset \mathbb{Z}$ eine Untergruppe von $(\mathbb{Z}, +)$ mit $U \neq \{0\}$. Sei $m := \min(a \in U \mid a > 0)$. Aus b) folgt mit $b = m$: zu einem $a \in U$ gibt es eindeutige $q \in \mathbb{Z}$ und $r \in \{0, 1, ..., m-1\}$ mit $a = qm + r$. Es ist $qm = m + ... + m \in U$ und $a \in U$, also auch $r = a - qm \in U$. Aus $0 \leq r < m$ und der Definition von m folgt $r = 0$. Also ist $a = qm \in m\mathbb{Z}$ und $U = m\mathbb{Z}$. □

Definition 1.25 a) Eine Relation auf einer Menge X ist eine Teilmenge R von $X \times X$. Zwei Elemente $a, b \in X$ *erfüllen die Relation* oder *stehen in der Relation*, wenn $(a, b) \in R$ gilt. Notation: aRb.

b) Beispiele für Relationen auf $X = \mathbb{Z}$: $=, \leq, \geq, <, >, \neq$;
Beispiele für Relationen auf der Potenzmenge einer Menge: $\subset, \supset, =, \neq$.

c) Eine Relation ist eine *Äquivalenzrelation*, falls sie erfüllt:
Reflexivität: xRx für $x \in X$,
Symmetrie: $xRy \Longrightarrow yRx$ für $x, y \in X$,
Transitivität: (xRy und yRz) $\Longrightarrow xRz$ für $x, y, z \in X$.
Notation: Bei einer Äquivalenzrelation wird statt R meistens $\sim$ geschrieben.

d) Sei $\sim$ eine Äquivalenzrelation auf einer Menge X . Die *Äquivalenzklasse* von $x \in X$ ist die Teilmenge

$$[x] := \{y \in X \mid y \sim x\} \subset X.$$

Triviales Lemma: $[x] = [y]$, falls $x \sim y$, sonst $[x] \cap [y] = \emptyset$.
X ist die disjunkte Vereinigung der Äquivalenzklassen in X.
Die Menge aller Äquivalenzklassen in X wird mit $X/\sim$ bezeichnet.
Ist $U \subset X$ eine Äquivalenzklasse und $x \in U$, so ist $U = [x]$, und x ist ein *Repräsentant* von U.

Definition/Lemma 1.26 *Sei $m \in \mathbb{N}$.*
a) (Definition) Auf $\mathbb{Z}$ wird eine Relation $\sim$ definiert durch

$$a \sim b \iff a - b \in m\mathbb{Z}.$$

b) (Lemma) Es ist eine Äquivalenzrelation. Eine Äquivalenzklasse ist

$$[a] = \{a + km \mid k \in \mathbb{Z}\} \subset \mathbb{Z}.$$

Die Menge der Äquivalenzklassen ist

$$\mathbb{Z}/\sim = \{[0], [1], ..., [m-1]\}.$$

c) Notationen : Diese Menge wird auch mit $\mathbb{Z}/m\mathbb{Z}$ bezeichnet. Die Äquivalenzklassen heißen hier auch Kongruenzklassen. Und

$$\begin{aligned} a - b \in m\mathbb{Z} &\iff a \equiv b \mod m \\ &\iff \text{“}a \text{ ist kongruent zu } b \text{ modulo } m\text{”}. \end{aligned}$$

d) (Lemma) Auf $\mathbb{Z}/m\mathbb{Z}$ ist die Verknüpfung $+$ mit

$$[a] + [b] := [a + b]$$

wohldefiniert, und damit wird $\mathbb{Z}/m\mathbb{Z}$ eine abelsche Gruppe mit m Elementen.

e) (Beispiel) $m = 3$,

$$\begin{aligned} ... = [-3] = [0] = [3] = [6] = ..., \\ ... = [-4] = [-1] = [2] = [5] = ..., \\ ... = [-5] = [-2] = [1] = [4] = ..., \\ [1013528] = [\text{Quersumme}] = [20] = [2], \\ [1+2] = [3] = [0]. \end{aligned}$$

f) Die Abbildung

$$f : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, \quad a \mapsto [a]$$

ist ein surjektiver Gruppenhomomorphismus mit $\ker f = m\mathbb{Z}$.

Beweis: b) ok. d) Für die Wohldefiniertheit ist zu zeigen, daß die Definition von + von der Wahl der Repräsentanten unabhängig ist:
Ist bei $[a] = [\tilde{a}]$ und $[b] = [\tilde{b}]$ auch $[a+b] = [\tilde{a}+\tilde{b}]$?
Ja, denn die Differenz $a + b - \tilde{a} - \tilde{b} = (a - \tilde{a}) + (b - \tilde{b})$ ist in $m\mathbb{Z}$.
Der Rest (Assoziativität, Existenz des neutralen Elements und Existenz von inversen Elementen) folgt aus den analogen Eigenschaften der Verknüpfung + in $\mathbb{Z}$.
f) Surjektiv: ok. Gruppenhomomorphismus? Ja, wegen $[a] + [b] = [a + b]$.
$\ker f = [0] = m\mathbb{Z}$ ok. □

Definition/Lemma 1.27 *a) (Definition) Eine Gruppe* $(G, \cdot)$ *heißt zyklische Gruppe, falls ein* $a \in G$ *existiert mit*

$$G = \{e, a, a^2, a^3, ..., a^{-1}, a^{-2}, a^{-3}, ...\}.$$

Dann heißt a *ein erzeugendes Element dieser Gruppe.*
b) (Lemma) Sei G *zyklisch mit Erzeugendem* a.
Im Fall $|G| = \infty$ *ist*

$$(\mathbb{Z}, +) \to (G, \cdot), \quad k \mapsto a^k \quad \text{ein Gruppenisomorphismus.}$$

Im Fall $|G| = m \in \mathbb{N}$ *ist* $m = \min(l \in \mathbb{N} \mid a^l = e)$, *und*

$$(\mathbb{Z}/m\mathbb{Z}, +) \to (G, \cdot), \quad [k] \mapsto a^k \quad \text{ist ein Gruppenisomorphismus.}$$

c) (Lemma) Ist $(G, \cdot)$ *eine Gruppe und* $a \in G$, *so ist*

$$\langle a \rangle := \{e, a, a^2, a^3, ..., a^{-1}, a^{-2}, a^{-3}, ...\} \subset G$$

eine zyklische Untergruppe.
(Definition) Sie heißt die von a *erzeugte Untergruppe. Die Ordnung von* a *ist*

$$o(a) := |\langle a \rangle| \overset{!}{=} \begin{cases} \min(l \in \mathbb{N} \mid a^l = e) \text{ falls so ein } l \text{ existiert,} \\ \infty \qquad \text{sonst.} \end{cases}$$

Beweis: b) Fall $|G| = \infty$: Die Abbildung $\mathbb{Z} \to G$ ist surjektiv: ok. Sie ist ein Gruppenhomomorphismus: ok. Sie ist injektiv: Sonst wäre $a^m = e$ und $a^{-m} = e$ für ein $m \in \mathbb{N}$; dann wäre $G = \{e, a, a^2, ..., a^{m-1}\}$ und $|G| \leq m < \infty$, ein Widerspruch.
Fall $|G| < \infty$: Sei $\widetilde{m} := \min(l \in \mathbb{N} \mid a^l = e)$. Dann ist $G = \{e, a, a^2, ..., a^{\widetilde{m}-1}\}$, $|G| = \widetilde{m}$, also $\widetilde{m} = m$. Der Rest ist klar.
c) Klar. □

Satz 1.28 *Sei G ein endliche zyklische Gruppe mit $|G| = m \in \mathbb{N}$, $G = \{e, a, a^2, ..., a^{m-1}\}$. Zu jedem Teiler $n \in \mathbb{N}$ von m existiert genau eine Untergruppe U von G der Ordnung $\frac{m}{n}$; sie ist*

$$U = \{e, a^n, a^{2n}, ..., a^{m-n}\}.$$

Das sind alle Untergruppen von G.

Beweis: OBdA $(G, \cdot) = (\mathbb{Z}/m\mathbb{Z}, +),\ a = [1]$.
Natürlich ist für jeden Teiler $n \in \mathbb{N}$ von m die Menge $\{[0], [n], [2n], ..., [m-n]\}$ eine Untergruppe der Ordnung $\frac{m}{n}$.
Zu zeigen bleibt, daß es keine anderen Untergruppen gibt. Sei $U \subset \mathbb{Z}/m\mathbb{Z}$ irgendeine Untergruppe. Betrachte den Gruppenhomomorphismus $f : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z},\ a \mapsto [a]$. Nach Lemma 1.22 ist $f^{-1}(U) \subset \mathbb{Z}$ eine Untergruppe von $\mathbb{Z}$, nach Satz 1.24 a) ist $f^{-1}(U) = n\mathbb{Z}$ für ein eindeutiges $n \in \mathbb{N}$. Wegen

$$n\mathbb{Z} = f^{-1}(U) \supset f^{-1}(0) = m\mathbb{Z}$$

gilt $n \mid m$. Nun ist

$$U = f(f^{-1}(U) = f(n\mathbb{Z}) = \{[0], [n], [2n], ..., [m-n]\} \subset \mathbb{Z}/m\mathbb{Z}.$$

□

Bemerkungen 1.29 i) Definition/Lemma 1.27 c) gibt eine Übersicht über alle zyklischen Gruppen bis auf Isomorphie. Satz 1.24 a) und Satz 1.28 geben eine Übersicht über ihre Untergruppen. Insbesondere ist jede Untergruppe einer zyklischen Gruppe zyklisch.
ii) Bei anderen Gruppen, auch endlichen, ist es viel schwieriger, eine Übersicht über ihre Untergruppen zu erhalten.
iii) Satz 1.28 sagt unter anderem: G zyklisch mit $|G| < \infty$ und $U \subset G$ Untergruppe $\Longrightarrow |U|$ teilt $|G|$. Diese Eigenschaft von Untergruppen U gilt tatsächlich für beliebige endliche Gruppen G. Satz 1.31 wird das auf beliebige endliche Gruppen verallgemeinern.
iv) Man kann $\mathbb{Z}/m\mathbb{Z}$ als Quotientengruppe von $\mathbb{Z}$ nach $m\mathbb{Z}$ auffassen. Satz 1.36 verallgemeinert das zu G/U mit U *Normalteiler* (Definition 1.34).

Definition 1.30 Sei G eine Gruppe.
a) Sei $a \in G$. Die Abbildung $l_a : G \to G,\ b \mapsto ab$ ist die Linksmultiplikation mit a. Die Abbildung $r_a : G \to G,\ b \mapsto ba$, ist die Rechtsmultiplikation mit a.
b) Sei $U \subset G$ eine Untergruppe. Die Mengen $l_a(U) =: aU$ für $a \in G$ heißen *Linksnebenklassen von* U. Die Mengen $r_a(U) =: Ua$ sind die *Rechtsnebenklassen von* U.
G/U bezeichnet die Menge $\{aU \mid a \in G\}$, die Menge der Linksnebenklassen von U. (Analog bezeichnet $U\backslash G$ die Menge der Rechtsnebenklassen; aber das wird weniger gebraucht.)
c) Ist $(G, +)$ eine abelsche Gruppe mit additiv geschriebener Verknüpfung, so stimmen die Links- und Rechtsnebenklassen paarweise überein; sie werden mit $a + U := \{a + u \mid u \in U\}$ bezeichnet, manchmal (wenn klar ist, welche Untergruppe U gemeint ist) auch mit $[a]$.

Satz 1.31 *Sei G eine Gruppe.*
a) Für jedes $a \in G$ sind die Abbildungen l_a und r_a bijektiv.
b) Sei U eine Untergruppe. Die Relation $\sim_l$ mit

$$a \sim_l b \iff \text{es existiert ein } u \in U \text{ mit } au = b$$

ist eine Äquivalenzrelation. Ihre Äquivalenzklassen sind genau die Linksnebenklassen aU mit $a \in G$. Daher ist G die disjunkte Vereinigung der Linksnebenklassen von U, und $G/U = G/\sim_l$.
c) (Satz von Lagrange) Sei die Gruppe G endlich und U eine Untergruppe. Dann sind auch U und G/U endlich, und es ist

$$|G| = |U| \cdot |G/U|.$$

Also teilt die Ordnung $|U|$ von U die Ordnung $|G|$ von G.
d) Sei G endlich und $a \in G$. Die Ordnung von a teilt $|G|$.

Beweis: a) l_a ist injektiv: $ab = ac \Rightarrow b = c$ (Kürzungsregel, Lemma 1.3).
l_a ist surjektiv: die Gleichung $a \cdot x = b$, wo x gesucht ist, hat die Lösung $x = a^{-1}b$.
Analog für r_a.
b) $a \sim_l a$: ok.
$a \sim_l b \iff b \sim_l a$: $au = b \iff bu^{-1} = a$.
$a \sim_l b$ und $b \sim_l c \Longrightarrow a \sim_l c$: $au_1 = b$ und $bu_2 = c \Longrightarrow a(u_1u_2) = c$.
Daher ist $\sim_l$ eine Äquivalenzrelation. Der Rest folgt mit Definition 1.25 d).
c) G ist die Vereinigungsmenge der nach b) paarweise disjunkten Linksnebenklassen. Daher ist die Menge G/U endlich, und es gibt geeignete $a_2, ..., a_{|G/U|} \in G$ mit

$$G/U = \{U, a_2U, ..., a_{|G/U|}U\}.$$

$l_{a_j} : U \to a_j U$ ist bijektiv. Daher ist $|G| = |U| \cdot |G/U|$.
Skizze in der Vorlesung
d) $\langle a \rangle \subset G$ ist eine endliche Untergruppe, und $o(a) = |\langle a \rangle|$ (1.27 c)) teilt $|G|$ wegen c). □

Beispiele 1.32 i) Die Ordnung einer zyklischen Permutation $(a_1...a_k) \in S_n$ ist k. Die Ordnung einer beliebigen Permutation ist das kgV der Ordnungen der zyklischen Permutationen mit disjunkten Trägern, deren Produkt die Permutation ist (Satz 1.12).
ii) $S_n = A_n \cup (12)A_n, \quad |A_n| = \frac{n!}{2}$.
iii) Die Ordnungen der Untergruppen der S_3 sind 1,2,3,6 (Beispiel 1.19 iii)).
iv) Die Ordnungen der Untergruppen der S_4 sind Teiler von $|S_4| = 4! = 24$, also höchstens $24, 12, 8, 6, 4, 3, 2, 1$. Tatsc̈hlich (ohne Beweis) treten sie alle auf.

Notation 1.33 Sei $(G, \cdot)$ eine Gruppe. Es seien $c_1, c_2, c_3, ... \in G$ und $A_1, A_2, A_3, ... \subset G$.

$$c_1 A_1 := \{c_1 a_1 \mid a_1 \in A_1\} = \{c_1\} A_1, \quad A_1 c_1 := \{a_1 c_1 \mid a_1 \in A_1\} = A_1 \{c_1\},$$

und analog z.B. $c_1 A_1 A_2 c_2 c_3 A_3 := \{c_1 a_1 a_2 c_2 c_3 a_3 \mid a_1 \in A_1, a_2 \in A_2, a_3 \in A_3\}$.

Lemma/Definition 1.34 *Sei U eine Untergruppe einer Gruppe G.*
a) (Lemma) Für jedes $a \in G$ ist aUa^{-1} eine Untergruppe von G.
(Definition) Diese Untergruppen heißen die zu U konjugierten Untergruppen.
b) (Definition) U ist ein Normalteiler von G genau dann, wenn $U = aUa^{-1}$ für alle $a \in G$ ist.
c) (Lemma) U ist ein Normalteiler von G genau dann, wenn $aU = Ua$ für alle $a \in G$ ist; d.h. wenn Links- und Rechtsnebenklassen übereinstimmen.

Beweis: a) Man muß prüfen, daß aUa^{-1} abgeschlossen unter Produkt und Inversen-Bildung ist:
$au_1a^{-1}, au_2a^{-1} \in aUa^{-1} \Rightarrow (au_1a^{-1})(au_2a^{-1}) = au_1u_2a^{-1} \in aUa^{-1}$;
$aua^{-1} \in aUa^{-1} \Rightarrow (aua^{-1})^{-1} = au^{-1}a^{-1} \in aUa^{-1}$.
b) o.k.
c) Man multipliziere $U = aUa^{-1}$ von rechts mit a
bzw $aU = Ua$ von rechts mit a^{-1}. □

Beispiele 1.35 i) Ist G abelsch, so ist jede Untergruppe von G ein Normalteiler von G.
ii) Ist $f : G \to H$ ein Gruppenhomomorphismus, so ist $U := \ker(f)$ ein Normalteiler von G.
Beweis: $f(aUa^{-1}) = f(a)\{e_H\}f(a^{-1}) = \{e_H\}$, also $aUa^{-1} \subset U$. Für a^{-1} statt a gibt das $a^{-1}Ua \subset U$, also $U \subset aUa^{-1}$. Also ist $aUa^{-1} = U$. □

iii) Die Untergruppen $Z_1, Z_2, Z_3 \subset S_3$ von Beispiel 1.19 iii) sind konjugiert zueinander; sie sind daher keine Normalteiler. Die Untergruppe $A_3 \subset S_3$ ist ein Normalteiler von S_3.

Satz 1.36 *Sei U ein Normalteiler einer Gruppe G. Für $a \in G$ sei $[a] := aU$ die (Links)Nebenklasse von a.*
Die Verknüpfung $\cdot$ auf G/U mit

$$[a] \cdot [b] := [a \cdot b]$$

ist wohldefiniert. $(G/U, \cdot)$ ist eine Gruppe, die Quotientengruppe von G nach U.
Die Abbildung $G \to G/U,\ a \mapsto aU$ ist ein surjektiver Gruppenhomomophismus. Der Kern ist U.

Beweis: Für die Wohldefiniertheit von $\cdot$ auf G/U muß man zeigen, daß $[ab]$ nur von den Nebenklassen $[a]$ und $[b]$ abhängt (und nicht von der Wahl der Repräsentanten a und b). Das ist ein Teil der

Behauptung: $[ab] = [a][b]$ im Sinne von 1.33, also $abU = aUbU$.

Beweis: Zuerst wird $UU = U$ festgestellt: $UU \subset U$ nach Definition einer Untergruppe (Definition 1.17); $UU \supset eU = U$ wegen $U \supset \{e\}$. Nun folgt auch die Behauptung:

$$[a][b] = aUbU \overset{U\text{Normalteiler}}{=} aUUb = aUb \overset{U\text{Normalteiler}}{=} abU$$

Mit dieser Verknp̈fung "erbt" G/U die Gruppeneigenschaften von G, z.B. Assoziativität:

$$([a] \cdot [b]) \cdot [c] = [ab] \cdot [c] = [(ab)c] = [a(bc)] = [a] \cdot [bc] = [a] \cdot ([b] \cdot [c]),$$

analog neutrales Element $[e]$ und Inverse $[a]^{-1} = [a^{-1}]$.
Natürlich ist die Abbildung $G \to G/U$ surjektiv. Sie ist ein Gruppenhomomorphismus gerade wegen $[a] \cdot [b] = [a \cdot b]$. □

Satz 1.37 *Sei $f : G \to H$ ein Gruppenhomomorphismus. Weil $\ker(f)$ ein Normalteiler ist (Beispiel 1.35 ii)), ist $G/\ker(f)$ eine Gruppe (Satz 1.36). Auch $f(G)$ ist eine Gruppe (Lemma 1.22).*
Die Vorschrift $a \ker(f) \mapsto f(a)$ definiert eine Abbildung

$$\widetilde{f} : G/\ker(f) \to f(G).$$

$\widetilde{f}$ ist ein Gruppenisomorphismus.

Beweis: 1) $\widetilde{f}$ ist „wohldefiniert“: zu zeigen ist

$$a\ker(f) = b\ker(f) \Rightarrow f(a) = f(b).$$

Das gilt, denn falls $a\ker(f) = b\ker(f)$ gilt, existiert ein $u \in \ker(f)$ mit $a = bu$. Dann ist $f(a) = f(bu) = f(b)f(u) = f(b)e_H = f(b)$.
2) $\widetilde{f}$ ist surjektiv: klar.
3) $\widetilde{f}$ ist injektiv: sei $\widetilde{f}(a_1\ker(f)) = \widetilde{f}(a_2\ker(f))$. Dann ist $f(a_1) = f(a_2)$; also $f(a_2^{-1}a_1) = f(a_2)^{-1}f(a_1) = e_H$; also $a_2^{-1}a_1 \in \ker(f)$; also $a_1 = a_2(a_2^{-1}a_1) \in a_2\ker(f)$; also ist $a_1\ker(f) = a_2\ker(f)$.
4) $\widetilde{f}$ ist ein Gruppenhomomorphismus:

$$\widetilde{f}\left((a\ker(f)) \cdot (b\ker(f))\right) \overset{\text{Satz 1.36}}{=} \widetilde{f}(ab\ker(f)) \overset{\text{Def. von } \widetilde{f}}{=} f(ab)$$
$$\overset{f \text{ Gruppenhom.}}{=} f(a)f(b) \overset{\text{Def. von } \widetilde{f}}{=} \widetilde{f}(a\ker(f)) \cdot \widetilde{f}(b\ker(f)).$$

□

Bemerkungen 1.38 Aus Satz 1.36 und Satz 1.37 folgt sofort:
Ist $f\colon G \to H$ ein Gruppenhomomorphismus zwischen endlichen Gruppen G und H, so gilt:

$$|G| = |\ker(f)| \cdot |f(G)|.$$

2 Ringe und Körper

Definition 2.1 a) Ein *Ring* ist eine Menge R zusammen mit zwei Verknüpfungen, einer Addition $+ : R \times R \to R$ und einer Multiplikation $\cdot : R \times R \to R$ mit folgenden Eigenschaften:

i) $(R, +)$ ist eine abelsche Gruppe; ihr neutrales Element wird als *Nullelement* oder *Null* bezeichnet und als 0 geschrieben.

ii) Die Multiplikation ist assoziativ: $(ab)c = a(bc)$ für $a, b, c \in R$.

iii) Es gelten die *Distributivgesetze:*

$$a(b + c) = ab + ac \quad \text{und} \quad (a + b)c = ac + bc \quad \text{für} \quad a, b, c \in R.$$

b) Falls ein Element $1_R \in R$ mit $1_R \cdot a = a \cdot 1_R = a$ für alle $a \in R$ existiert, so heißt es *Einselement* oder *Eins*; es wird oft einfach als 1 geschrieben.

c) Ein Ring heißt *kommutativ*, falls die Multiplikation kommutativ ist, $ab = ba$ für $a, b \in \mathbb{R}$.

d) Ein *Körper* $(K, +, \cdot)$ ist ein Ring, bei dem $K - \{0\} \neq \emptyset$ ist und $(K - \{0\}, \cdot)$ eine abelsche Gruppe ist.

Bemerkungen 2.2 i) Ein Ring ist genaugenommen ein Tripel $(R, +, \cdot)$, aber wie bei Gruppen werden wir vom Ring R sprechen, von Elementen und von Teilmengen des Ringes R. Die Menge R wird als primäres Objekt angesehen, die Verknüpfungen darauf als sekundär. Analog bei Körpern.
ii)

$$\{\text{Körper}\} \subset \{\text{kommutative Ringe mit 1}\} \begin{array}{l} \subset \{\text{komm. Ringe}\} \subset \\ \subset \{\text{Ringe mit 1}\} \subset \end{array} \{\text{Ringe}\}.$$

iii) Die 1 in einem Ring mit Eins ist eindeutig wegen $1 = 1 \cdot 1' = 1'$.

Beispiele 2.3 a) $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind Körper, ebenso $(\mathbb{Q}[\sqrt{2}], +, \cdot)$ (Übung 4, Blatt 5: $(\mathbb{Q}[\sqrt{2}] - \{0\}, \cdot)$ ist eine abelsche Gruppe).

b) $(\mathbb{C}, +, \cdot)$ ist ein Körper: Satz/Definition 2.20 (vgl. auch Analysis I, Schmidt).

c) $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit 1, aber kein Körper.

d) Für $m \in \mathbb{N},\ m \geq 2$, ist $(m\mathbb{Z}, +, \cdot)$ ein kommutativer Ring ohne 1.

e) Satz 2.17: für $m \in \mathbb{N}$ ist $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ein kommutativer Ring mit 1. Satz 2.19: es ist ein Körper genau dann, wenn m eine Primzahl ist.

f) Zu einem Ring R kann man den Polynomring $R[x]$ definieren. Die Addition und Multiplikation von Polynomen ist bekannt. Beide Verknüpfungen sind assoziativ, es gelten die Distributivgesetze, und die Addition ist kommutativ. Die Multiplikation von Polynomen ist genau dann kommutativ, wenn R ein kommutativer Ring ist.

Das Nullpolynom 0 ist das neutrale Element der Polynomaddition, und zu einem Polynom p ist $-p$ das additive Inverse. Somit ist $R[x]$ bzgl. der Addition eine abelsche Gruppe.

Das Polynom 1 ist ein neutrales Element bzgl. der Polynommultiplikation, und $R[x]$ ist damit ein Ring mit Eins.

$R[x]$ ist nie ein Körper, da das Polynom x kein multiplikatives Inverses haben kann.

g) Beispiele für nichtkommutative Ringe: später.

h) $(\{0,\}, +, \cdot)$ ist ein kommutativer Ring mit 1. Er ist der einzige mit $1 = 0$ (Lemma 2.4 b)).

i) Für eine Menge M sei $P(M) := \{\, A \mid A \subseteq M \,\}$ die Potenzmenge von M. Weiter sei für $A, B \in P(M)$ die symmetrische Differenz definiert durch:

$$A \ominus B := (A \cup B) - (A \cap B).$$

Dann ist $\big(P(M), \ominus, \cap\big)$ ein kommutativer Ring mit 1.

Lemma 2.4 *Sei R ein Ring.*

a) Für alle $a \in R$ ist $a \cdot 0 = 0 \cdot a = 0$.

b) Ist $R \neq \{0\}$ und hat R eine 1, so ist $1 \neq 0$.

c) $(-a) \cdot b = -(a \cdot b) = a \cdot (-b)$ für $a, b \in R$.

d) Ist R ein Körper und $a \cdot b = 0$ so ist $a = 0$ oder $b = 0$ (wichtig).

Beweis: a) $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$, also $0 = a \cdot 0$; analog $0 \cdot a = 0$.
b) Sei $a \in R - \{0\}$. Es ist $a \cdot 0 = 0 \neq a = a \cdot 1$, also $0 \neq 1$.
c) $a \cdot b + (-a) \cdot b = (a + (-a)) \cdot b = 0 \cdot b = 0$, also $(-a) \cdot b = -(a \cdot b)$; Rest analog.
d) Ist $a \neq 0$, so ist $b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0$.

□

Definition 2.5 Sei R ein Ring mit 1, und sei $a \in R - \{0\}$.
a) Das Element a heißt *Einheit* in R, wenn es ein $b \in R$ gibt mit $ab = ba = 1$.
b) Das Element a heißt *Nullteiler* in R, falls es ein Element $b \in R - \{0\}$ gibt mit $ab = 0$ oder $ba = 0$.

Lemma 2.6 *Sei R ein Ring mit Eins. Dann gilt für $a \in R$:*

$$\begin{aligned} a \text{ Nullteiler} &\quad \Rightarrow \quad a \text{ keine Einheit.} \\ a \text{ Einheit} &\quad \Rightarrow \quad a \text{ kein Nullteiler.} \end{aligned}$$

Beweis: Beide Aussagen sind äquivalent zueinander, so daß nur eine bewiesen werden muß.
Sei a eine Einheit, d.h. es gibt ein b mit $ab = ba = 1$. Wäre nun a ein Nullteiler mit $ca = 0$ für ein $c \neq 0$, so würde

$$c = c1 = cab = 0b = 0$$

folgen, im Widerspruch zur Wahl von c.
Analog würde aus der Gleichung $ac = 0$ mit $c \neq 0$ wieder ein Widerspruch zur Wahl von c folgen:

$$c = 1c = bac = b0 = 0.$$

Somit kann a kein Nullteiler sein. □

Bemerkungen 2.7 Man vergleiche die Aussage von Lemma 2.6 mit der Aussage von Lemma 2.4 d): Da in einem Körper alle Elemente ungleich 0 Einheiten sind, darf es dort außer der 0 keine Nullteiler geben.

Definition 2.8 a) Eine Teilmenge U eines Ringes R heißt *Unterring*, falls $(U, +)$ eine Untergruppe von $(R, +)$ ist und falls U bezüglich der Multiplikation abgeschlossen ist.
Ein Unterring I von R heißt *Ideal*, falls gilt:

$$x \in R, i \in I \quad \Rightarrow \quad xi \in I \text{ und } ix \in I.$$

b) Eine Teilmenge U eines Körpers K heißt *Unterkörper*, falls $(U, +)$ eine Untergruppe von $(K, +)$ ist und $(U - \{0\}, \cdot)$ eine Untergruppe von $(K - \{0\}, \cdot)$ ist.
c) Eine Abbildung $f : R \to S$ von einem Ring R in einen Ring S heißt *Ringhomomorphismus*, falls für $a, b \in R$ sowohl $f(a + b) = f(a) + f(b)$ als auch $f(a \cdot b) = f(a) \cdot f(b)$ gilt. Sie heißt *Ringisomorphismus*, falls sie darüber hinaus auch bijektiv ist.
d) Ist $f \colon R \to S$ ein Ringhomomorphismus, so ist sein *Kern* definiert durch:

$$\ker(f) := \{\, a \in R \mid f(a) = 0_S \,\}.$$

Bemerkungen 2.9 i) Einen Ringhomomorphismus $f : K \to L$ zwischen zwei Körpern K und L mit $f(K) \neq \{0\}$ nennt man auch *Körperhomomorphismus*. Analog *Körperisomorphismus*.
ii) Ein Unterring (Def. 2.8 a)) ist ein Ring.
iii) Ein Unterkörper (Def. 2.8 b)) ist ein Körper.
iv) Das Bild $f(R) \subset S$ eines Ringhomomorphismus $f : R \to S$ ist ein Unterring von S. Beweis: analog zu Satz 1.22.
v) $m\mathbb{Z}$ ist ein Unterring von $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}[\sqrt{2}]$ und $\mathbb{R}$;
$\mathbb{Z}$ ist ein Unterring von $\mathbb{Q}$, $\mathbb{Q}[\sqrt{2}]$ und $\mathbb{R}$;
$\mathbb{Q}$ ist ein Unterkörper von $\mathbb{Q}[\sqrt{2}]$ und $\mathbb{R}$;
$\mathbb{Q}[\sqrt{2}]$ ist ein Unterkörper von $\mathbb{R}$

Lemma 2.10 *Sei $f\colon R \to S$ ein Ringhomomorphismus. Dann ist* $\ker(f)$ *ein Ideal in R.*

Beweis: Da der Ringhomomorphismus f auch ein Gruppenhomomorphismus von $(R,+)$ nach $(S,+)$ ist, folgt aus Lemma 1.22, daß $\ker(f)$ eine Untergruppe von $(R,+)$ ist.
Für Elemente $a, b \in \ker(f)$ gilt

$$f(ab) = f(a)f(b) = 0 \cdot 0 = 0,$$

so daß $\ker(f)$ auch bzgl. der Multiplikation abgeschlossen und damit ein Unterring von R ist.
Für $x \in R$ und $i \in \ker(f)$ gilt:

$$f(xi) = f(x)f(i) = f(x) \cdot 0 = 0 \quad \text{und} \quad f(ix) = f(i)f(x) = 0 \cdot f(x) = 0,$$

so daß $\ker(f)$ sogar ein Ideal in R ist. □

Lemma 2.11 *Sei $f\colon R \to S$ ein Ringhomomorphismus. Dann gilt:*

$$f \text{ injektiv} \quad \Longleftrightarrow \quad \ker(f) = \{0_R\}.$$

Beweis:
$\Rightarrow$: Da der Ringhomomorphismus f als Gruppenhomomorphismus von $(R,+)$ nach $(S,+)$ das neutrale Element 0_R auf das neutrale Element 0_S abbildet und f injektiv ist, kann kein weiteres Element außer 0_R in $\ker(f)$ liegen.
$\Leftarrow$: Es ist zu zeigen: $f(a) = f(b) \Rightarrow a = b$:

$$f(a) = f(b) \quad \Rightarrow \quad f(a) - f(b) = 0_S \quad \Rightarrow \quad f(a-b) = 0_R.$$

Somit ist $a - b \in \ker(f) = \{0_R\}$, d.h. $a - b = 0_R$, also $a = b$. □

Lemma 2.12 *Sei K ein Körper und $I \subseteq K$ ein Ideal. Dann gilt:*

$$I = \{0\} \quad \text{oder} \quad I = K.$$

Beweis: Sei $I \neq \{0\}$. Dann gibt es ein $a \in I$ mit $a \neq 0$. Im Körper K existiert a^{-1}, und es ist

$$1 = \underbrace{a^{-1}}_{\in K} \underbrace{a}_{\in I} \in I.$$

Dann gilt für alle $x \in K$:

$$x = \underbrace{x}_{\in K} \underbrace{1}_{\in I} \in I, \qquad \text{also } K \subseteq I, \quad \text{also } K = I.$$

□

Lemma 2.13 *Ein Körperhomomorphismus $f : K \to L$ ist injektiv. Das Bild $f(K)$ ist ein Unterkörper von L; er ist isomorph zum Körper K.*

Beweis:
1) $f\colon K \to L$ ist Ringhomomorphismus. Somit ist nach Lemma 2.10 $\ker(f)$ ein Ideal im Körper K.
2) Nach Lemma 2.12 ist entweder $\ker(f) = \{0\}$ oder $\ker(f) = K$.
3) Da f ein Körperhomomorphismus ist, gilt definitionsgemäß $f(K) \neq \{0\}$ und somit $\ker(f) \neq K$, also ist $\ker(f) = \{0\}$.
4) Nach Lemma 2.11 ist f injektiv wegen $\ker(f) = \{0\}$.
5) Es bildet f $K - \{0\}$ auf $L - \{0\}$ ab. Man wendet Satz 1.22 auf die Gruppenhomomorphismen $f : (K, +) \to (L, +)$ und $f : (K - \{0\}, \cdot) \to (L - \{0\}, \cdot)$ an. Daher ist $f(K)$ eine Untergruppe von $(L, +)$ und $f(K - \{0\})$ eine Untergruppe von $(L - \{0\}, \cdot)$; also ist $f(K)$ ein Unterkörper von L. □

Satz 2.14 *Sei R ein Ring und $I \subseteq R$ ein Ideal. Für $a \in R$ sei $[a] := a + I$ die Linksnebenklasse von a bezüglich des Normalteilers I der abelschen Gruppe $(R, +)$. Dann sind auf R/I die beiden Vernüpfungen*

$$[a] + [b] := [a + b] \quad \textit{und} \quad [a] \cdot [b] := [ab]$$

wohldefiniert und R/I ist mit diesen Verknüpfungen ein Ring.
Ist R kommutativ, so auch R/I, und besitzt R eine 1, so ist $[1]$ die 1 in R/I.
Weiter ist die Abbildung

$$\pi_I\colon R \to R/I \quad \textit{mit} \quad \pi_I(a) := [a]$$

ein surjektiver Ringhomomorphismus mit $\ker(\pi_I) = I$.

Beweis: Die Verknüpfung $[a] + [b] := [a + b]$ ist nach Satz 1.36 wohldefiniert, und $(R/I, +)$ ist eine abelsche Gruppe.
Zur Wohldefiniertheit von $[a] \cdot [b] := [ab]$: Sei $[a] = [\tilde{a}]$ und $[b] = [\tilde{b}]$, d.h. $a + I = \tilde{a} + I$ und $b + I = \tilde{b} + I$. Dann gibt es Elemente $x, y \in I$ mit

$$a + x = \tilde{a} \quad \text{und} \quad b + y = \tilde{y}.$$

Es folgt dann wegen $x, y \in I$ und damit $ay, xb, xy \in I$ (Definition Ideal):

$$\begin{aligned}[\tilde{a}\tilde{b}] &= \tilde{a}\tilde{b} + I = (a+x)(b+y) + I \\ &= (ab+I) + (\underbrace{ay}_{\in I} + I) + (\underbrace{xb}_{\in I} + I) + (\underbrace{xy}_{\in I} + I) \\ &= (ab+I) + I + I + I = ab + I = [ab].\end{aligned}$$

Die Multiplikation ist assoziativ, und es gelten die Distributivgesetze, da sie sich aus dem Ring R übertragen:

$$\begin{aligned}&[a]([b][c]) = [a][(bc)] = [a(bc)] = [(ab)c] = [ab][c] = ([a][b])[c], \\ &[a]([b]+[c]) = [a][(b+c)] = [a(b+c)] = [ab+ac] = [ab]+[ac] = [a][b]+[a][c], \\ &([b]+[c])[a] = [(b+c)][a] = [(b+c)a] = [ba+ca] = [ba]+[ca] = [b][a]+[c][a].\end{aligned}$$

Somit ist R/I ein Ring.
Ist R kommutativ, so auch R/I wegen

$$[a][b] = [ab] = [ba] = [b][a].$$

Ebenso liefert $1 \in R$ eine 1 in R/I:

$$[1][a] = [1a] = [a] = [a1] = [a][1].$$

Nach Satz 1.37 ist π_I ein surjektiver Gruppenhomomorphismus mit $\ker(\pi_I) = I$, und π_I ist auch ein Ringhomomorphismus wegen

$$\pi_I(ab) = [ab] = [a][b] = \pi_I(a)\pi_I(b).$$

□

Die Ringe $\mathbb{Z}$ und $\mathbb{Z}/m\mathbb{Z}$

Definition 2.15 a) Seien $a, b \in \mathbb{Z} - \{0\}$.

$$\begin{aligned}\mathrm{kgV}(a,b) &:= \text{“kleinstes gemeinsames Vielfaches”} = \min(n \in \mathbb{N} \mid a|n \text{ und } b|n), \\ \mathrm{ggT}(a,b) &:= \text{“größter gemeinsamer Teiler”} = \max(n \in \mathbb{N} \mid n|a \text{ und } n|b).\end{aligned}$$

b) $p \in \mathbb{N}$ mit $p \neq 1$ ist eine Primzahl, falls 1 und p seine einzigen Teiler in $\mathbb{N}$ sind.

Satz 2.16 *Seien $a, b \in \mathbb{Z} - \{0\}$.*
a) $a\mathbb{Z} \cap b\mathbb{Z} = \mathrm{kgV}(a,b)\mathbb{Z}$.
b) Es gibt $k, l \in \mathbb{Z}$ mit $\mathrm{ggT}(a,b) = ka + lb$. Man kann k oder l in $\mathbb{N}$ wählen.
c) Sei nun p eine Primzahl mit $p|ab$. Dann gilt $p|a$ oder $p|b$.

d) Seien $p_1, ..., p_k$ und $q_1, ..., q_l$ Primzahlen mit

$$p_1 \cdot ... \cdot p_k = q_1 \cdot ... \cdot q_l.$$

Dann ist $k = l$, und es gibt eine Bijektion $\sigma \in S_k$ mit

$$p_i = q_{\sigma(i)} \quad \text{für } i = 1, ..., k.$$

Dies ist die Eindeutigkeit der Zerlegung einer natürlichen Zahl in Primzahlen. Sie ist NICHT *selbstverständlich.*
e) Sei $c \in \mathbb{Z} - \{0\}$ und $\mathrm{ggT}(a, c) = 1$, $\mathrm{ggT}(b, c) = 1$. Dann ist auch $\mathrm{ggT}(ab, c) = 1$.

Beweis: a) $a\mathbb{Z}$ und $b\mathbb{Z}$ sind Untergruppen von $(\mathbb{Z}, +)$, also ist auch $a\mathbb{Z} \cap b\mathbb{Z}$ eine. Nach Satz 1.24 a) existiert ein $m \in \mathbb{N}$ mit $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.
Aus $m \in a\mathbb{Z}$ und $m \in b\mathbb{Z}$ folgt $a|m$ und $b|m$, also $m \geq \mathrm{kgV}(a, b)$.
Andererseits ist $\mathrm{kgV}(a, b) \in a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$, also $\mathrm{kgV}(a, b) \geq m$.
Also ist $\mathrm{kgV}(a, b) = m$.
b) Die Menge $\{ka + lb \mid k, l \in \mathbb{Z}\}$ ist eine Untergruppe von $(\mathbb{Z}, +)$. Nach Satz 1.24 a) existiert ein $m \in \mathbb{N}$ mit $\{ka + lb \mid k, l \in \mathbb{Z}\} = m\mathbb{Z}$, und es existieren $k_0, l_0 \in \mathbb{Z}$ mit $m = k_0 a + l_0 b$. Mit

$$c := k_0 \frac{a}{\mathrm{ggT}(a, b)} + l_0 \frac{b}{\mathrm{ggT}(a, b)} \in \mathbb{N}$$

ist $m = c \cdot \mathrm{ggT}(a, b)$, also $m \geq \mathrm{ggT}(a, b)$.
Wegen $a \in m\mathbb{Z}$ ($\Leftarrow k = 1, l = 0$) und $b \in m\mathbb{Z}$ ($\Leftarrow k = 0, l = 1$) ist m ein Teiler von a und b, also $m \leq \mathrm{ggT}(a, b)$. Es folgt $m = \mathrm{ggT}(a, b)$.
Wenn man k_0 und l_0 abändert zu

$$k_1 = k_0 + \alpha \cdot \frac{b}{\mathrm{ggT}(a, b)}, \quad l_1 = l_0 - \alpha \cdot \frac{a}{\mathrm{ggT}(a, b)}$$

mit einem beliebigen $\alpha \in \mathbb{Z}$, gilt immer noch $k_1 a + l_1 b = \mathrm{ggT}(a, b)$. Insbesondere kann man $k_1 > 0$ oder $l_1 > 0$ erreichen (aber meistens nicht beides zugleich).
c) Annahme: $p \not| a$. Zu zeigen: $p|b$.
Annahme und p Primzahl $\Longrightarrow \mathrm{ggT}(a, p) = 1$.
Aus b) folgt, daß $k, l \in \mathbb{Z}$ mit $ka + lp = 1$ existieren. Dann ist

$$b = 1 \cdot b = (ka + lp) \cdot b = k(ab) + (lb)p.$$

Mit $p|ab$ folgt $p|b$.
d) Aus c) und

$$p_1|(p_1 \cdot ... \cdot p_k) = q_1 \cdot (q_2 \cdot ... \cdot q_l)$$

folgt $p_1|q_1$ oder $p_1|(q_2 \cdot ... \cdot q_l)$. Induktiv folgt: p_1 teilt ein q_j.

Weil q_j eine Primzahl ist, ist $p_1 = q_j$. Daher ist

$$p_2 \cdot \ldots \cdot p_k = q_1 \cdot \ldots \cdot q_{j-1} \cdot q_{j+1} \cdot \ldots \cdot q_l.$$

Induktiv folgen $k = l$ und die Existenz von $\sigma \in S_k$ mit $p_i = q_{\sigma(i)}$.
e) Wegen d) hat man nun die eindeutige Primfaktorzerlegung von a, b und c zur Verfügung. Man hat *die* Primfaktoren von a, b und c. Nun gilt:

$$\begin{aligned} \mathrm{ggT}(a,c) &\iff \text{die Primfaktoren von } a \text{ und } c \text{ sind disjunkt,} \\ \mathrm{ggT}(b,c) &\iff \text{die Primfaktoren von } b \text{ und } c \text{ sind disjunkt.} \end{aligned}$$

Die Primfaktoren von ab sind die Vereinigungsmenge der Primfaktoren von a und b. Daher sind die Primfaktoren von ab und c disjunkt, und daher ist $\mathrm{ggT}(ab, c) = 1$. □

Satz 2.17 *Sei $m \in \mathbb{N}$. Auf $\mathbb{Z}/m\mathbb{Z}$ ist eine Multiplikation wohldefiniert durch*

$$[a] \cdot [b] := [a \cdot b].$$

(Hier ist $[a] = a + m\mathbb{Z}$ die Kongruenzklasse von $a \in \mathbb{Z}$.) Damit ist $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ein kommutativer Ring mit 1.

1. Beweis: Anwendung von Satz 2.14. Man muß bloß noch zeigen, daß $m\mathbb{Z}$ ein Ideal in $\mathbb{Z}$ ist: leicht, Übung.
2. Beweis (er wiederholt Argumente des Beweises von Satz 2.14 im Spezialfall $R = \mathbb{Z}$): Multiplikation wohldefiniert: zu zeigen ist, daß die Multiplikation von der Wahl der Repräsentanten unabhängig ist, d.h. zu zeigen ist

$$[a_1] = [a_2] \text{ und } [b_1] = [b_2] \Rightarrow [a_1 \cdot b_1] = [a_2 \cdot b_2].$$

Sei $[a_1] = [a_2]$ und $[b_1] = [b_2]$; also $a_1 = a_2 + m\alpha$ und $b_1 = b_2 + m\beta$ mit geeigneten $\alpha, \beta \in \mathbb{Z}$.

$$a_1 b_1 = (a_2 + m\alpha)(b_2 + m\beta) = a_2 b_2 + m(a_2\beta + \alpha b_2 + m\alpha\beta),$$

also $[a_1 b_1] = [a_2 b_2]$.
Es bleibt zu zeigen: die Multiplikation ist assoziativ und kommutativ, die Distributivgesetze gelten, 1 ist ein Einselement.
Aber weil man mit Repräsentanten rechnen darf, bekommt man alle gewünschten Eigenschaften in $\mathbb{Z}/m\mathbb{Z}$ von den entsprechenden Eigenschaften in $\mathbb{Z}$.
Beispiel 1. Distributivgesetz:

$$\begin{aligned} & [a]([b] + [c]) = [a][b + c] = [a(b + c)] \\ \overset{\text{Distg.in}\mathbb{Z}}{=} \; & [ab + ac] = [ab] + [ac] = [a][b] + [a][c] \end{aligned}$$

□

Beispiele 2.18 i) In In $\mathbb{Z}/5\mathbb{Z}$ hat jedes Element ein multiplikatives Inverses: $[1][1] = [1]$, $[2][3] = [6] = [1]$, $[4][4] = [16] = [1]$.
ii) In $\mathbb{Z}/6\mathbb{Z}$ ist $[2] \cdot [3] = [6] = [0] = 0$, aber $[2] \neq 0$ und $[3] \neq 0$; $[2]$ und $[3]$ haben keine multiplikativen Inversen. Sie sind Nullteiler.

Satz 2.19 *Sei $m \in \mathbb{N}$, $m \geq 2$.*

a) Sei $a \in \mathbb{Z}$. Die Kongruenzklasse $[a] \in \mathbb{Z}/m\mathbb{Z}$ hat ein multiplikatives Inverses in $\mathbb{Z}/m\mathbb{Z}$ genau dann, wenn $\mathrm{ggT}(a, m) = 1$.

b) Die Teilmenge $\{[a] \in \mathbb{Z}/m\mathbb{Z} \mid 0 < a < m,\ \mathrm{ggT}(a, m) = 1\}$ von $\mathbb{Z}/m\mathbb{Z}$ ist zusammen mit der Multiplikation von $\mathbb{Z}/m\mathbb{Z}$ eine Gruppe. Sie wird mit $(\mathbb{Z}/m\mathbb{Z})^*$ bezeichnet und Einheitengruppe von $\mathbb{Z}/m\mathbb{Z}$ genannt.

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

d) Für $[a] \in \mathbb{Z}/m\mathbb{Z}$ sind äquivalent:

$[a]$ ist eine Einheit in $\mathbb{Z}/m\mathbb{Z}$ $\iff$ *$[a]$ ist ein Erzeuger der zyklischen Gruppe $(\mathbb{Z}/m\mathbb{Z}, +)$.*

Beweis: a) „$\Rightarrow$“: Sei $[b]$ ein multiplikatives Inverses von $[a]$. $[a][b] = [1]$ sagt: m teilt $ab - 1$. Daher ist $\mathrm{ggT}(a, m) = 1$.
„$\Leftarrow$“: $\mathrm{ggT}(a, m) = 1$ und Satz 2.16 b) geben $k, l \in \mathbb{Z}$ mit $ka + lm = 1$. Also ist $[k][a] = [1]$.
b) Die Menge ist abgeschlossen unter Produkt und Inversen-Bildung: $\mathrm{ggT}(a, m) = 1$ und $\mathrm{ggT}(b, m) = 1 \Rightarrow \mathrm{ggT}(ab, m) = 1$ (Satz 2.16 e));
$[a][b] = [1] \Rightarrow m$ teilt $ab - 1 \Rightarrow \mathrm{ggT}(b, m) = 1$.
c) $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ist ein Körper
$\iff$ $(\mathbb{Z}/m\mathbb{Z} - \{0\}, \cdot)$ ist eine abelsche Gruppe
$\iff$ alle Elemente von $\mathbb{Z}/m\mathbb{Z} - \{0\}$ haben ein multiplikatives Inverses
$\iff$ alle $a \in \{1, ..., m-1\}$ erfüllen $\mathrm{ggT}(a, m) = 1$
$\iff$ m ist eine Primzahl.
d) Es ist zu zeigen:

$$[a] \in (\mathbb{Z}/m\mathbb{Z})^* \quad \iff \quad \langle [a] \rangle = \mathbb{Z}/m\mathbb{Z}.$$

$\Rightarrow$: Ist $[a]$ eine Einheit, so existiert ein $[b] \in \mathbb{Z}/m\mathbb{Z}$ mit $[a][b] = [1]$. Dabei kann b gewählt werden mit $0 < b < m$. Es folgt für $\mathbb{Z}/m\mathbb{Z} = \langle [1] \rangle$:

$$\begin{aligned} [a][b] = [1] \quad &\Rightarrow \quad \underbrace{[a] + \ldots + [a]}_{0 < b < m\text{-mal}} = [1] \quad \Rightarrow \quad [1] \in \langle [a] \rangle \subseteq \mathbb{Z}/m\mathbb{Z} \\ &\Rightarrow \quad \langle [1] \rangle \subseteq \langle [a] \rangle \subseteq \mathbb{Z}/m\mathbb{Z} \quad \Rightarrow \quad \langle [a] \rangle = \mathbb{Z}/m\mathbb{Z}. \end{aligned}$$

$\Leftarrow$: Aus $\langle[a]\rangle = \mathbb{Z}/m\mathbb{Z}$ folgt $[1] \in \langle[a]\rangle$, und $[1]$ kann in der endlichen Gruppe $\langle[a]\rangle$ durch ein Vielfaches $k \in \mathbb{N}$ von $[a]$ ausgedrückt werden:

$$[1] = \underbrace{[a] + \ldots + [a]}_{k\text{-mal}} \quad \Rightarrow \quad [1] = [\underbrace{a + \ldots + a}_{k\text{-mal}}] = [ka] = [k][a].$$

Somit ist $[a]$ eine Einheit in $\mathbb{Z}/m\mathbb{Z}$ mit dem multiplikativen Inversen $[k]$. □

Komplexe Zahlen

Vgl. auch Analysis I, Schmidt.

Satz/Definition 2.20 *a) Die Menge $\mathbb{C} := \mathbb{R} \times \mathbb{R}$ mit den folgendermaßen definierten Verknüpfungen $+$ und $\cdot$ ist ein Körper.*

$$\begin{aligned}(x_1, y_1) + (x_2, y_2) &:= (x_1 + x_2, y_1 + y_2),\\ (x_1, y_1) \cdot (x_2, y_2) &:= (x_1 \cdot x_2 - y_1 \cdot y_2, x_1 y_2 + y_1 x_2).\end{aligned}$$

Seine Elemente heißen komplexe Zahlen. $(0,0) =: 0$ ist das Nullelement, $(1,0) =: 1$ ist das Einselement. Ist $(x,y) \in \mathbb{C} - \{0\}$, so ist

$$(x,y)^{-1} = (\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2}).$$

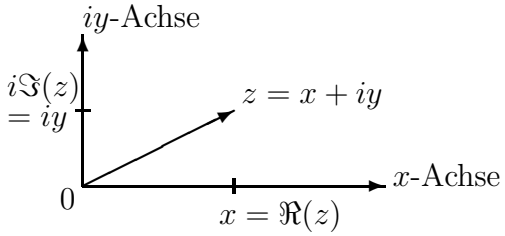
b) Das Element $(0,1) =: i$ erfüllt $i^2 = -1$. Es wird manchmal als $i = \sqrt{-1}$ geschrieben.
c) Die Abbildung $\mathbb{R} \to \mathbb{C}$, $x \mapsto (x,0)$, ist ein (natürlich injektiver) Körperhomomorphismus. Mit Hilfe dieser Abbildung wird $\mathbb{R}$ mit einem Unterkörper von $\mathbb{C}$ identifiziert.
d) Es ist (mit der Identifikation in c)) für $x, y, x_1, y_1, x_2, y_2 \in \mathbb{R}$

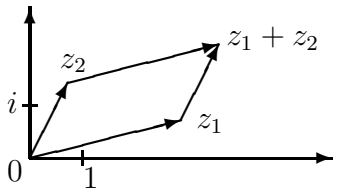
$$\begin{aligned}&(x,y) = (x,0) + (0,y) = (x,0) + (0,1)(y,0) = x + iy \in \mathbb{C},\\ &(x_1 + iy_1) + (x_2 + iy_2) = (x_1 + x_2) + i(y_1 + y_2),\\ &(x_1 + iy_1) \cdot (x_2 + iy_2) = x_1x_2 + x_1 \cdot iy_2 + iy_1 \cdot x_2 + iy_1 \cdot iy_2\\ &\qquad\qquad = (x_1x_2 - y_1y_2) + i(x_1y_2 + y_1x_2).\end{aligned}$$

Man schreibt oft $z = x + iy \in \mathbb{C}$. Der Realteil von z ist $\Re(z) := x \in \mathbb{R}$, der Imaginärteil ist $\Im(z) = y \in \mathbb{R}$. z heißt reell, falls $\Im(z) = 0$; z heißt rein imaginär, falls $\Re(z) = 0$.

Beweis: a) $(\mathbb{C}, +)$ abelsche Gruppe: klar.
Die Multiplikation $\cdot$ ist kommutativ und assoziativ, Distributivgesetze: einfache Rechnungen, Übung.
Die Formel für $(x,y)^{-1}$: nachrechnen.
b) $(0,1) \cdot (0,1) = (-1,0)$. c) Klar. d) Klar. □

Bemerkung 2.21 Man veranschaulicht sich die komplexen Zahlen in der Gaußschen Zahlenebene. Die Addition ist die komponentenweise Addition im $\mathbb{R}^2$. Multiplikation: siehe Bemerkung 2.23 iv).





Lemma/Definition 2.22 *a) Die Abbildung*

$$\bar{\cdot} : \mathbb{C} \to \mathbb{C}, \quad x + iy \mapsto x - iy,$$

ist ein Isomorphismus des Körpers $\mathbb{C}$ *auf sich, also*

$$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}, \quad \overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2} \text{ für } z_1, z_2 \in \mathbb{C}.$$

Sie heißt komplexe Konjugation.
b) Es ist $\overline{z} = z \iff z$ *reell.*
Es ist $\Re(z) = \frac{1}{2}(z + \overline{z})$, $\Im(z) = \frac{1}{2i}(z - \overline{z})$.
Es ist $\overline{\overline{z}} = z$.
Ist $z = x + iy$, *so ist* $z \cdot \overline{z} = x^2 + y^2 \in \mathbb{R}_0^+$ *und, falls* $z \neq 0$, $z^{-1} = \frac{\overline{z}}{x^2+y^2}$.
c) Der Absolutbetrag $|z|$ *von* $z = x + iy \in \mathbb{C}$ *ist*

$$|z| := \sqrt{z \cdot \overline{z}} = \sqrt{x^2 + y^2} \in \mathbb{R}_0^+.$$

Er erfüllt $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$, $\quad |\overline{z}| = |z|$ *und die Dreiecksungleichung:*
$|z_1 + z_2| \leq |z_1| + |z_2|$.

Beweis: a) Nachrechnen, Übung.
b) Klar.
c) Nachrechnen, Übung (vgl. Analysis I). □

Bemerkungen 2.23 i) Ist $z \in \mathbb{C} - \{0\}$, so ist

$$z = x + iy = |z| \cdot \left(\frac{x}{|z|} + i \frac{y}{|z|} \right) = |z| \cdot (\cos\varphi + i \sin\varphi)$$

mit einem eindeutigen $\varphi \in [0, 2\pi)$, denn $(\frac{x}{|z|})^2 + (\frac{y}{|z|})^2 = 1$. φ heißt das Argument von z. Es ist der Winkel zwischen $x - Achse$ und dem Vektor von 0 nach z in der Gaußschen Zahlenebene.

ii) In der Analysis wird die Exponentialfunktion $\exp : \mathbb{C} \to \mathbb{C} - \{0\},\ z \mapsto \exp(z) = e^z$ definiert und die *Eulersche Formel*

$$e^{i\varphi} = \cos\varphi + i\sin\varphi \quad \text{für } \varphi \in \mathbb{R}$$

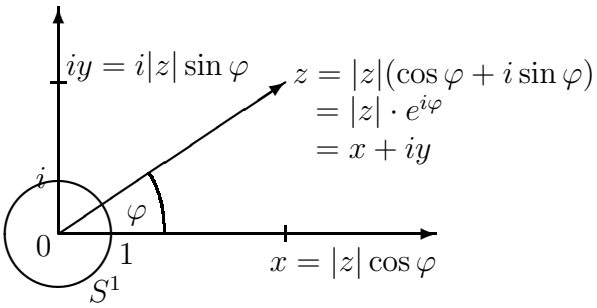
bewiesen. Die Abbildung exp ist ein Gruppenhomomorphismus $\exp : (\mathbb{C}, +) \to (\mathbb{C} - \{0\}, \cdot)$, d.h. sie erfüllt $e^{z_1+z_2} = e^{z_1}e^{z_2}$.
iii) Daher ist auch die Abbildung

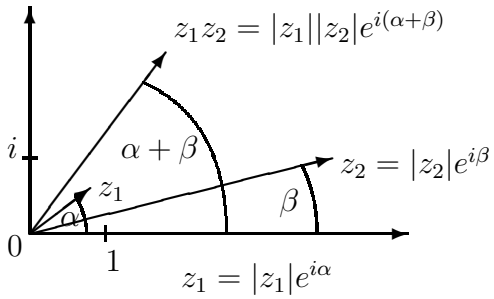
$$\mathbb{R} \to \mathbb{C},\ \varphi \mapsto e^{i\varphi} = \cos\varphi + i\sin\varphi$$

ein Gruppenhomomorphismus von $(\mathbb{R}, +)$ nach $(\mathbb{C} - \{0\}, \cdot)$. Der Kern ist $2\pi\mathbb{Z} \subset \mathbb{R}$. Das Bild ist die 1-Sphäre $S^1 := \{z \in \mathbb{C} \mid |z| = 1\}$. Es ist $(S^1, \cdot)$ eine Untergruppe von $(\mathbb{C} - \{0\}, \cdot)$.
Für $\alpha, \beta \in \mathbb{R}$ erhält man

$$\begin{aligned} & (\cos\alpha + i\sin\alpha) \cdot (\cos\beta + i\sin\beta) \\ = \ & e^{i\alpha} \cdot e^{i\beta} = e^{i(\alpha+\beta)} \\ = \ & \cos(\alpha+\beta) + i\sin(\alpha+\beta). \end{aligned}$$

Die Gleichheit der 1. und 3. Zeile ist äquivalent zu den Additionstheoremen: Gleichheit von Realteil und Imaginärteil sind die Additionstheoreme.
iv) Sind $z_1 = |z_1|e^{i\alpha}$ und $z_2 = |z_2|e^{i\beta}$, so ist $z_1 z_2 = |z_1||z_2|e^{i(\alpha+\beta)}$, d.h. beim Multiplizieren multipliziert man die Absolutwerte und addiert die Argumente.





3 Vektorräume

Definition 3.1 Sei K ein Körper.
Ein *Vektorraum über* K (oder K*-Vektorraum* oder einfach *Vektorraum*) ist eine abelsche Gruppe $(V, +)$ zusammen mit einer Abbildung

$$\cdot : K \times V \to V, \quad (\lambda, v) \mapsto \lambda \cdot v$$

mit folgenden Eigenschaften:
i) ein Distributivgesetz:

$$(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v \quad \text{für } \lambda, \mu \in K, v \in V;$$

ii) ein anderes Distributivgesetz:

$$\lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w \quad \text{für } \lambda \in K, v, w \in V;$$

iii) ein Assoziativgesetz:

$$\lambda \cdot (\mu \cdot v) = (\lambda\mu) \cdot v \quad \text{für } \lambda, \mu \in K, v \in V;$$

iv) das Einselement $1 = 1_K$ von K erfüllt:

$$1 \cdot v = v \quad \text{für } v \in V.$$

Die Abbildung $\cdot : K \times V \to V$ heißt *Multiplikation mit Skalaren* oder *skalare Multiplikation*. Die Elemente des Vektorraums V heißen *Vektoren*.

Bemerkungen 3.2 i) Wie bei Gruppen, Ringen und Körpern wird die Menge V als das primäre Objekt angesehen, die additive Gruppenstruktur, die skalare Multiplikation und auch der Körper K als sekundär. Daher spricht man vom Vektorraum V und von Elementen des Vektorraums V.
ii) Die Multiplikation mit Skalaren schreibt man mal mit, mal ohne $\cdot$ (genau wie bei den Multiplikationen in Gruppen, Ringen, Körpern).
iii) Ersetzt man in Definition 3.1 den Körper K durch einen Ring R mit 1, so heißt V ein R*-Modul*.

Beispiele 3.3 a) Sei K ein Körper und $n \in \mathbb{N}$. Dann ist K^n ein K-Vektorraum mit

$$\begin{aligned} (a_1, ..., a_n) + (b_1, ..., b_n) &:= (a_1 + b_1, ..., a_n + b_n), \\ \lambda \cdot (a_1, ..., a_n) &:= (\lambda a_1, ..., \lambda a_n). \end{aligned}$$

Im Falle $n = 0$ ist $K^0 = \{0\}$. Die Vektorräume K^n, $n \in \mathbb{N}_0$, sind mit Abstand die wichtigsten Vektorräume.

b) Am allerwichtigsten sind die $\mathbb{R}$-Vektorräume $\mathbb{R}^n$. Bei (fast) allen abstrakten Aussagen über Vektorräume ist es nützlich, an diese Vektorräume zu denken.
c) Aber es gibt auch andere Vektorräume. Sei $X \neq \emptyset$ eine Menge und K ein Körper. Die Menge $\mathrm{Abb}(X, K)$ ist ein Vektorraum, mit punktweiser Addition und punktweiser skalarer Multiplikation: bei $f, g \in \mathrm{Abb}(X, K)$, $\lambda \in K$ sind $f + g$ und $\lambda \cdot f \in \mathrm{Abb}(X, K)$ definiert durch

$$(f + g)(x) := f(x) + g(x),\ (\lambda \cdot f)(x) := \lambda \cdot f(x) \quad \text{für } x \in X.$$

d) Die Menge $\mathrm{Abb}([0, 1], \mathbb{R})$ und die Teilmengen

$$\begin{aligned} \mathcal{C}^0([0, 1], \mathbb{R}) &:= \{f : [0, 1] \to \mathbb{R} \mid f \text{ ist stetig}\}, \\ \mathcal{C}^1([0, 1], \mathbb{R}) &:= \{f : [0, 1] \to \mathbb{R} \mid f \text{ ist stetig differenzierbar}\} \end{aligned}$$

(Def. von *stetig* und *stetig differenzierbar* in der Analysis) sind $\mathbb{R}$-Vektorräume.
e) Sei K ein Körper. Der Polynomring $K[t]$ ist auch ein K-Vektorraum.
f) Ist V ein $\mathbb{R}$-Vektorraum, so ist V mit der Einschränkung der skalaren Multiplikation auf $\mathbb{Q} \times V$ natürlich auch ein $\mathbb{Q}$-Vektorraum.

Lemma 3.4 *Sei V ein K-Vektorraum, $0_K \in K$ die Null in K, $0_V \in V$ die Null in V.*
a) $0_K \cdot v = 0_V$ *bei* $v \in V$.
b) $\lambda \cdot 0_V = 0_V$ *bei* $\lambda \in K$.
c) $\lambda \cdot v = 0_V \Rightarrow \lambda = 0_K$ *oder* $v = 0_V$.
d) $(-1) \cdot v = -v$ *bei* $v \in V$.

Beweis: a) $0_k \cdot v = (0_K + 0_K) \cdot v = 0_K \cdot v + 0_K \cdot v$, also $0_V = 0_K \cdot v$.
b) $\lambda \cdot 0_V = \lambda \cdot (0_V + 0_V) = \lambda \cdot 0_V + \lambda \cdot 0_V$, also $0_V = \lambda \cdot 0_V$.
c) Sei $\lambda \cdot v = 0_V$ und $\lambda \neq 0$. Dann ist $v = 1 \cdot v = (\lambda^{-1}\lambda) \cdot v = \lambda^{-1} \cdot (\lambda \cdot v) = \lambda^{-1} \cdot 0_V = 0_V$.
d) $v + (-1) \cdot v = (1 + (-1)) \cdot v = 0_K \cdot v = 0_V$. □

Von nun an werden die Nullen 0_K und 0_V beide als 0 bezeichnet; die Verwechslungsgefahr ist gering.

Definition/Lemma 3.5 *a) (Definition) Sei V ein K-Vektorraum. Eine Teilmenge U heißt Untervektorraum, falls $U \neq \emptyset$ ist und falls U abgeschlossen unter der Addition und der skalaren Multiplikation ist, d.h. falls gilt:*

$$\begin{aligned} v \in U, w \in U &\Rightarrow v + w \in U, \\ \lambda \in K, v \in U &\Rightarrow \lambda \cdot v \in U. \end{aligned}$$

b) (Lemma) Ein Untervektorraum U eines K-Vektorraums V ist selber ein K-Vektorraum.

Beweis: a) Definition. b) Wegen $U \neq \emptyset$ gibt es ein $v \in U$. Es ist $(-1) \cdot v \in U$ und $0 = v + (-1) \cdot v \in U$. Also ist $(U, +)$ eine abelsche Gruppe. Die Eigenschaften i) – iv) von Definition 3.1 gelten in U, weil sie in V gelten. □

Beispiele 3.6 a) Sei U ein Untervektorraum von $\mathbb{R}^2$ als $\mathbb{R}$-Vektorraum. Ist $v \in U$ und $v \neq 0$, so ist $\{\lambda \cdot v \mid \lambda \in \mathbb{R}\} \subset U$. Ist darüberhinaus $w \in U$ und $w \notin \{\lambda \cdot v \mid \lambda \in \mathbb{R}\}$, so ist

$$U \supset \{\lambda \cdot v + \mu \cdot w \mid \lambda, \mu \in \mathbb{R}\} = \mathbb{R}^2,$$

also $U = \mathbb{R}^2$. Skizze in der Vorlesung
Daher sind die einzigen Untervektorräume von $\mathbb{R}^2$ (als $\mathbb{R}$-Vektorraum) die Mengen

$$\begin{array}{ll} \{0\}, & \\ \{\lambda \cdot v \mid \lambda \in \mathbb{R}\} & \text{mit } v \in \mathbb{R}^2 - \{0\}, \\ \mathbb{R}^2. & \end{array}$$

b) Daher sind die folgenden Teilmengen alle keine Untervektorräume von $\mathbb{R}^2$ als $\mathbb{R}$-Vektorraum (Skizzen in der Vorlesung):

$$\begin{array}{l} \{(x,y) \in \mathbb{R}^2 \mid y = x^2\}, \\ \{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 1\}, \\ \{(x,y) \in \mathbb{R}^2 \mid |x| \leq 1\}, \\ \{(x,y) \in \mathbb{R}^2 \mid x \cdot y = 0\}, \\ \{(x,y) \in \mathbb{R}^2 \mid x \geq 0, y \geq 0\}. \\ \{(x,y) \in \mathbb{R}^2 \mid (x,y) \in \mathbb{Q}^2\}. \end{array}$$

Man sieht auch direkt, daß sie nicht invariant unter der Addition und/oder der skalaren Multiplikation sind.
c) $\mathbb{C}$ ist ein $\mathbb{R}$-Vektorraum, und $\mathbb{R} \subset \mathbb{C}$ ist ein Untervektorraum von $\mathbb{C}$ als $\mathbb{R}$-Vektorraum.
d) Die $\mathbb{R}$-Vektorräume $\mathcal{C}^0([0,1], \mathbb{R})$ und $\mathcal{C}^1([0,1], \mathbb{R})$ (vgl. Beispiele 3.3 d)) sind Untervektorräume von $\mathrm{Abb}([0,1], \mathbb{R})$.
e) Sei K ein Körper. Es gilt (Beweis hier nicht):
Ein Polynom $f(t) \in K[t]$ vom Grad n hat höchstens n verschiedene Nullstellen. Konkreter: Seien $\lambda_1, ..., \lambda_k \in K$ verschiedene Nullstellen von $f(t) = a_n t^n + ... + a_1 t + a_0$. Dann ist $k \leq n$, und es gibt $b_{n-k}, ..., b_1, b_0 \in K$ mit

$$f(t) = (t - \lambda_1) \cdot ... \cdot (t - \lambda_k) \cdot (b_{n-k} t^{n-k} + ... + b_1 t + b_0).$$

Falls $|K| = \infty$ ist, so ist daher die Abbildung

$$\Phi : K[t] \to \mathrm{Abb}(K, K), \quad f(t) \mapsto (a \mapsto f(a)),$$

injektiv. Dann kann $K[t]$ mit seinem Bild $\Phi(K[t]) \subset \mathrm{Abb}(K,K)$ identifiziert werden. Der Polynomring wird dann ein Untervektorraum von $\mathrm{Abb}(K,K)$. Im Fall $|K| < \infty$ ist Φ nicht injektiv: Sei $K = \{\lambda_1, ..., \lambda_k\}$ und $f(t) = (t-\lambda_1) \cdot ... \cdot (t-\lambda_k)$. Dann ist $f(t) \neq 0$, $\mathrm{grad}\, f(t) = k$, aber $\Phi(f(t)) = 0$.
f) Im Fall $K = \mathbb{R}$ ist auch die Abbildung $\mathbb{R}[t] \to \mathrm{Abb}([0,1], \mathbb{R})$ injektiv (denn $[0,1]$ hat unendlich viele Elemente). Wieder kann man $\mathbb{R}[t]$ mit seinem Bild identifizieren. Dann hat man folgende Kette von Untervektorräumen von $\mathrm{Abb}([0,1], \mathbb{R})$,

$$\mathbb{R}[t] \subset \mathcal{C}^1([0,1], \mathbb{R}) \subset \mathcal{C}^0([0,1], \mathbb{R}) \subset \mathrm{Abb}([0,1], \mathbb{R}).$$

Bemerkungen 3.7 i) *Vektorraumhomomorphismen* (=*lineare Abbildungen*) werden erst in Kapitel 5 diskutiert.
ii) Im folgenden werden die Begriffe *Erzeugendensystem*, *Basis* und *Dimension* etabliert. Die *Dimension* eines Vektorraums V soll definiert werden als die Anzahl der Elemente einer Basis von V (Def. 3.12). Dazu muß gezeigt werden, daß alle Basen von V gleich viele Elemente haben (Satz 3.17). Es wird u.a. $\dim_K K^n = n$ herauskommen.

Notationen 3.8 a) Sei X eine nichtleere Menge und $n \in \mathbb{N}$. Die Menge der n-Tupel, $X^n = \{(x_1, ..., x_n) \mid x_i \in X\}$ wird mit der Menge der Abbildungen $\{1, ..., n\} \to X$ identifiziert: zu einem n-Tupel $(x_1, ..., x_n)$ gehört die Abbildung $i \mapsto x_i$.
b) Sind I und X nichtleere Mengen, so wird eine Abbildung $I \to X, i \mapsto x_i$ auch *Familie* $(x_i)_{i \in I}$ genannt. Die Menge I wird dann *Indexmenge* genannt. Ein n-Tupel $(y_1, ..., y_n)$ ist also eine Familie $(y_j)_{j \in \{1,...,n\}}$.
c) Sei $(V, +)$ eine abelsche Gruppe und $(v_1, ..., v_n) \in V^n$, $n \in \mathbb{N}$. Dann ist

$$\sum_{i=1}^{n} v_i := v_1 + ... + v_n.$$

Ist allgemeiner $(w_j)_{j \in J}$ eine Familie mit $w_j \in V$ und J eine *endliche* Indexmenge, so ist $\sum_{j \in J} w_j$ die Summe aller Mitglieder w_j der endlichen Familie $(w_j)_{j \in J}$; genauer: man wählt eine Bijektion $\sigma : \{1, ..., |J|\} \to J$ und definiert

$$\sum_{j \in J} w_j := \sum_{i=1}^{|J|} w_{\sigma(i)} = w_{\sigma(1)} + ... + w_{\sigma(|J|)}.$$

(*Unendliche Summen* werden in der Analysis und Funktionalanalysis behandelt, nicht in der linearen Algebra.) Die folgende Konvention ist nützlich: für $K := \emptyset \subset J$ ist $\sum_{k \in K} w_k := 0$.
d) Ist $(G, \cdot)$ eine abelsche Gruppe (mit multiplikativ geschriebener Verknüpfung) und $(w_j)_{j \in J}$ eine Familie mit $w_j \in V$ und mit *endlicher* Indexmenge J, so ist (analog zu c)) $\prod_{j \in J} w_j$ das Produkt aller Mitglieder der Familie.

e) Ist I eine beliebige (nicht notwendig endliche) Indexmenge und hat man für jedes $i \in I$ eine Menge M_i, so ist ihre Schnittmenge

$$\bigcap_{i \in I} M_i := \{a \mid a \in M_i \text{ für alle } i \in I\}$$

und ihre Vereinigungsmenge

$$\bigcup_{i \in I} M_i := \{a \mid \text{ es gibt ein } i \in I \text{ mit } a \in M_i\}.$$

Definition 3.9 Sei V ein K-Vektorraum.
a) Sei $(v_1, ..., v_n) \in V^n$, $n \in \mathbb{N}$. Dann ist

$$\text{span}_K(v_1, ..., v_n) := \langle v_1, ..., v_n \rangle_K := \{\sum_{i=1}^{n} \lambda_i v_i \mid \lambda_i \in K\}.$$

Ist allgemeiner I eine beliebige (nicht notwendig endliche) Indexmenge, so ist

$$\text{span}_K(v_i)_{i \in I} := \langle v_i \mid i \in I \rangle_K := \bigcup_{J \subset I, J \text{ endlich}} \text{span}(v_j)_{j \in J}.$$

Ein Element $\sum_{j \in J} \lambda_j v_j$ mit $J \subset I$ endlich heißt *(endliche) Linearkombination* der v_i, $i \in I$. Die Menge $\text{span}_K(v_i)_{i \in I}$ heißt der von $(v_i)_{i \in I}$ *erzeugte Raum.*
b) Ist $T \subset V$ eine nichtleere Teilmenge, so ist

$$\text{span}_K T := \text{span}_K(t)_{t \in T}.$$

(Hier dient T selbst als Indexmenge: die Elemente von T sind durch sich selbst indiziert.) Die folgende Konvention ist nützlich: $\text{span}_K \emptyset := \{0\} \subset V$.

Beispiele 3.10 i) Jedes Element des K-Vektorraums K^n ($n \in \mathbb{N}$) ist eine Linearkombination der Vektoren $e_1 := (1, 0, ..., 0)$, $e_2 := (0, 1, 0, ..., 0)$,...,$e_n := (0, .., 0, 1)$; es ist

$$(x_1, ..., x_n) = \sum_{i=1}^{n} x_i e_i, \quad \text{span}_K(e_1, ..., e_n) = K^n.$$

ii) Jedes Polynom im K-Vektorraum $K[t]$ ist eine Linearkombination der Monome $1, t, t^2, t^3, ...$ Es ist $\text{span}_K(t^i)_{i \in \mathbb{N}_0} = K[t]$.
iii) Ist T eine beliebige der 6 Teilmengen von $\mathbb{R}^2$ in Beispiel 3.6 b), so ist $\text{span}_{\mathbb{R}} T = \mathbb{R}^2$.

Lemma 3.11 *Sei V ein K-Vektorraum und $(v_i)_{i \in I}$ eine Familie von Elementen von V. Der erzeugte Raum $\text{span}_K(v_i)_{i \in I}$ ist ein Untervektorraum von V. Er ist der kleinste Untervektorraum, der alle v_i enthält.*

Beweis: Erinnerung an die Definition von span:

$$\begin{aligned}\mathrm{span}_K(v_i)_{i\in I} &= \bigcup_{J\subset I} \mathrm{span}_K(v_j)_{j\in J} \\ &= \{\sum_{j\in J} \lambda_j v_j \mid J \subset I \text{ endlich}, \lambda_j \in K \text{ für } j \in J\}.\end{aligned}$$

Abgeschlossen unter skalarer Multiplikation:

$$\lambda \cdot (\sum_{j\in J} \lambda_j v_j) = \sum_{j\in J} (\lambda \cdot \lambda_j) v_j.$$

Abgeschlossen unter Addition: sind $a = \sum_{j\in J_1} \lambda_j v_j$ und $b = \sum_{j\in J_2} \mu_j v_j$ mit $J_1, J_2 \subset I$ endlich, so kann man definieren

$$\begin{aligned}\lambda_j &:= 0 \text{ für } j \in J_2 - J_1 \text{ und} \\ \mu_j &:= 0 \text{ für } j \in J_1 - J_2;\end{aligned}$$

dann ist

$$a + b = \sum_{j\in J_1\cup J_2} (\lambda_j + \mu_j) v_j.$$

Jeder Untervektorraum, der alle v_i, $i \in I$, enthält, enthält auch alle Linearkombinationen, denn er ist abgeschlossen unter Addition und skalarer Multiplikation. Also umfaßt er $\mathrm{span}_K(v_i)_{i\in I}$. □

Definition 3.12 Sei V ein K-Vektorraum und $(v_i)_{i\in I}$ eine Familie von Elementen von V.
a) Die Familie $(v_i)_{i\in I}$ heißt *Erzeugendensystem* von V, falls $V = \mathrm{span}_K(v_i)_{i\in I}$ ist.
b) Die Familie $(v_i)_{i\in I}$ heißt *linear unabhängig*, falls für jede endliche Teilmenge $J \subset I$ gilt

$$\sum_{j\in J} \lambda_j v_j = 0 \Rightarrow \lambda_j = 0 \text{ für alle } j \in J.$$

Sonst heißt sie *linear abhängig*.
c) Die Familie $(v_i)_{i\in I}$ heißt *Basis* von V, falls sie ein Erzeugendensystem von V ist und linear unabhängig ist.

Beispiele 3.13 Sei K ein Körper.
i) Das n-Tupel $(e_1, ..., e_n)$ (vgl. Bsp. 3.10) ist eine Basis des K-Vektorraums K^n $(n \in \mathbb{N})$.
ii) Die Familie $(t^i)_{i\in\mathbb{N}\cup\{0\}}$ aller Monome t^i ist eine Basis des K-Vektorraums $K[t]$.
iii) $(1, i)$ ist eine Basis des $\mathbb{R}$-Vektorraums $\mathbb{C}$.

iv) Für jedes $x \in [0,1]$ wird eine Abbildung $\chi_x : [0,1] \to K$ definiert durch $\chi_x(x) := 1$ und $\chi_x(y) := 0$, falls $y \in [0,1] - \{x\}$. Die Familie $(\chi_x)_{x\in[0,1]}$ ist linear unabhängig, aber sie ist keine Basis von $\mathrm{Abb}([0,1], K)$. Sie ist eine Basis des Unterraums aller Abbildungen, die nur bei endlich vielen Elementen von $[0,1]$ Werte $\neq 0$ haben.

Satz 3.14 *Sei V ein K-Vektorraum.*
a) Eine Familie $(v_i)_{i\in I}$ ist zum Beispiel linear abhängig, falls ein $v_i = 0$ ist oder falls $v_i = v_j$ für zwei Indices $i \neq j$ ist. Sie ist linear abhängig genau dann, wenn ein Mitglied v_i Linearkombination der anderen ist.
b) Sei $(v_i)_{i\in I}$ eine Familie von Vektoren in V. Die folgenden vier Bedingungen sind äquivalent:

i) Sie ist eine Basis.

ii) Jedes Element von V läßt sich mit eindeutigen Koeffizienten als Linearkombination der v_i, $i \in I$, schreiben, d.h. für jede endliche Teilmenge $J \subset I$ gilt

$$\sum_{j\in J} \lambda_j v_j = \sum_{j\in J} \mu_j v_j \Rightarrow \lambda_j = \mu_j \text{ für alle } j \in J.$$

iii) Sie ist ein minimales Erzeugendensystem, *d.h. sie ist ein Erzeugendensystem, und wenn man ein v_i wegläßt, so ist die Restfamilie $(v_j)_{j\in I-\{i\}}$ nicht mehr ein Erzeugendensystem.*

iv) Sie ist maximal linear unabhängig, *d.h. sie ist linear unabhängig, und wenn man ein $v_0 \in V$ mit $0 \notin I$ hinzufügt, so ist die erweiterte Familie $(v_j)_{j\in I\cup\{0\}}$ linear abhängig.*

Beweis: a) Die Beispielfälle sind klar:

$$\text{Für beliebiges } \lambda \in K \text{ ist } \lambda \cdot v_i = 0 \text{ falls } v_i = 0.$$
$$\text{Für beliebiges } \lambda \in K \text{ ist } \lambda \cdot v_i + (-\lambda) \cdot v_j = 0, \text{ falls } v_i = v_j.$$

Zur "genau dann wenn"-Aussage: "⇒": Ist $\sum_{j\in J} \lambda_j v_j = 0$ und $\lambda_k \neq 0$ für ein $k \in J$, so ist $v_k = \sum_{j\in J-\{k\}} (-\frac{\lambda_j}{\lambda_k}) v_j$.
"⇐": Ist $v_k = \sum_{j\in J-\{k\}} \mu_j v_j$, so ist $0 = (-1)v_k + \sum_{j\in J-\{k\}} \mu_j v_j$.
b) "i) ⇒ ii)": Basis ⇒ Erzeugendensystem ⇒ Jedes Element ist Linearkombination der v_i, $i \in I$.
Eindeutigkeit der Koeffizienten: Man wendet die lineare Unabhängigkeit (d.h. Def. 3.12 b)) an auf die Differenz von rechter und linker Seite in ii); man erhält $\lambda_j - \mu_j = 0$.
"ii) ⇒ i)": i) ist der Spezialfall von ii) mit $\mu_j = 0$ für alle j.
"i) ⇒ iii)": Basis ⇒ Erzeugendensystem.

Zu zeigen bleibt, daß es minimal ist. Indirekter Beweis. Annahme: für ein geeignetes $i \in I$ ist $(v_j)_{j\in I-\{i\}}$ immer noch ein Erzeugendensystem von V. Dann ist v_i Linearkombination der anderen Mitglieder. Nach a) ist die Familie $(v_j)_{j\in I}$ linear abhängig, also keine Basis.
"iii) $\Rightarrow$ i)": Indirekter Beweis. Annahme: die Familie ist linear abhängig. Nach a) gibt es ein v_i, das Linearkombination der anderen Mitglieder ist. Dies v_i kann man weglassen; die Familie $(v_j)_{j\in I-\{i\}}$ ist immer noch ein Erzeugendensystem von V.
"i) $\Rightarrow$ iv)": Basis $\Rightarrow$ Linear unabhängig.
Zu zeigen bleibt, daß die Familie maximal linear unabhängig ist. Sei $v_0 \in V$ und $0 \notin I$. Basis $\Rightarrow$ v_0 ist Linearkombination der v_i, $i \in I$. Mit a) folgt, daß $(v_j)_{j\in I\cup\{0\}}$ linear abhängig ist.
"iv) $\Rightarrow$ i)": $(v_i)_{i\in I}$ ist linear unabhängig laut iv). Zu zeigen bleibt, daß es ein Erzeugendensystem ist. Sei $v \in V$ beliebig.
Sei $0 \notin I$ und sei $v_0 := v$. Laut iv) ist $(v_j)_{j\in I\cup\{0\}}$ linear abhängig. Also gibt es eine endliche Menge $J \subset I \cup \{0\}$ und Koeffizienten $\lambda_j \in K$ für $j \in J$, die nicht alle 0 sind und die $0 = \sum_{j\in J} \lambda_j \cdot v_j$ erfüllen. Weil $(v_i)_{i\in I}$ linear unabhängig ist, ist $0 \in J$, *und* es ist $\lambda_0 \neq 0$. Daher ist $v_0 = \sum_{j\in J-\{0\}} \frac{-\lambda_j}{\lambda_0} v_j$. Weil v_0 beliebig war, ist $(v_i)_{i\in I}$ ein Erzeugendensystem. □

Satz 3.15 *a) Hat ein Vektorraum V ein endliches Erzeugendensystem, so erhält man durch Weglassen geeigneter Mitglieder dieser Familie eine Basis von V. Insbesondere hat ein Vektorraum mit endlichem Erzeugendensystem eine endliche Basis.*
b) (Verallgemeinerung von a), ohne Beweis) Jeder Vektorraum hat eine Basis.

Beweis von a): Man läßt so lange Mitglieder des endlichen Erzeugendensystems weg, bis man im Fall iii) von Satz 3.14 b) landet. Dann hat man eine Basis. □

Bemerkungen 3.16 i) Der Beweis von b) ist viel schwieriger. Er benutzt nichttriviale Aussagen aus der Mengenlehre, das *Auswahlaxiom* oder das *Zornsche Lemma*. In dieser Vorlesung werden Sie gebeten, den Satz einfach zu akzeptieren.
ii) Beim $\mathbb{Q}$-Vektorraum $\mathbb{Q}[t]$ kann man eine unendliche Basis angeben, die Familie $(t^i)_{i\in\mathbb{N}\cup\{0\}}$. Die Basis ist *abzählbar unendlich*, d.h. es gibt eine Bijektion von $\mathbb{N}$ auf die Indexmenge $\mathbb{N} \cup \{0\}$.
iii) Nach Satz 3.15 b) hat auch der $\mathbb{Q}$-Vektorraum $\mathbb{R}$ eine Basis $(v_i)_{i\in I}$. Aber hier ist die Basis bzw. die Indexmenge I *überabzählbar*, d.h. sie ist unendlich und es gibt keine Bijektion $\mathbb{N} \to I$ (Beweis: Übung). Es ist unmöglich, die Basis "explizit" anzugeben (das kann man präzisieren).
iv) Tatsächlich haben die Basen von Vektorräumen ohne endliche oder abzählbar unendliche Erzeugendensysteme wenig Bedeutung. Bei ihnen sind

"konvergente Reihen" wichtiger als endliche Linearkombinationen (Definition und Diskussion in Analysis und Funktionalanalysis).
v) (Zu Satz 3.17) Bei einer Basis $(v_i)_{i\in I}$ eines Vektorraums sind alle Mitglieder verschieden wegen Satz 3.14 a). Daher ist die Abbildung $I \to \{v_i \mid i \in I\}$, $i \mapsto v_i$, eine Bijektion, und die Unterscheidung zwischen der Familie $(v_i)_{i\in I}$ und der Menge $\{v_i \mid i \in I\}$ ist nicht so wichtig. Man nennt die Mitglieder v_i der Familie auch *Elemente der Basis.*

Satz/Definition 3.17 *a) (Satz) Hat ein Vektorraum eine endliche Basis, so sind alle Basen endlich und haben gleich viele Elemente.*
b) (Definition) Die Dimension eines K-Vektorraums V ohne endliche Basis ist ∞. Die Dimension eines K-Vektorraums mit einer endlichen Basis ist die Anzahl der Elemente einer Basis. Notation: $\dim_K V \in \{0\} \cup \mathbb{N} \cup \{\infty\}$.
c) (Satz) Ist U ein Untervektorraum eines K-Vektorraums V, so ist $\dim U \leq \dim V$. *Ist* $\dim V < \infty$, *so ist* $\dim U = \dim V \iff U = V$.
d) $\dim K^n = n, \quad \dim K[t] = \infty$.

Beweis: nach Satz 3.18

Satz 3.18 *(Austauschsatz von Steinitz) Sei V ein K-Vektorraum, $(v_1, ..., v_n)$ eine Basis von V und $(w_1, ..., w_k)$ eine linear unabhängige Familie in V. Dann ist $k \leq n$, und es gibt lauter verschiedene Indices $i_1, ..., i_k \in \{1, ..., n\}$, so daß man nach Austauschen von $v_{i_1}, ..., v_{i_k}$ gegen $w_1, ..., w_k$ wieder eine Basis von V erhält.*

Beweis: Fall $V = \{0\}$: $n = 0$, $k = 0$, leere Aussagen. Es bleibt der Fall $V \neq \{0\}$, $n \geq 1$. Nun Induktion nach k. Induktionsanfang: $k = 0$, trivial.
Induktionsschritt, $k - 1 \to k$: Nach Induktionsannahme ist $k - 1 \leq n$, und wir können annehmen, daß bei geeigneter Numerierung der v_i $(w_1, ..., w_{k-1}, v_k, ..., v_n)$ eine Basis von V ist.
Daher gibt es $\lambda_j \in K$, $j = 1, ..., n$ mit

$$w_k = \lambda_1 w_1 + ... + \lambda_{k-1} w_{k-1} + \lambda_k v_k + ... + \lambda_n v_n.$$

Behauptung: $k - 1 < n$, und es gibt ein $j \geq k$ mit $\lambda_j \neq 0$.
Andernfalls wäre w_k eine Linearkombination der $w_1, ..., w_{k-1}$. Dann wäre nach Satz 3.14 a) $(w_1, ..., w_k)$ nicht linear unabhängig. Widerspruch. Also stimmt die Behauptung.
Nach Umnumerieren der $v_k, ..., v_n$ können wir annehmen, daß $\lambda_k \neq 0$ ist. Nun wird v_k gegen w_k ausgetauscht.
Behauptung: $(w_1, ..., w_k, v_{k+1}, ..., v_n)$ ist eine Basis von V.
Daß es ein Erzeugendensystem ist, ist klar: man kann

$$v_k = \frac{1}{\lambda_k} w_k - \frac{\lambda_1}{\lambda_k} w_1 - ... - \frac{\lambda_{k-1}}{\lambda_k} w_{k-1} - \frac{\lambda_{k+1}}{\lambda_k} v_{k+1} - ... - \frac{\lambda_n}{\lambda_k} v_n$$

erzeugen und dann mit v_k alle Elemente von V.
Es ist auch eine Basis: Sei

$$0 = \mu_1 w_1 + ... + \mu_k w_k + \mu_{k+1} v_{k+1} + ... + \mu_n v_n.$$

Zu zeigen ist $\mu_1 = ... = \mu_n = 0$. Die rechte Seite ist gleich zu

$$\begin{aligned}&(\mu_1 + \mu_k\lambda_1)w_1 + ... + (\mu_{k-1} + \mu_k\lambda_{k-1})w_{k-1} + \mu_k\lambda_k v_k \\ &+(\mu_{k+1} + \mu_k\lambda_{k+1})v_{k+1} + ... + (\mu_n + \mu_k\lambda_n)v_n.\end{aligned}$$

$(w_1, ..., w_{k-1}, v_k, ..., v_n)$ ist eine Basis. Daher sind alle Koeffizienten hier gleich Null. Insbesondere ist $\mu_k\lambda_k = 0$. Wegen $\lambda_k \neq 0$ ist $\mu_k = 0$. Daher sind alle $\mu_1 = ... = \mu_n = 0$. Das beendet den Beweis der Behauptung und den Induktionsbeweis. □

Beweis von Satz 3.17: a) Sei $(v_1, ..., v_n)$ eine endliche Basis eines Vektorraums V.
Hätte V eine unendliche Basis, so könnte man aus dieser eine linear unabhängige Teilfamilie mit $k > n$ Mitgliedern auswählen. Widerspruch zum Austauschsatz. Also ist jede Basis von V endlich.
Ist $(w_1, ..., w_l)$ eine endliche Basis, so ist sie eine linear unabhängige Familie. Also ist nach dem Austauschsatz $l \leq n$. Genauso folgt $n \leq l$. Also ist $l = n$.
b) Definition.
c) Im Fall $\dim_K V = \infty$ ist nichts zu zeigen. Sei $\dim_K V = n \in \mathbb{N}_0$. Wie in a) folgt, daß U keine unendliche Basis hat. Ist $(w_1, ..., w_l)$ eine Basis von U, so ist sie eine linear unabhängige Familie in V. Nach dem Austauschsatz ist $l \leq n$.
Wäre $l = n$, aber $U \neq V$, so gäbe es ein $w_{l+1} \in V - U$. Die Familie $(w_1, ..., w_l, w_{l+1})$ wäre linear unabhängig. Nach dem Austauschsatz wäre $l + 1 \leq n$. Widerspruch.
d) Mit 3.13 i) und ii). □

Manchmal ist folgender Satz nützlich.

Satz 3.19 *(Basisergänzungssatz)*
Sei V ein endlichdimensionaler K-Vektorraum mit $\dim_K V = n$. Sei $(w_1, ..., w_k)$ eine linear unabhängige Familie in V mit $k \leq n$.
Dann gibt es $w_{k+1}, ..., w_n$, so daß $(w_1, ..., w_n)$ eine Basis von V ist.

Beweis: Man wählt irgendeine Basis $(v_1, ..., v_n)$, tauscht nach dem Austauschsatz geeignete Elemente der Basis gegen $w_1, ..., w_k$ aus und benennt die anderen um in $w_{k+1}, ..., w_n$. □

4 Matrizen

In diesem Kapitel bezeichnet K stets irgendeinen Körper.

Notation/Definition 4.1 a) Sei X eine nichtleere Menge und seien $m, n \in \mathbb{N}$. Eine $(m \times n)$-*Matrix A mit Einträgen in X* besteht aus der folgenden Anordnung von $m \cdot n$ Elementen $a_{ij} \in X$, für $i = 1, ..., m$, $j = 1, ..., n$, in einem rechteckigen Schema mit Klammern drumherum:

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}.$$

Eine kürzere Schreibweise ist $A = (a_{ij})_{i=1,...,m;j=1,...,n}$; wenn klar ist, von wo bis wo i und j laufen, schreibt man auch einfach $A = (a_{ij})$. Die *i-te Zeile* von A ist $(a_{i1} \ \cdots \ a_{in})$, die j-te Spalte ist

$$\begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}.$$

Der erste Index des *Koeffizienten* a_{ij} (also i hier) ist der Zeilenindex, der zweite Index (also j hier) ist der Spaltenindex. Der Koeffizient a_{ij} steht in der i-ten Zeile und j-ten Spalte.
Die Einträge einer Matrix A werden auch mit $(A)_{ij}$ bezeichnet; also hier $(A)_{ij} = a_{ij}$. Skizze in der Vorlesung

b) Die Menge aller $(m \times n)$-Matrizen mit Koeffizienten in X heißt $M(m \times n, X)$. Ist $X = K$ ein Körper, so ist sie (natürlich) ein K-Vektorraum der Dimension $m \cdot n$. Die Elemente von $M(m \times 1, K)$ heißen *Spaltenvektoren*. Die Elemente von $M(1 \times n, K)$ heißen *Zeilenvektoren*.

c) Der Vektorraum $M(1 \times n, K)$ der Zeilenvektoren $(a_1 \cdots a_n)$ wird mit dem Vektorraum K^n der n-Tupel $(a_1, ..., a_n)$ identifiziert. Vorsicht: bei Tupeln stehen Kommata zwischen den Einträgen, bei Zeilenvektoren eigentlich nicht. Wir benutzen im Text überwiegend die Notation mit Kommata, in Formeln immer die Notation ohne Kommata.

d) Die Zeilen $v_i := (a_{i1}, ..., a_{in})$ einer $(m \times n)$-Matrix $A = (a_{ij})$ erzeugen einen Untervektorraum $\operatorname{span}(v_i)_{i \in \{1,...,m\}}$ des K-Vektorraums $K^n = M(1 \times n, K)$. Der *Zeilenrang* von A ist

$$\text{Zeilenrang}(A) := \dim_K \operatorname{span}(v_i)_{i \in \{1,...,m\}}.$$

Analog ist der *Spaltenrang* von A

$$\text{Spaltenrang}(A) := \dim_K \text{span}_K(\begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix}, ..., \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix})$$

die Dimension des von den Spalten von A erzeugten Untervektorraums von $M(m \times 1, K)$.

e) Eine $(m \times n)$-Matrix läßt sich verschieden interpretieren:
1.: Eine Liste von Elementen des Vektorraums $K^n = M(1 \times n, K)$ von Zeilenvektoren (untereinandergeschrieben).
2.: Eine Liste von Elementen des Vektorraums $M(m \times 1, K)$ von Spaltenvektoren (nebeneinandergeschrieben).
3., in Kapitel 5: Eine *lineare Abbildung* von $M(n \times 1, K)$ nach $M(m \times 1, K)$.
4., in LA II: Eine *Bilinearform* auf $M(n \times 1, K)$, falls $m = n$.

Satz 4.2 *Sei $A \in M(m \times n, K)$. Es ist*

$$\text{Zeilenrang}(A) = \text{Spaltenrang}(A).$$

Beweis: in Kapitel 5.

Bemerkungen 4.3 i) In der Literatur wird auch öfters $M(m \times 1, K)$ mit K^m identifiziert, aber nicht in dieser Vorlesung.
ii) Wenn eine Matrix gegeben ist, möchte man den Zeilenrang bestimmen und ein besonders übersichtliches Erzeugendensystem des Vektorraums finden, der von den Zeilen erzeugt wird. Im folgenden wird dazu ein Algorithmus angegeben, der in mehreren Schritten neue Matrizen konstruiert, deren Zeilen Linearkombinationen der Ausgangsmatrix sind, den gleichen Vektorraum erzeugen und einfacher aussehen.

Definition/Lemma 4.4 *a)* (Definition) Sei $\lambda \in K - \{0\}$, $i, j \in \{1, ..., m\}$, $i \neq j$. Die folgenden Abbildungen $Z_I(\lambda, i)$, $Z_{II}(\lambda; i, j)$ und $Z_{III}(i, j)$ von $M(m \times n, K)$ auf $M(m \times n, K)$ heißen *elementare Zeilenumformungen.* Die i-te Zeile einer Matrix $A = (a_{ij}) \in M(m \times n, K)$ wird $v_i := (a_{i1}, ..., a_{in})$ genannt.

$Z_I(\lambda; i)$ ersetzt die i-te Zeile v_i durch $\lambda \cdot v_i$.

$Z_{II}(\lambda; i, j)$ ersetzt die j-te Zeile v_j durch $v_j + \lambda \cdot v_i$.

$Z_{III}(i, j)$ vertauscht die i-te und j-te Zeile.

b) (Lemma) Die Zeilen einer Matrix A erzeugen den gleichen Untervektorraum von $K^n = M(1 \times n, K)$ wie die Zeilen einer Matrix, die man aus A durch eine Folge von elementaren Zeilenumformungen erhält.

Beweis: a) Definition. b) Im Fall einer einzigen Zeilenumformung ist es klar. Der allgemeine Fall folgt mit Induktion. □

Beispiel 4.5

$$\begin{pmatrix} 0 & 1 & 3 & 0 \\ 1 & 2 & 2 & -1 \\ 3 & 4 & 0 & 3 \end{pmatrix} \overset{Z_{III}(1,2)}{\longrightarrow} \begin{pmatrix} 1 & 2 & 2 & -1 \\ 0 & 1 & 3 & 0 \\ 3 & 4 & 0 & 3 \end{pmatrix}$$

$$\overset{Z_{II}(-3;1,3)}{\longrightarrow} \begin{pmatrix} 1 & 2 & 2 & -1 \\ 0 & 1 & 3 & 0 \\ 0 & -2 & -6 & 6 \end{pmatrix} \overset{Z_{II}(2;2,3)}{\longrightarrow} \begin{pmatrix} 1 & 2 & 2 & -1 \\ 0 & 1 & 3 & 0 \\ 0 & 0 & 0 & 6 \end{pmatrix}.$$

Definition 4.6 Eine Matrix $A = (a_{ij}) \in M(m \times n, K)$ ist in *Zeilenstufenform*, wenn ihre Zeilen $v_i := (a_{i1}, ..., a_{in})$ folgendes erfüllen:

i) Es gibt ein $k \in \{0, 1, .., m\}$, so daß $v_i = 0$ für $i > k$ (leere Bedingung bei $k = m$) und $v_i \neq 0$ für $i \leq k$ (leere Bedingung bei $k = 0$) ist.

ii) Für $i \leq k$ sei $j_{min}(i) := \min(j \mid a_{ij} \neq 0)$. Dann ist

$$j_{min}(1) < ... < j_{min}(k).$$

Skizze in der Vorlesung

Satz 4.7 *(Gauß-Algorithmus)*
a) Ist eine Matrix A in Zeilenstufenform, so daß genau die ersten k Zeilen nicht verschwinden, so bilden diese eine Basis des von ihnen erzeugten Untervektorraums, und es ist Zeilenrang$(A) = k$.

b) Jede Matrix $A = (a_{ij}) \in M(m \times n, K)$ läßt sich durch eine geeignete Folge von elementaren Zeilenumformungen in Zeilenstufenform bringen. Der von den Zeilen erzeugte Unterraum bleibt dabei gleich. Also bleibt auch der Zeilenrang gleich.
Genauer: Die Aneinanderkettung von Schritten folgenden Typs gibt eine eindeutige Folge von elementaren Zeilenumformungen, die es tut.
1. Schritt:

$$\begin{aligned} j_1 &:= \min(j \mid \text{ es gibt ein } i \text{ mit } a_{ij} \neq 0), \\ i_1 &:= \min(i \mid a_{ij_1} \neq 0). \end{aligned}$$

Ist $i_1 \neq 1$, so führt man zuerst $Z_{III}(1, i_1)$ aus. Die neue Matrix (= alte Matrix A bei $i_1 = 1$) nennt man $\widetilde{A} = (\widetilde{a}_{ij})$. Für $i = 2, ..., m$ führt man $Z_{II}(-\widetilde{a}_{i,j_1}/\widetilde{a}_{1,j_1}; 1, i)$ aus.

2. Schritt: *Man streicht die erste Zeile und die ersten j_1 Spalten und führt den 1. Schritt mit der neuen kleineren Matrix aus.*
Skizzen in der Vorlesung

Beweis: a) Zu zeigen ist nur, daß die ersten k Zeilen $v_i := (a_{i1}, ..., a_{in})$ linear unabhängig sind. Sei $0 = \sum_{i=1}^{k} \lambda_i v_i$. Es ist $0 = \sum_{i=1}^{k} \lambda_i a_{ij_{min}(1)} = \lambda_1 a_{ij_{min}(1)}$, also $\lambda_1 = 0$. Analog folgt $\lambda_2 = 0$, ..., $\lambda_k = 0$.
b) Die ersten $j_1 - 1$ Spalten von A und $\widetilde{A}$ sind Null. Offenbar ist $\widetilde{a}_{1j_1} \neq 0$. Nach dem ersten Schritt ist $\widetilde{a}_{1j_1}$ der einzige Eintrag in der j_1-ten Spalte ungleich Null. Der Rest ist klar. (Am Ende wird $j_1 = j_{min}(1)$ sein.) □

Bemerkungen 4.8 i) Selbstverständlich kann man in konkreten Beispielen von der Schrittfolge oben abweichen, wenn andere Zeilenumformungen günstiger sind.
ii) Statt Zeilen kann man in 4.4, 4.6 und 4.7 genausogut Spalten betrachten: Man hat den von den Spalten einer Matrix erzeugten Untervektorraum von $M(m \times 1, K)$, *elementare Spaltenumformungen* $S_I(\lambda; i), S_{II}(\lambda, i, j), S_{III}(i, j)$, eine Spaltenstufenform und dafür einen Gauß-Algorithmus.
Skizze in der Vorlesung

Definition 4.9 (Matrizen-Multiplikation) Seien $A \in M(l \times m, K)$ und $B \in M(m \times n, K)$ $(l, m, n \in \mathbb{N})$ Matrizen mit

$$(\text{Anzahl der Spalten von } A) = m = (\text{Anzahl der Zeilen von } B).$$

Das *Produkt* $C := A \cdot B$ von A und B ist die $(l \times n)$-Matrix $C = (c_{ik})_{i=1,...,l;k=1,...,n}$ mit

$$c_{ik} := \sum_{j=1}^{m} a_{ij} \cdot b_{jk}.$$

Also

$$(l \times m)\text{-Matrix} \cdot (m \times n)\text{-Matrix} = (l \times n)\text{-Matrix}.$$

Skizze in der Vorlesung
Eine Anschauung dazu: man dreht die k-te Spalte von B mathematisch positiv um 90 Grad, legt sie auf die i-te Zeile von A, multipliziert aufeinanderliegende Koeffizienten, summiert die Produkte und erhält c_{ik}.

Beispiele 4.10 i)

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & -1 & 3 \\ 0 & 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & -1 & 3 \\ 0 & 1 & 3 & 2 \\ 1 & 2 & 5 & 7 \end{pmatrix}.$$

ii) Die i-te Zeile von A (in Definition 4.1 b)) und die k-te Spalte von B sind auch Matrizen; ihr Produkt ist die 1×1-Matrix mit Koeffizient c_{ik}:

$$\begin{pmatrix} a_{i1} & \cdots & a_{im} \end{pmatrix} \cdot \begin{pmatrix} b_{1k} \\ \vdots \\ b_{mk} \end{pmatrix} = (\sum_{j=1}^{m} a_{ij} \cdot b_{jk}).$$

Also: Zeilenvektor $\cdot$ Spaltenvektor $= 1 \times 1$-Matrix.
iii) Spaltenvektor $\cdot$ Zeilenvektor $= l \times n$-Matrix:

$$\begin{pmatrix} a_{11} \\ \vdots \\ a_{l1} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & \cdots & b_{1n} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & \cdots & a_{11}b_{1n} \\ \vdots & \ddots & \vdots \\ a_{l1}b_{11} & \cdots & a_{l1}b_{1n} \end{pmatrix}.$$

iv) Das *Kroneckersymbol* δ_{ij} für i und j in einer (gegebenen) Indexmenge ist

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

Die $(n \times n)$-*Einheitsmatrix* E_n hat die Einträge $(E_n)_{ij} := \delta_{ij}$, also Einsen in der Diagonalen, Nullen außerhalb. Es ist für $A \in M(m \times n, K)$

$$E_m \cdot A = A = A \cdot E_n.$$

v) Die Zeilen einer Produktmatrix $A \cdot B$ sind Linearkombinationen der Zeilen der rechten Matrix B, die Spalten von $A \cdot B$ sind Linearkombinationen der Spalten der linken Matrix A.
Skizzen in der Vorlesung
vi) Daher lassen sich die elementaren Zeilenumformungen

$$Z_I(\lambda; i), Z_{II}(\lambda, i, j), Z_{III}(i, j) : M(m \times n, K) \to M(m \times n, K)$$

durch Multiplikation von links mit geeigneten Matrizen $Z_I^{mat}(\lambda, i), Z_{II}^{mat}(\lambda, i, j), Z_{III}^{mat}(i, j) \in M(m \times m, K)$ beschreiben:

$$Z_I(\lambda; i)(A) \;=\; Z_I^{mat}(\lambda; i) \cdot A = \begin{pmatrix} 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & \cdot & & & & & \cdot \\ \cdot & & 1 & & & & \cdot \\ \cdot & & & \lambda & & & \cdot \\ \cdot & & & & 1 & & \cdot \\ \cdot & & & & & \cdot & 0 \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 & 1 \end{pmatrix} \cdot A,$$

$$Z_{II}(\lambda,i,j)(A) = Z_{II}^{mat}(\lambda,i,j)\cdot A = \begin{pmatrix} 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & \cdot & & & & & \cdot \\ \cdot & & 1 & & & & \cdot \\ \cdot & & & \cdot & & & \cdot \\ \cdot & & \lambda & & 1 & & \cdot \\ \cdot & & & & & \cdot & 0 \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 & 1 \end{pmatrix} \cdot A,$$

$$Z_{III}(i,j)(A) = Z_{III}^{mat}(i,j)\cdot A = \begin{pmatrix} 1 & 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & \cdot & & & & & \cdot \\ \cdot & & 0 & & 1 & & \cdot \\ \cdot & & & 1 & & & \cdot \\ \cdot & & 1 & & 0 & & \cdot \\ \cdot & & & & & \cdot & 0 \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 & 1 \end{pmatrix} \cdot A;$$

hier ist

$$(Z_I^{mat}(\lambda;i))_{kl} = \begin{cases} \delta_{kl} & \text{für } (k,l) \neq (i,i) \\ \lambda & \text{für } (k,l) = (i,i), \end{cases}$$

$$(Z_{II}^{mat}(\lambda;i,j))_{kl} = \begin{cases} \delta_{kl} & \text{für } (k,l) \neq (j,i) \\ \lambda & \text{für } (k,l) = (j,i), \end{cases}$$

$$(Z_{III}^{mat}(i,j))_{kl} = \begin{cases} \delta_{kl} & \text{für } (k,l) \notin \{(i,i),(i,j),(j,i),(j,j)\}, \\ 1 & \text{für } (k,l) \in \{(i,j),(j,i)\}, \\ 0 & \text{für } (k,l) \in \{(i,i),(j,j)\}. \end{cases}$$

vii) Analog lassen sich die elementaren Spaltenumformungen (Bemerkung 4.8 ii)) durch Multiplikation von rechts mit geeigneten Matrizen beschreiben.

Satz 4.11 *a) Die Multiplikation von Matrizen ist im allgemeinen nicht kommutativ.*
b) Aber sie ist assoziativ: Sind $A \in M(k\times l,K)$, $B \in M(l\times m,K)$, $C \in M(m\times n,K)$, *so ist*

$$(A\cdot B)\cdot C = A\cdot(B\cdot C).$$

c) Die Menge $M(n\times n,K)$ *ist ein Ring mit Eins. Die Eins ist* E_n. *Für* $n \geq 2$ *ist der Ring nicht kommutativ.*

Beweis: a) Wenn $A \in M(p\times q,K)$ und $B \in M(q\times r,K)$ ist mit $p \neq r$, so existiert $B\cdot A$ nicht einmal. Bei $p = q = r = 2$ ist zum Beispiel

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\cdot\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\cdot\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}.$$

b) Es ist (mit der Notation $(A)_{ij}$ für die Koeffizienten einer Matrix A)

$$\begin{aligned}((A\cdot B)\cdot C)_{il} &\overset{\text{Def.}}{=} \sum_{k=1}^{m}(A\cdot B)_{ik}\cdot(C)_{kl}\\ &\overset{\text{Def.}}{=} \sum_{k=1}^{m}\left(\sum_{j=1}^{l}(A)_{ij}(B)_{jk}\right)\cdot(C)_{kl}\\ &\overset{!}{=} \sum_{j=1}^{l}(A)_{ij}\cdot\left(\sum_{k=1}^{m}(B)_{jk}(C)_{kl}\right)\\ &\overset{\text{Def.}}{=} \sum_{j=1}^{l}(A)_{ij}\cdot(B\cdot C)_{jl} \overset{\text{Def.}}{=} (A\cdot(B\cdot C))_{il}.\end{aligned}$$

c) Distributivgesetze: Übung. Der Rest folgt aus a) und b). □

Definition/Lemma 4.12 *a) (Definition) Eine quadratische Matrix $A = (a_{ij}) \in M(n\times n, K)$ ist eine obere Dreiecksmatrix, falls $a_{ij} = 0$ ist für $i > j$.* Skizze in der Vorlesung
b) (Lemma) Eine obere Dreiecksmatrix $A = (a_{ij}) \in M(n\times n, K)$ hat genau dann Zeilenrang n, wenn alle Diagonaleinträge a_{ii} ungleich 0 sind.

Beweis: a) Definition. b) "⇐": Dann ist A in Zeilenstufenform und Zeilenrang$(A) = n$ nach Satz 4.7 a).
"⇒": Indirekter Beweis. Annahme: $a_{i_0i_0} = 0$ und $a_{ii} \neq 0$ für $1 \leq i < i_0$.
Die hinteren $n - (i_0 - 1)$ Zeilen liegen im $n - i_0$ dimensionalen Unterraum $\{(x_1, ..., x_n) \mid x_1 = ... = x_{i_0} = 0\}$ von K^n. Zusammen mit den ersten $i_0 - 1$ Zeilen erzeugen sie einen höchstens $n-1$ dimensionalen Unterraum von K^n. Also ist Zeilenrang$(A) \leq n - 1$. Skizze in der Vorlesung □

Satz/Definition 4.13 *a) (Satz) Sei $A \in M(n\times n, K)$ eine quadratische Matrix. Die folgenden Bedingungen sind äquivalent.*

i) Zeilenrang$(A) = n$.

ii) Es gibt eine Matrix $B \in M(n\times n, K)$ mit $B\cdot A = E_n$.

iii) Es gibt genau eine Matrix $B \in M(n\times n, K)$ mit $B\cdot A = E_n$, und sie erfüllt auch $A\cdot B = E_n$.

b) (Definition) Eine quadratische Matrix, die die Eigenschaften in a) erfüllt, heißt invertierbar. Dann heißt die Matrix B in iii) die inverse Matrix zu A und wird mit A^{-1} bezeichnet.
*c) (Definition/Satz) Die Menge $GL(n, K)$ aller invertierbaren Matrizen in $M(n\times n, K)$ ist eine Gruppe. Für $n \geq 2$ ist sie nicht abelsch. Es ist $(A\cdot B)^{-1} = B^{-1}\cdot A^{-1}$. ("GL" steht für "**g**eneral **l**inear (group)".)*

d) (Satz) Eine obere Dreiecksmatrix ist genau dann invertierbar, wenn alle Diagonaleinträge ungleich 0 sind.
e) (Satz, wichtige Formel, auswendig lernen) Eine (2×2)*-Matrix* $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ *ist genau dann invertierbar, wenn* $ad - bc \neq 0$ *ist. Dann ist*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Beweis: a) "i) $\Rightarrow$ ii)": Es reicht zu zeigen, daß A durch Zeilenumformungen in E_n transformiert werden kann. Denn jede Zeilenumformung ist eine Multiplikation mit einer Matrix von links (Bemerkung 4.10 vi)). Wegen der Assoziativität der Multiplikation ist dann B das Produkt der Matrizen zu den Zeilenumformungen.
Mit dem Gauß-Algorithmus (Satz 4.7) erhält man eine Matrix $\widetilde{A}$ in Zeilenstufenform aus A. Wegen Zeilenrang$(\widetilde{A})$ = Zeilenrang$(A) = n$ und Lemma 4.12 sind alle Diagonaleinträge ungleich 0. Mit Zeilenumformungen vom Typ I normiert man sie zu 1. Mit Zeilenumformungen vom Typ II löscht man alle Einträge oberhalb der Diagonalen. Skizzen in der Vorlesung
"ii) $\Rightarrow$ iii)": Aus $B \cdot (A \cdot B) = (B \cdot A) \cdot B = E_n \cdot B = B$ folgt $B \cdot (A \cdot B - E_n) = 0$. Es ist Spaltenrang$(B) \geq$ Spaltenrang$(B \cdot A) = n$, also Spaltenrang$(B) = n$. Also bilden die Spalten von B eine Basis von $M(n \times 1, K)$. Daher ist $A \cdot B - E_n = 0$, also $A \cdot B = E_n$.
Ist $\widetilde{B} \cdot A = E_n$, so ist $B = (\widetilde{B} \cdot A) \cdot B = \widetilde{B} \cdot (A \cdot B) = \widetilde{B}$.
"iii) $\Rightarrow$ i)": Es ist Zeilenrang$(A) \geq$ Zeilenrang$(B \cdot A) = n$, also Zeilenrang$(A) = n$.
b) Definition.
c) Multiplikation assoziativ: 4.11 b); E_n neutrales Element: 4.10 iv); inverse Elemente: 4.13 a). $GL(n, K)$ nicht abelsch: siehe Beweis von Satz 4.11 a). $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$ gilt wegen

$$(A \cdot B) \cdot (B^{-1} \cdot A^{-1}) = A \cdot (B \cdot B^{-1}) \cdot A^{-1} = A \cdot A^{-1} = E_n.$$

d) Lemma 4.12 b).
e) Bei $ad - bc = 0$ ist eine Zeile (falls eine gleich 0 ist, nur die) Linearkombination der anderen. Formel: nachrechnen. □

Bemerkung 4.14 Aus dem Beweis von "i) $\Rightarrow$ ii)" erhält man einen Algorithmus zur Berechnung der inversen Matrix: Man schreibt A und E_n nebeneinander und führt an beiden die gleichen Zeilenumformungen durch, so daß man E_n aus A erhält. Dann erhält man A^{-1} aus E_n.
Denn sind $Z_1, ..., Z_k$ die Matrizen zu den Zeilenumformungen (Beispiel 4.10 vi)), so ist $Z_k \cdot ... \cdot Z_1 \cdot A = E_n$, also $Z_K \cdot ... \cdot Z_1 \cdot E_n = A^{-1}$.

Ein Beispiel: (die Zeilenumformungen sind nach Gefühl gewählt, nicht strikt nach dem Gauß-Algorithmus)

$$A = \begin{pmatrix} 0 & 1 & 2 \\ 3 & 4 & 5 \\ 6 & 7 & 9 \end{pmatrix} \quad , \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = E_n$$

$$Z_{II}(-1;1,3) \circ Z_{II}(-1;1,2): \quad \begin{pmatrix} 0 & 1 & 2 \\ 3 & 3 & 3 \\ 6 & 6 & 7 \end{pmatrix} \quad , \quad \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix}$$

$$Z_{II}(-2;2,3): \quad \begin{pmatrix} 0 & 1 & 2 \\ 3 & 3 & 3 \\ 0 & 0 & 1 \end{pmatrix} \quad , \quad \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 1 & -2 & 1 \end{pmatrix}$$

$$Z_{III}(1,2): \quad \begin{pmatrix} 3 & 3 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \quad , \quad \begin{pmatrix} -1 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & -2 & 1 \end{pmatrix}$$

$$Z_I(\frac{1}{3};1): \quad \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \quad , \quad \begin{pmatrix} -\frac{1}{3} & \frac{1}{3} & 0 \\ 1 & 0 & 0 \\ 1 & -2 & 1 \end{pmatrix}$$

$$Z_{II}(-1;3,1) \circ Z_{II}(-2;3,2): \quad \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad , \quad \begin{pmatrix} -\frac{4}{3} & \frac{7}{3} & -1 \\ -1 & 4 & -2 \\ 1 & -2 & 1 \end{pmatrix}$$

$$Z_{II}(-1;2,1): \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad , \quad \begin{pmatrix} -\frac{1}{3} & -\frac{5}{3} & 1 \\ -1 & 4 & -2 \\ 1 & -2 & 1 \end{pmatrix} = A^{-1}$$

Definition/Lemma 4.15 *a) Die transponierte Matrix A^{tr} einer Matrix $A = (a_{ij}) \in M(k \times l, K)$ ist die Matrix $A^{tr} \in M(l \times k, K)$ mit*

$$(A^{tr})_{ij} := a_{ji}.$$

b) Ist $A \in M(k \times l, K)$ und $B \in M(l \times m, K)$, so ist

$$(A \cdot B)^{tr} = B^{tr} \cdot A^{tr}.$$

Beweis: a) Definition. b) Übung. Skizze in der Vorlesung □

5 Lineare Abbildungen

In diesem Kapitel bezeichnet K stets irgendeinen Körper.

Definition 5.1 a) Eine Abbildung $f : V \to W$ von einem K-Vektorraum V in einen K-Vektorraum W heißt *linear* (oder *K-linear*), falls sie folgende Eigenschaften erfüllt:

i) f ist ein Gruppenhomomorphismus von $(V, +)$ nach $(W, +)$, d.h.

$$f(a + b) = f(a) + f(b) \quad \text{für } a, b \in V;$$

ii) f ist kompatibel mit den skalaren Multiplikationen von V und W, d.h.

$$f(\lambda \cdot a) = \lambda \cdot f(a) \quad \text{für } \lambda \in K, a \in V.$$

Ein anderer (seltener benutzter) Name für *lineare Abbildung* ist *Vektorraumhomomorphismus*.
b) Eine lineare Abbildung $f : V \to W$ zwischen zwei Vektorräumen ist
ein *Isomorphismus*, falls sie bijektiv ist,
ein *Endomorphismus*, falls $V = W$ ist,
ein *Automorphismus*, falls sie bijektiv ist und $V = W$ ist.
c) Zwei Vektorräume V und W heißen *isomorph*, wenn ein Isomorphismus $f : V \to W$ existiert.

Beispiele 5.2 i) Der einfachste Fall: $f : \mathbb{R} \to \mathbb{R}, \quad x \mapsto a \cdot x$, für ein $a \in \mathbb{R}$.
Skizze in der Vorlesung
ii) (Verallgemeinerung von i)) $f : \mathbb{R}^n \to \mathbb{R}, \quad (x_1, ..., x_n) \mapsto \sum_{j=1}^{n} a_j x_j$, für $a_1, ..., a_n \in \mathbb{R}$.
iii) (Äquivalent zu ii)) $f : M(n \times 1, \mathbb{R}) \to M(1 \times 1, \mathbb{R})$,

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} a_1 \cdots a_n \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (\sum_{i=1}^{n} a_i x_i)$$

für $a_1, ..., a_n \in \mathbb{R}$.
iv) (Verallgemeinerung von iii), mit K statt $\mathbb{R}$)
Sei $A = (a_{ij}) \in M(m \times n, K)$. Die Abbildung

$$\begin{array}{rcl} f : M(n \times 1, K) & \to & M(m \times 1, K), \\ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} & \mapsto & \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^{n} a_{1i} x_i \\ \vdots \\ \sum_{i=1}^{n} a_{mi} x_i \end{pmatrix} \end{array}$$

ist linear. Beweis: Details im Kopf; man muß 5.1 i) und ii) zeigen. Mit $x \in M(n \times 1, K)$ läßt sich die Abbildung ganz kurz schreiben als

$$x \mapsto A \cdot x.$$

In Satz 5.5 a)+b) und Satz 5.11 a)+b) werden wir sehen, daß jede lineare Abbildung von $M(n \times 1, K)$ nach $M(m \times 1, K)$ von dieser Gestalt ist und daß jede lineare Abbildung zwischen endlich-dimensionalen Vektorräumen "äquivalent" zu einer solchen Abbildung ist.
v) Sei X eine nichtleere Menge, $x_0 \in X$, K ein Körper. Die Einsetzungsabbildung

$$\Phi_{x_0} : \mathrm{Abb}(X, K) \to K, \quad g \mapsto g(x_0)$$

ist eine lineare Abbildung.
vi) Die Mengen $\mathcal{C}^0([0,1], \mathbb{R})$, $\mathcal{C}^1([0,1], \mathbb{R})$ und $\mathbb{R}[t]$ sind $\mathbb{R}$-Vektorräume (Beispiel 3.3 d)). Die Ableitung

$$\frac{\mathrm{d}}{\mathrm{d}x} : \mathcal{C}^1([0,1], \mathbb{R}) \to \mathcal{C}^0([0,1], \mathbb{R}), \quad g \mapsto \frac{\mathrm{d}g}{\mathrm{d}x}$$

ist linear, ebenso ihre Einschränkung $\frac{\mathrm{d}}{\mathrm{d}x} : \mathbb{R}[x] \to \mathbb{R}[x], \quad g \mapsto \frac{\mathrm{d}g}{\mathrm{d}x}$.

Satz/Definition 5.3 *Sei $f : V \to W$ eine lineare Abbildung zwischen K-Vektorräumen*
a) (Satz) Dann ist $f(\sum_{i=1}^n \lambda_i v_i) = \sum_{i=1}^n \lambda_i f(v_i)$ für $n \in \mathbb{N}$, $\lambda_1, ..., \lambda_n \in K$, $v_1, ..., v_n \in V$.
b) (Definition) Der Kern von f ist $\ker f := \{x \in V \mid f(x) = 0\}$. *Das Bild ist $f(V) \subset W$.*
c) (Satz) $\ker f$ *ist ein Untervektorraum von V, $f(V)$ ist ein Untervektorraum von W.*
d) (Satz) f ist genau dann injektiv, wenn $\ker f = \{0\}$ *ist (und f ist nach Definition genau dann surjektiv, wenn $f(V) = W$ ist).*
e) (Satz) Ist f ein Isomorphismus, so ist auch die (natürlich ebenfalls bijektive) Umkehrabbildung $f^{-1} : W \to V$ linear und damit ein Isomorphismus von Vektorräumen.
f) (Definition) Der Rang von f ist $\mathrm{rang}\, f := \dim_K f(V)$.
g) (Satz)

$$\dim_K V = \dim_K \ker f + \mathrm{rang}\, f$$

(mit $\infty = \infty + n = n + \infty = \infty + \infty$ für $n \in \mathbb{N}_0$).
h) (Satz) Ist $g : U \to V$ eine zweite lineare Abbildung zwischen K-Vektorräumen, so ist auch die Komposition $f \circ g : U \to W$ eine lineare Abbildung.

Beweis: a) Klar. b) Definition. c) Nach Lemma 1.22 sind $\ker f$ und $f(V)$ Untergruppen von V bzw. W. Es bleibt zu zeigen, daß sie abgeschlossen unter der skalaren Multiplikation sind:

$$\begin{aligned} v_1 \in \ker f, \lambda \in K &\Rightarrow f(\lambda \cdot v_1) = \lambda \cdot f(v_1) = \lambda \cdot 0 = 0 \\ &\Rightarrow \lambda \cdot v_1 \in \ker f; \\ v_2 \in V, \lambda \in K &\Rightarrow \lambda \cdot f(v_2) = f(\lambda \cdot v_2) \in f(V). \end{aligned}$$

d) Es ist $f(0) = 0$, denn für ein beliebiges $v \in V$ gilt

$$f(0_V) = f(0_K \cdot v) = 0_K \cdot f(v) = 0_V.$$

"$\Rightarrow$": f injektiv und $f(a) = 0 \Rightarrow a = 0$.
"$\Leftarrow$": $f(a) = f(b) \Rightarrow f(a-b) = 0 \Rightarrow$ (wegen $\ker f = 0$) $a - b = 0 \Rightarrow a = b$.
e) Lemma 1.22 $\Rightarrow f^{-1} : (W, +) \to (V, +)$ ist ein Isomorphismus abelscher Gruppen. Aus $f(\lambda \cdot a) = \lambda \cdot f(a)$ und $a = f^{-1}(b)$ folgt $\lambda \cdot f^{-1}(b) = f^{-1}(\lambda \cdot b)$.
f) Definition.
g) **1. Fall,** $\dim_K \ker f = \infty$:
Nach Satz 3.17 c) ist $\dim V \geq \dim \ker f = \infty$.
2. Fall, $\dim_K f(V) = \infty$:
Wäre $(a_1, ..., a_n)$ ein Erzeugendensystem von V, so wäre $(f(a_1), ..., f(a_n))$ ein Erzeugendensystem von $f(V)$, also $\dim f(V) < \infty$, Widerspruch. Also hat V kein endliches Erzeugendensystem; also ist $\dim V = \infty$.
3. Fall (der interessanteste Fall), $\dim_K \ker f < \infty$ und $\dim_K f(V) < \infty$:
Man wählt eine Basis $(v_1, ..., v_k)$ von $\ker f$, und man wählt $w_1, ..., w_l \in V$, so daß $(f(w_1), ..., f(w_l))$ eine Basis von $f(V)$ ist. Es reicht, folgende Behauptung zu beweisen.
Behauptung: $(v_1, ..., v_k, w_1, ..., w_l)$ ist eine Basis von V.
Beweis: i) Erzeugendensystem: sei $a \in V$. Es gibt $\mu_1, ..., \mu_l \in K$ mit $f(a) = \sum_{j=1}^{l} \mu_j f(w_j)$. Man sieht sofort

$$a - \sum_{j=1}^{l} \mu_j w_j \in \ker f.$$

Also gibt es $\lambda_1, ..., \lambda_k \in K$ mit

$$a - \sum_{j=1}^{l} \mu_j w_j = \sum_{i=1}^{k} \lambda_i v_i.$$

Also ist a eine Linearkombination der v_i und w_j.
ii) Linear unabhängig: Sei $\sum_{i=1}^{k} \alpha_i v_i + \sum_{j=1}^{l} \beta_j w_j = 0$. Sein Bild unter f ist $\sum_{j=1}^{l} \beta_j f(w_j) = 0$. Weil $(f(w_1), ..., f(w_l))$ eine Basis von $f(V)$ ist, sind alle $\beta_j = 0$. Weil $(v_1, ..., v_k)$ eine Basis von $\ker f$ ist, sind auch alle $\alpha_i = 0$.
h) Klar. □

Beispiel 5.4 In Beispiel 5.2 v) ist $\ker \Phi_{x_0} = \{g \in \mathrm{Abb}(X, K) \mid g(x_0) = 0\}$. In Beispiel 5.2 vi) ist $\ker \frac{\mathrm{d}}{\mathrm{d}x} = \{$ konstante Abbildungen.$\}$. In beiden Fällen ist die betrachtete Abbildung surjektiv.

Satz/Definition 5.5 *(Matrizen und lineare Abbildungen, 1. Teil)*
a) (Satz) Zu jeder linearen Abbildung $f : M(n \times 1, K) \to M(m \times 1, K)$ gibt es genau eine Matrix $A \in M(m \times n, K)$ mit

$$f(x) = A \cdot x.$$

(Definition) Diese Matrix wird $\mathrm{Mat}(f)$ *genannt. Also ist $f(x) = \mathrm{Mat}(f) \cdot x$.*
b) (Definition/Satz) Die Menge

$$\begin{aligned} & \mathrm{Hom}_K(M(n \times 1, K), M(m \times 1, K)) \\ := \; & \{f : M(n \times 1, K) \to M(m \times 1, K) \mid f \text{ ist linear}\} \end{aligned}$$

ist ein K-Vektorraum, und die Abbildung

$$Mat : \mathrm{Hom}_K(M(n \times 1, K), M(m \times 1, K)) \to M(m \times n, K), \quad f \mapsto \mathrm{Mat}(f),$$

ist ein Isomorphismus von K-Vektorräumen.
c) Sind

$$f : M(n \times 1, K) \to M(m \times 1, K)$$

und

$$g : M(m \times 1, K) \to M(l \times 1, K)$$

lineare Abbildungen, so ist auch

$$g \circ f : M(n \times 1, K) \to M(l \times 1, K)$$

linear (Satz 5.3), und es ist

$$\mathrm{Mat}(g \circ f) = \mathrm{Mat}(g) \cdot \mathrm{Mat}(f).$$

d) Eine lineare Abbildung $f : M(n \times 1, K) \to M(n \times 1, K)$ ist genau dann ein Isomorphismus, wenn $\mathrm{Mat}(f)$ *invertierbar ist. Dann ist* $\mathrm{Mat}(f^{-1}) = (\mathrm{Mat}(f))^{-1}$.

Beweis: a) Es sei $e_1^{(n)} = (1, 0, ..., 0)^{tr}$,...,$e_n^{(n)} = (0, ..., 0, 1)^{tr}$ die Standardbasis von $M(n \times 1, K)$ und $e_1^{(m)}$,...,$e_m^{(m)}$ die Standardbasis von $M(m \times 1, K)$. Für jedes $e_j^{(n)}$ (mit $j = 1, ..., n$) gibt es *eindeutige* $a_{ij} \in K$ (mit $i = 1, ..., m$) mit

$$f(e_j^{(n)}) = \sum_{i=1}^{m} a_{ij} e_i^{(m)},$$

denn $e_1^{(m)}$,...,$e_m^{(m)}$ ist eine Basis von $M(m \times 1, K)$. Also ist

$$f(e_j^{(n)}) = \sum_{i=1}^{m} a_{ij} e_i^{(m)} = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} = (a_{ij}) \cdot e_j^{(n)}.$$

Daraus folgt schon die Eindeutigkeit der Matrix $A = (a_{ij})$. Es ist

$$\begin{aligned} f\left(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}\right) &= f\left(\sum_{j=1}^{n} x_j e_j^{(n)}\right) = \sum_{j=1}^{n} x_j \cdot f(e_j^{(n)}) \\ &= \sum_{j=1}^{n} x_j \cdot (a_{ij}) \cdot e_j^{(n)} = (a_{ij}) \cdot \left(\sum_{j=1}^{n} x_j e_j^{(n)}\right) = (a_{ij}) \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}. \end{aligned}$$

Das sagt, daß $f(x) = (a_{ij}) \cdot x$ ist.
b) $\mathrm{Mat}(f)$ bestimmt f. Daher ist die Abbildung $f \mapsto \mathrm{Mat}(f)$ injektiv. Sie ist surjektiv, denn die Multiplikation von links mit einer Matrix ist eine lineare Abbildung (Bemerkung 5.2 iv)). Die Abbildung $f \mapsto \mathrm{Mat}(f)$ ist linear:

$$\begin{aligned} (f+g)(x) &\overset{\text{Def.}}{=} f(x) + g(x) = \mathrm{Mat}(f) \cdot x + \mathrm{Mat}(g) \cdot x \\ &= (\mathrm{Mat}(f) + \mathrm{Mat}(g)) \cdot x, \end{aligned}$$

und weil $\mathrm{Mat}(f+g)$ eindeutig ist, ist $\mathrm{Mat}(f+g) = \mathrm{Mat}(f) + \mathrm{Mat}(g)$. Genauso folgt aus

$$(\lambda \cdot f)(x) \overset{\text{Def.}}{=} \lambda \cdot f(x) = \lambda \cdot (\mathrm{Mat}(f) \cdot x) = (\lambda \cdot \mathrm{Mat}(f)) \cdot x,$$

daß $\mathrm{Mat}(\lambda \cdot f) = \lambda \cdot \mathrm{Mat}(f)$ ist.
c) Es ist

$$\begin{aligned} (g \circ f)(x) &= g(f(x)) = g\,(\mathrm{Mat}(f) \cdot x) = \mathrm{Mat}(g) \cdot (\mathrm{Mat}(f) \cdot x) \\ &= (\mathrm{Mat}(g) \cdot \mathrm{Mat}(f)) \cdot x. \end{aligned}$$

Weil $\mathrm{Mat}(g \circ f)$ eindeutig ist, ist

$$\mathrm{Mat}(g \circ f) = \mathrm{Mat}(g) \cdot \mathrm{Mat}(f).$$

d) "$\Rightarrow$": Sei f ein Isomorphismus. Nach Satz 5.3 ist $f^{-1} : M(n \times 1, K) \to M(n \times 1, K)$ linear. Es ist $f^{-1} \circ f = \mathrm{id} = f \circ f^{-1}$. Mit c) folgt

$$\mathrm{Mat}(f^{-1}) \cdot \mathrm{Mat}(f) = \mathrm{Mat}(f^{-1} \circ f) = \mathrm{Mat}(\mathrm{id}) = E_n.$$

Also ist $\mathrm{Mat}(f)$ invertierbar und $\mathrm{Mat}(f^{-1})$ die inverse Matrix.

"$\Leftarrow$": Sei $\mathrm{Mat}(f)$ invertierbar und A die inverse Matrix, also

$$\mathrm{Mat}(f) \cdot A = E_n = A \cdot \mathrm{Mat}(f).$$

Wegen b) gibt es eine eindeutige Abbildung $g : M(n \times 1, K) \to M(n \times 1, K)$ mit $A = \mathrm{Mat}(g)$. (g ist die Multiplikation mit A von links.) Also ist

$$Mat(g \circ f) = \mathrm{Mat}(g) \cdot \mathrm{Mat}(f) = E_n = \mathrm{Mat}(f) \cdot \mathrm{Mat}(g) = \mathrm{Mat}(f \circ g),$$

also

$$g \circ f = \mathrm{id} = f \circ g.$$

Also ist f invertierbar und g das Inverse, und f ist ein Isomorphismus. □

Bemerkungen 5.6 i) Ein Beispiel ist die Abbildung $f : M(2 \times 1, K) \to M(3 \times 1, K)$ mit

$$f(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}) = \begin{pmatrix} 0 & 2 \\ 1 & -1 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 2x_2 \\ x_1 - x_2 \\ 3x_1 + 4x_2 \end{pmatrix}.$$

ii) Im Beweis von c) wurde die Assoziativität der Matrizenmultiplikation benutzt. Umgekehrt folgt aus c) und der Assoziativität der Komposition von Abbildungen, $(h \circ g) \circ f = h \circ (g \circ f)$, die Assoziativität der Matrizenmultiplikation sofort.
iii) Oft hat man lineare Abbildungen zwischen abstrakten endlichdimensionalen Vektorräumen. Um dann Matrizen zu erhalten, muß man Basen der Vektorräume wählen. Eine Korrespondenz ist in Definition 5.8 a) und Satz 5.11 b) formuliert. Ihre Eigenschaften sind in Satz 5.11 diskutiert. Er verallgemeinert Satz 5.5. Mit Lemma 5.10 kann man ihn weitgehend auf Satz 5.5 zurückspielen.

Notation 5.7 (Eine Verallgemeinerung der Matrizenmultiplikation)
Sei V ein K-Vektorraum und $m, n \in \mathbb{N}$. Die Menge V^m wird mit der Menge $M(1 \times m, V)$ der Zeilenvektoren mit Einträgen in V identifiziert (vgl. Notation 4.1 c)). Die Abbildung

$$V^m \times M(m \times n, K) \to V^n,$$
$$((b_1, ..., b_m), (a_{ij})) \mapsto (\sum_{i=1}^{m} a_{i1} b_i, ..., \sum_{i=1}^{m} a_{in} b_i)$$

wird als eine Verallgemeinerung der Matrizenmultiplikation aufgefaßt:

$$(\sum_{i=1}^{m} a_{i1} b_i \cdots \sum_{i=1}^{m} a_{in} b_i) = (b_1 \cdots b_m) \cdot \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}.$$

(Die Verallgemeinerung besteht darin, daß hier $(b_1, ..., b_m)$ Einträge in V und nicht in K hat und daß die Körpermultiplikation durch die skalare Multiplikation ersetzt ist und deshalb die a_{ij} links von den b_i stehen.) Mit $\mathcal{B} := (b_1, ..., b_m) \in V^m = M(1 \times m, V)$ und $A = (a_{ij})$ läßt sich die Abbildung $V^m \times M(m \times n, K) \to V^n$ sehr kurz schreiben als

$$(\mathcal{B}, A) \mapsto \mathcal{B} \cdot A.$$

Definition 5.8 (Matrizen und lineare Abbildungen, 2. Teil)
a) Es sei $f : U \to V$ eine lineare Abbildung zwischen endlich-dimensionalen K-Vektorräumen U und V. Es sei $\mathcal{A} = (a_1, ..., a_n)$ eine Basis von U und $\mathcal{B} = (b_1, ..., b_m)$ eine Basis von V.
Weil $\mathcal{B}$ eine Basis von V ist, gibt es eindeutige Koeffizienten $\lambda_{ij} \in K$ mit

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

Mit der Verallgemeinerung der Matrixmultiplikation oben lassen sich diese Gleichungen für $j = 1, ..., n$ schön kompakt zusammenfassen zu

$$(f(a_1), ..., f(a_n)) = (b_1, ..., b_m) \cdot (\lambda_{ij}).$$

Die Matrix (λ_{ij}) wird $M(\mathcal{B}, f, \mathcal{A})$ genannt. Mit ihrer Hilfe wird das Bild von $\mathcal{A}$ unter f in $\mathcal{B}$ ausgedrückt. Wenn wir (etwas unsauber, aber elegant) $f(\mathcal{A}) := (f(a_1), ..., f(a_n))$ schreiben, wird die Gleichung oben noch kompakter,

$$f(\mathcal{A}) = \mathcal{B} \cdot M(\mathcal{B}, f, \mathcal{A}).$$

b) Im Spezialfall $U = V$ und $f = \mathrm{id}$ heißt die Matrix $M(\mathcal{B}, \mathrm{id}, \mathcal{A})$ *Basiswechselmatrix* und wird auch mit $M(\mathcal{B}, \mathcal{A})$ bezeichnet.

Beispiele 5.9 i) Die Menge $\mathbb{R}[t]_{\leq n} := \{f \in \mathbb{R}[t] \mid \deg f \leq n\}$ ist ein Vektorraum der Dimension $n + 1$ mit Basis $\mathcal{B}_n := (1, t, t^2, ..., t^n)$. Die Ableitung $\frac{\mathrm{d}}{\mathrm{d}t}$ kann man auffassen als eine lineare Abbildung $\mathbb{R}[t]_{\leq n} \to \mathbb{R}[t]_{\leq n-1}$. Für $n = 3$ ist

$$\frac{\mathrm{d}}{\mathrm{d}t} \begin{pmatrix} 1 & t & t^2 & t^3 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2t & 3t^2 \end{pmatrix} = \begin{pmatrix} 1 & t & t^2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix},$$

$$\text{also} \qquad M(\mathcal{B}_2, \frac{\mathrm{d}}{\mathrm{d}t}, \mathcal{B}_3) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}.$$

ii) $\mathbb{C}$ als $\mathbb{R}$-Vektorraum hat die Standardbasis $(1, i)$. Die Multiplikation $m_z : \mathbb{C} \to \mathbb{C}$ mit einer komplexen Zahl $z = |z|e^{i\alpha}$ ist ein Endomorphismus auf $\mathbb{C}$

als $\mathbb{C}$-Vektorraum und erst recht als $\mathbb{R}$-Vektorraum. Wegen $z = |z|\cos\alpha + i|z|\sin\alpha$ und $z \cdot i = -|z|\sin\alpha + i|z|\cos\alpha$ ist

$$\begin{pmatrix} z\cdot 1 & z\cdot i \end{pmatrix} = \begin{pmatrix} 1 & i \end{pmatrix} \cdot \begin{pmatrix} |z|\cos\alpha & -|z|\sin\alpha \\ |z|\sin\alpha & |z|\cos\alpha \end{pmatrix},$$

$$\text{also} \qquad M((1,i), m_z, (1,i)) = \begin{pmatrix} |z|\cos\alpha & -|z|\sin\alpha \\ |z|\sin\alpha & |z|\cos\alpha \end{pmatrix}.$$

iii) Eine Basis des K-Vektorraum $K[t]_{\leq 3}$ ist $\mathcal{B} := (1, t, t^2, t^3)$, eine andere ist $\mathcal{A} := (1+2t, 3-t+2t^2+t^3, 5t^3, t)$. Die Basiswechselmatrizen sind

$$\begin{aligned} M(\mathcal{B},\mathcal{A}) &= \begin{pmatrix} 1 & 3 & 0 & 0 \\ 2 & -1 & 0 & 1 \\ 0 & 2 & 0 & 0 \\ 0 & 1 & 5 & 0 \end{pmatrix} \quad \text{und} \\ M(\mathcal{A},\mathcal{B}) &= M(\mathcal{B},\mathcal{A})^{-1} \quad \text{(vgl. Satz 5.11 e))} \end{aligned}$$

iv) Der K-Vektorraum $M(n\times 1, K)$ hat die Standardbasis

$$\mathcal{B}^{(n)} = (e_1^{(n)}, ..., e_n^{(n)}) = (\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, ..., \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}).$$

Sei $f : M(n\times 1, K) \to M(m\times 1, K)$ eine lineare Abbildung. Die Konstruktion von $\mathrm{Mat}(f)$ im Beweis von Satz 5.5 a) zeigt

$$f(\mathcal{B}^{(n)}) = \mathcal{B}^{(m)} \cdot \mathrm{Mat}(f),$$

also

$$\mathrm{Mat}(f) = M(\mathcal{B}^{(m)}, f, \mathcal{B}^{(n)}).$$

Das gibt eine direkte Beziehung zwischen den Notationen $\mathrm{Mat}(f)$ und $M(\mathcal{B}, f, \mathcal{A})$. Satz 5.11 a) verallgemeinert diese Formel.

Lemma 5.10 *a) Sei V ein n-dimensionaler K-Vektorraum und $\mathcal{B} = (b_1, ..., b_n)$ eine Basis von V. Die Abbildung*

$$l_{\mathcal{B}} : M(n\times 1, K) \to V, \quad x \mapsto \mathcal{B}\cdot x,$$

ist ein Isomorphismus von K-Vektorräumen.
b) Da $M(n\times 1, K)$ natürlich isomorph zu $K^n = M(1\times n, K)$ ist, ist jeder n-dimensionale K-Vektorraum isomorph zu K^n.

Beweis: a) $l_{\mathcal{B}}$ ist bijektiv, denn $\mathcal{B}$ ist eine Basis von V.
$l_{\mathcal{B}}$ ist linear: klar.
b) Klar. □

Satz 5.11 *(Matrizen und lineare Abbildungen, 3. Teil)*
Es seien U und V endlich-dimensionale K-Vektorräume. Es sei $\mathcal{A} = (a_1, ..., a_n)$ eine Basis von U und $\mathcal{B} = (b_1, ..., b_m)$ eine Basis von V.

a) (Bemerkung) Es sei $f : U \to V$ eine lineare Abbildung. Mit den Isomorphismen $l_{\mathcal{A}} : M(n \times 1, K) \to U$ und $l_{\mathcal{B}} : M(m \times 1, K) \to V$ induziert $f : U \to V$ eine lineare Abbildung

$$l_{\mathcal{B}}^{-1} \circ f \circ l_{\mathcal{A}} : M(n \times 1, K) \to M(m \times 1, K).$$

Sie ist gerade so definiert, daß das Diagramm

$$\begin{array}{ccccc} M(n \times 1, K) & \xrightarrow{l_{\mathcal{A}}} & U & , x \mapsto & \mathcal{A} \cdot x \\ \downarrow l_{\mathcal{B}}^{-1} \circ f \circ l_{\mathcal{A}} & & \downarrow f & & \\ M(m \times 1, K) & \xrightarrow{l_{\mathcal{B}}} & V & , y \mapsto & \mathcal{B} \cdot y, \end{array}$$

kommutiert*, d.h. beide Wege von links oben nach rechts unten geben die gleiche Abbildung.*
(Satz) Es ist

$$\mathrm{Mat}(l_{\mathcal{B}}^{-1} \circ f \circ l_{\mathcal{A}}) = M(\mathcal{B}, f, \mathcal{A}).$$

Das heißt, daß die Abbildung f mit Hilfe von $l_{\mathcal{A}}$ und $l_{\mathcal{B}}$ gerade in die Matrixmultiplikation mit $M(\mathcal{B}, f, \mathcal{A})$ übergeht. Die folgende Gleichung sagt dasselbe etwas anders,

$$f(\mathcal{A} \cdot x) = \mathcal{B} \cdot M(\mathcal{B}, f, \mathcal{A}) \cdot x.$$

b) (Verallgemeinerung von Satz 5.5 b)) Die Menge $\mathrm{Hom}_K(U, V) := \{f : U \to V \mid f \text{ ist linear}\}$ ist ein K-Vektorraum, und die Abbildung

$$\mathrm{Hom}_K(U, V) \to M(m \times n, K), \quad f \mapsto M(\mathcal{B}, f, \mathcal{A}),$$

ist ein Isomorphismus von K-Vektorräumen

c) (Verallgemeinerung von Satz 5.5 c)) Ist W ein K-Vektorraum mit einer Basis $\mathcal{C} = (c_1, ..., c_l)$ und sind $f : U \to V$ und $g : V \to W$ linear, so ist auch $g \circ f : U \to W$ linear (Satz 5.3 h)), und es ist

$$M(\mathcal{C}, g \circ f, \mathcal{A}) = M(\mathcal{C}, g, \mathcal{B}) \cdot M(\mathcal{B}, f, \mathcal{A}).$$

d) (Verallgemeinerung von Satz 5.5 d)) Eine Abbildung $f : U \to V$ ist genau dann ein Isomorphismus, wenn die Matrix $M(\mathcal{B}, f, \mathcal{A})$ invertierbar ist. Dann ist $M(\mathcal{B}, f, \mathcal{A})^{-1} = M(\mathcal{A}, f^{-1}, \mathcal{B})$.

e) Im Fall $U = V$ und $f = \mathrm{id}$ heißt $M(\mathcal{B}, \mathrm{id}, \mathcal{A}) =: M(\mathcal{B}, \mathcal{A})$ ja Basiswechselmatrix (Definition 5.8 b)). Sie ist invertierbar; die inverse Matrix ist $M(\mathcal{A}, \mathcal{B})$.

f) Die Menge $\mathrm{End}_K(V) := \mathrm{Hom}_K(V,V)$ *der Endomorphismen von* V *ist ein Ring und ein* K*-Vektorraum. Die Abbildung*

$$\mathrm{End}_K(V) \to M(m \times m, K), \quad f \mapsto M(\mathcal{B}, f, \mathcal{B})$$

ist ein Isomorphismus von Ringen und K*-Vektorräumen. Für* $m \geq 2$ *sind die Ringe nicht kommutativ.*

g) Die Menge $\mathrm{Aut}_K(V)$ *der Automorphismen von* V *ist eine Gruppe. Die Abbildung*

$$\mathrm{Aut}_K(V) \to GL(m,K), \quad f \mapsto M(\mathcal{B}, f, \mathcal{B})$$

ist ein Isomorphismus von Gruppen (Def. von $GL(m,K)$ *in Satz 4.13 c)). Für* $m \geq 2$ *sind die Gruppen nicht kommutativ.*

Beweis: a) Mit der Notation $f(\mathcal{A}) = (f(a_1), ..., f(a_n))$ von Definition 5.8 ist

$$f(\mathcal{A} \cdot x) \overset{f \text{ linear}}{=} f(\mathcal{A}) \cdot x \overset{\text{Def. } 5.8}{=} \mathcal{B} \cdot M(\mathcal{B}, f, \mathcal{A}) \cdot x.$$

Das ist äquivalent zur Behauptung

$$l_{\mathcal{B}}^{-1} \circ f \circ l_{\mathcal{A}} = \text{ Matrixmultiplikation von links mit } M(\mathcal{B}, f, \mathcal{A}).$$

b) Wegen a) ist die Abbildung

$$\mathrm{Hom}_K(U,V) \to M(m \times n, K), \quad f \mapsto M(\mathcal{B}, f, \mathcal{A}),$$

die Komposition der beiden Abbildungen

$$\mathrm{Hom}_K(U,V) \to \mathrm{Hom}_K(M(n \times 1, K), M(m \times 1, K)), \quad f \mapsto l_{\mathcal{B}}^{-1} \circ f \circ l_{\mathcal{A}}$$

und

$$\mathrm{Hom}_K(M(n \times 1, K), M(m \times 1, K)) \to M(m \times n, K), \quad g \mapsto \mathrm{Mat}(g).$$

Die zweite ist ein Vektorraumisomorphismus nach Satz 5.5 b). Die erste ist ein Vektorraumisomorphismus, weil $l_{\mathcal{A}}$ und $l_{\mathcal{B}}$ Vektorraumisomorphismen sind: sie ist bijektiv, denn ein Element $g \in \mathrm{Hom}_K(M(n \times 1, K), M(m \times 1, K))$ hat genau ein Urbild, nämlich $l_{\mathcal{B}} \circ g \circ l_{\mathcal{A}}^{-1}$. Die Linearität ist auch klar.
c) Es ist

$$\begin{aligned} M(\mathcal{C}, g \circ f, \mathcal{A}) &= \mathrm{Mat}(l_{\mathcal{C}}^{-1} \circ g \circ f \circ l_{\mathcal{A}}) \quad \text{(mit a))} \\ &= \mathrm{Mat}(l_{\mathcal{C}}^{-1} \circ g \circ l_{\mathcal{B}}) \cdot \mathrm{Mat}(l_{\mathcal{B}}^{-1} \circ f \circ l_{\mathcal{A}}) \quad \text{(Satz 5.5 c))} \\ &= M(\mathcal{C}, g, \mathcal{B}) \cdot M(\mathcal{B}, f, \mathcal{A}) \quad \text{(mit a))}. \end{aligned}$$

d) Wie Satz 5.5 d) (bzw. mit Satz 5.5 d) und Satz 5.11 a)).
e) folgt aus d).
f) folgt aus b) und c).
g) folgt aus c) und d). □

Bemerkungen 5.12 i) Es seien $U, V, f : U \to V, \mathcal{A}$ und $\mathcal{B}$ wie in Satz 5.11. Es sei $\widetilde{\mathcal{A}}$ eine andere Basis von U und $\widetilde{\mathcal{B}}$ eine andere Basis von V. Dann ist wegen Satz 5.11 c)

$$M(\widetilde{\mathcal{B}}, f, \widetilde{\mathcal{A}}) = M(\widetilde{\mathcal{B}}, \mathcal{B}) \cdot M(\mathcal{B}, f, \mathcal{A}) \cdot M(\mathcal{A}, \widetilde{\mathcal{A}}).$$

Diese Formel zeigt, wie $M(\mathcal{B}, f, \mathcal{A})$ von $\mathcal{B}$ und $\mathcal{A}$ abhängt, bzw. wie sich die Matrix transformiert, wenn man $\mathcal{B}$ und $\mathcal{A}$ ändert.
Die Abhängigkeit von $M(\mathcal{B}, f, \mathcal{A})$ von f ist linear (Satz 5.11 b)).

ii) Satz 5.13 a) zeigt, daß man $M(\mathcal{B}, f, \mathcal{A})$ durch Wahl geeigneter Basen $\mathcal{B}$ und $\mathcal{A}$ auf eine sehr einfache Gestalt bringen kann. Aus $M(\mathcal{B}, f, \mathcal{A})$ allein kann man nur $\operatorname{rang}(f)$ ablesen.

iii) Viel reicher und interessanter wird die Situation, wenn f eine Endomorphismus ist und wenn man nur die Matrizen $M(\mathcal{B}, f, \mathcal{B})$ ansieht. Das kommt in LA II.

Satz 5.13 *a) Zu jeder linearen Abbildung $f : U \to V$ von endlichdimensionalen K-Vektorräumen gibt es eine Basis $\mathcal{A} = (a_1, ..., a_n)$ von U und eine Basis $\mathcal{B} = (b_1, ..., b_m)$ von V, so daß für $k := \operatorname{rang} f$ gilt:*

$$M(\mathcal{B}, f, \mathcal{A}) = \begin{pmatrix} (\delta_{ij})_{i,j=1,...,k} & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdot & 0 \\ 0 & \ddots & & \\ \cdot & & 1 & 0 \\ 0 & \cdot & 0 & 0 \end{pmatrix};$$

d.h. die Einheitsmatrix in den ersten k Zeilen und Spalten und 0 außerhalb.
b) (Matrix-Version von a)) Zu jeder Matrix $C \in M(m \times n, K)$ gibt es Matrizen $A \in GL(n, K)$ und $B \in GL(m, K)$, so daß mit $k := \operatorname{Spaltenrang}(C)$ gilt:

$$B \cdot C \cdot A = \begin{pmatrix} (\delta_{ij})_{i,j=1,...,k} & 0 \\ 0 & 0 \end{pmatrix}.$$

c) Durch Links- oder Rechtsmultiplikation mit einer invertierbaren Matrix ändern sich Zeilen- und Spaltenrang einer gegebenen Matrix nicht.
d) (=Satz 4.2) Für jede Matrix $C \in M(m \times n, K)$ ist

$$\operatorname{Zeilenrang}(C) = \operatorname{Spaltenrang}(C).$$

Beweis: a) Man wählt $a_1, ..., a_k \in U$ so, daß $(b_1, ..., b_k) := (f(a_1), ..., f(a_k))$ eine Basis von $f(U) \subset V$ ist. Man ergänzt diese Basis zu einer Basis $\mathcal{B} = (b_1, ..., b_m)$ von V (Satz 3.19). Wegen Satz 5.3 g) ist $\dim \ker(f) = \dim U - \operatorname{rang}(f) = n - k$. Man wählt eine Basis $(a_{k+1}, ..., a_n)$ von $\ker(f)$. Aus dem Beweis von Satz 5.3 g) folgt, daß $(a_1, ..., a_n)$ eine Basis von U ist. Dann sieht $M(\mathcal{B}, f, \mathcal{A})$ aus wie gewünscht.

b) [Es gibt einen Beweis, der nur Zeilen- und Spaltenumformungen benutzt; der hier gegebene Beweis benutzt a).] Sei $U := M(n \times 1, K)$, $\widetilde{\mathcal{A}}$ seine Standardbasis, $V := M(m \times 1, K)$, $\widetilde{\mathcal{B}}$ seine Standardbasis, $l_C : U \to V$ die Linksmultiplikation mit C. Dann ist

$$M(\widetilde{\mathcal{B}}, l_C, \widetilde{\mathcal{A}}) = C$$

und

$$\text{Spaltenrang}(C) = \text{rang}(l_C).$$

Laut a) gibt es Basen $\mathcal{A}$ von U und $\mathcal{B}$ von V mit

$$M(\mathcal{B}, l_C, \mathcal{A}) = \begin{pmatrix} (\delta_{ij})_{i,j=1,\ldots,k} & 0 \\ 0 & 0 \end{pmatrix}.$$

Mit den Bezeichnungen $A := M(\widetilde{\mathcal{A}}, \mathcal{A})$ und $B := M(\mathcal{B}, \widetilde{\mathcal{B}})$ für die Basiswechselmatrizen ist

$$M(\mathcal{B}, l_C, \mathcal{A}) = M(\mathcal{B}, \widetilde{\mathcal{B}}) \cdot M(\widetilde{\mathcal{B}}, l_C, \widetilde{\mathcal{A}}) \cdot M(\widetilde{\mathcal{A}}, \mathcal{A}) = B \cdot C \cdot A.$$

c) **1. Schritt**: Sei $B \in GL(m, K)$ und $C \in M(m \times n, K)$. Die Zeilen von $B \cdot C$ sind Linearkombinationen der Zeilen von C, und die Zeilen von $C = B^{-1} \cdot (B \cdot C)$ sind Linearkombinationen der Zeilen von $B \cdot C$. Daher ist

$$\text{Zeilenrang}(B \cdot C) = \text{Zeilenrang}(C).$$

2. Schritt: Ist $f : W \to W$ ein Automorphismus eines Vektorraums W und ist $W_1 \subset W$ ein endlich-dimensionaler Untervektorraum, so ist $\dim W_1 = \dim f(W_1)$. Denn das Bild einer Basis von W_1 ist eine Basis von $f(W_1)$.
3. Schritt: Sei $C \in M(m \times n, K)$ mit den Spalten $w_1, ..., w_n \in M(m \times 1, K)$. Ist nun $B \in GL(m, K)$, so ist die Linksmultiplikation l_B ein Automorphismus von $M(m \times 1, K)$. Also ist

$$\begin{aligned} \text{Spaltenrang}(B \cdot C) &= \dim_K(\text{span}_K(B \cdot w_1, ..., B \cdot w_n)) \\ &= \dim_K(\text{span}_K(l_B(w_1), ..., l_B(w_n))) \\ &= \dim_K l_B(\text{span}_K(w_1, ..., w_n)) \\ &= \dim_K(\text{span}_K(w_1, ..., w_n)) = \text{Spaltenrang}(C). \end{aligned}$$

4. Schritt: Sei $A \in GL(n, K)$ und C wie oben. Analog zum 1. Schritt zeigt man $\text{Spaltenrang}(C \cdot A) = \text{Spaltenrang}(C)$; analog zum 3. Schritt zeigt man $\text{Zeilenrang}(C \cdot A) = \text{Zeilenrang}(C)$.
d) folgt aus c) und b), denn bei der Matrix $B \cdot C \cdot A$ in b) sind Zeilenrang und Spaltenrang gleich. □

Satz 5.14 *a) Ist I eine nichtleere Menge und K ein Körper, so ist die Menge*

$$\mathrm{Abb}_{endlich}(I,K) := \{g : I \to K \quad | \quad \text{die Menge } \{j \in I \mid g(j) \neq 0\} \text{ ist endlich}\}$$

ein Untervektorraum von $\mathrm{Abb}(I,K)$.
b) (Verallgemeinerung von Lemma 5.10 b) auf Vektorräume mit beliebig großen Basen) Sei V ein K-Vektorraum mit Basis $(v_i)_{i\in I}$. Die Abbildung

$$\begin{array}{rcl} V & \to & \mathrm{Abb}_{endlich}(I,K) \\ \sum_{j\in J} \lambda_j v_j & \mapsto & g, \quad \text{mit } g(j) := \begin{cases} \lambda_j & \text{für } j \in J, \\ 0 & \text{für } j \in I - J, \end{cases} \end{array}$$

ist ein Isomorphismus von Vektorräumen.

Beweis: Übung. □

Satz 5.15 *a) Ist $U \subset V$ ein Untervektorraum eines K-Vektorraums, so trägt die Quotientengruppe $(V/U,+)$ (vgl. Satz 1.36) eine natürliche Struktur eines K-Vektorraums; mit der skalaren Multiplikation $\lambda \cdot [v] := [\lambda \cdot v]$.*
b) (Verfeinerung von Satz 5.3 g)) Sei $f : V \to W$ eine lineare Abbildung zwischen K-Vektorräumen. $\ker f \subset V$ *ist ein Untervektorraum (Satz 5.3). Die Abbildung f induziert eine Abbildung*

$$\widetilde{f} : V/ker f \to f(W), \quad [v] = v + \ker f \mapsto f(v).$$

$\widetilde{f}$ ist ein Vektorraumisomorphismus.

Beweis: Übung. □

6 Lineare Gleichungssysteme

In diesem Kapitel bezeichnet K irgendeinen Körper.

Definition 6.1 Ein *lineares Gleichungssystem* ist ein Gleichungssystem der Gestalt

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n &= b_1, \\ a_{21}x_1 + a_{22}x_2 + ... + a_{2n}x_n &= b_2, \\ &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + ... + a_{mn}x_n &= b_m. \end{aligned}$$

Hier sind $A = (a_{ij}) \in M(m \times n, K)$ und $b = (b_1, ..., b_m)^{tr} \in M(m \times 1, K)$ gegeben, und $x = (x_1, ..., x_n)^{tr}$ ist ein Spaltenvektor von "Unbestimmten". Man kann es kürzer schreiben, in der Form

$$A \cdot x = b.$$

Es heißt *inhomogenes lineares Gleichungssystem*, falls $b \neq 0$ ist, sonst *homogenes lineares Gleichungssystem*.
Einem inhomogenen linearen Gleichungssystem $A \cdot x = b$ ist das homogene lineare Gleichungssystem $A \cdot x = 0$ zugeordnet.
Man möchte die *Lösungsmengen*

$$\begin{aligned} & \text{Lös}(A, b) &:= \{x \in M(n \times 1, K) \mid A \cdot x = b\} \\ \text{und} \quad & \text{Lös}(A, 0) &:= \{x \in M(n \times 1, K) \mid A \cdot x = 0\} \end{aligned}$$

bestimmen.

Beispiel 6.2

$$\begin{pmatrix} 1 & 2 & 0 & 1 \\ 3 & 7 & 4 & 0 \\ 2 & 4 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

In der Matrix $(A\ b)$ trennen wir b von A durch einen senkrechten Strich, um anzuzeigen, daß b die rechte Seite des linearen Gleichungssystems ist. Bei Zeilenumformungen ändert sich $\text{Lös}(A, b)$ nicht.

$$\left(\begin{array}{cccc|c} 1 & 2 & 0 & 1 & 1 \\ 3 & 7 & 4 & 0 & 1 \\ 2 & 4 & 1 & 0 & 1 \end{array}\right) \overset{\text{Z.umf.}}{\longrightarrow} \left(\begin{array}{cccc|c} 1 & 2 & 0 & 1 & 1 \\ 0 & 1 & 4 & -3 & -2 \\ 0 & 0 & 1 & -2 & -1 \end{array}\right)$$

$$\overset{\text{Z.umf.}}{\longrightarrow} \left(\begin{array}{cccc|c} 1 & 0 & 0 & -9 & -3 \\ 0 & 1 & 0 & 5 & 2 \\ 0 & 0 & 1 & -2 & -1 \end{array}\right)$$

Bei den Lösungen ist $x_4 =: t$ beliebig, und x_1, x_2, x_3 sind dann eindeutig. $(x_1, x_2, x_3, x_4)^{tr}$ ist genau dann eine Lösung, wenn

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 9t-3 \\ -5t+2 \\ 2t-1 \\ t \end{pmatrix} = \begin{pmatrix} 9 \\ -5 \\ 2 \\ 1 \end{pmatrix} \cdot t + \begin{pmatrix} -3 \\ 2 \\ -1 \\ 0 \end{pmatrix}$$

ist mit $t \in K$ beliebig.

Satz 6.3 *Sei $A \cdot x = b$ ein lineares Gleichungssystem wie in Definition 6.1.*
a) $\text{Lös}(A, 0)$ *ist ein Untervektorraum von $M(n \times 1, K)$ der Dimension*

$$\dim_K \text{Lös}(A, 0) = n - \operatorname{rang} A.$$

b) Sei $U := \operatorname{span}_K(\text{Spalten von } A) \subset M(m \times 1, K)$.
1. Fall, *$b \notin U$:* *dann ist* $\text{Lös}(A, b) = \emptyset$.
2. Fall, *$b \in U$:* *dann ist* $\text{Lös}(A, b)$ *nicht leer und*

$$\text{Lös}(A, b) = \text{Lös}(A, 0) + v,$$

wobei $v \in \text{Lös}(A, b)$ eine beliebige Lösung ist.
c) Ist $B \in GL(m, K)$, so ist $\text{Lös}(B \cdot A, B \cdot b) = \text{Lös}(A, b)$. *Mit anderen Worten: Bei Zeilenumformungen der Matrix $(A\ b) \in M(m \times (n+1), K)$ ändert sich die Lösungsmenge des Gleichungssytems nicht.*

Beweis: a) Die Multiplikation von links mit A ist eine lineare Abbildung

$$l_A : M(m \times 1, K) \to M(n \times 1, K), \quad x \mapsto A \cdot x.$$

Es ist $\text{Lös}(A, 0) = \ker(l_A)$, also ein Untervektorraum (Satz 5.3 c)). Nach Satz 5.3 g) ist

$$\dim \ker(l_A) = n - \operatorname{rang} l_A = n - \text{Spaltenrang}(A) = n - \operatorname{rang} A.$$

b) $A \cdot v = b$ sagt gerade, daß b eine Linearkombination der Spalten von A ist, mit Koeffizienten $v_1, ..., v_n$. Daher ist $b \in U$ natürlich äquivalent zur Lösbarkeit von $A \cdot x = b$.
Ist $v \in \text{Lös}(A, b)$, so ist

$$\text{Lös}(A, b) = \{x \mid l_A(x) = b\} = v + \ker l_a,$$

denn l_A ist linear.
c) Klar. □

Beispiel 6.4 Hier sollen für jedes $a \in K$ die Lösungen des Gleichungssystems $A \cdot x = b$ bestimmt werden, wo

$$(A|b) = \left(\begin{array}{cc|c} 1 & -a & -1 \\ a+1 & 0 & -1 \end{array} \right).$$

Eine Zeilenumformung gibt

$$\left(\begin{array}{cc|c} 1 & -a & -1 \\ 0 & a(a+1) & a \end{array} \right).$$

1. Fall, $a = -1$: $\text{Lös}(A, b) = \emptyset$.
2. Fall, $a = 0$: $\text{Lös}(A, b) = \left\{ \begin{pmatrix} 0 \\ 1 \end{pmatrix} \cdot t + \begin{pmatrix} -1 \\ 0 \end{pmatrix} \mid t \in K \right\}$.
3. Fall, $a \notin \{0, -1\}$: $\text{Lös}(A, b) = \left\{ \begin{pmatrix} \frac{-1}{a+1} \\ \frac{1}{a+1} \end{pmatrix} \right\}$.

(Bei $K = \mathbb{F}_2$ ist $K = \{0, -1\}$, und der 3. Fall tritt nicht ein.)

Bemerkungen 6.5 (Methoden zur Lösung eines linearen Gleichungssystems)
i) Wenn $m = n$ ist und A invertierbar ist, ist l_A ein Isomorphismus, und zu jedem b gibt es genau eine Lösung von $A \cdot x = b$. Sie ist einfach $A^{-1} \cdot b$. Ein Weg, A^{-1} zu berechnen, ist in Bemerkung 4.14 beschrieben. Ein anderer kommt in Kapitel 7.
Man muß aber nicht wirklich A^{-1} und $A^{-1} \cdot b$ ausrechnen. Es reicht, die $(n \times (n+1))$-Matrix $(A\ b)$ durch Zeilenumformungen in die Gestalt $(E_n\ \widetilde{b})$ zu bringen. Dann ist $\widetilde{b} = A^{-1} \cdot b$.

ii) Im allgemeinen Fall bestimmt man $\text{Lös}(A, b)$ so: Mit dem Gauß-Algorithmus bringt man die Matrix $(A\ b) \in M(m \times (n+1), K)$ in Zeilenstufenform $(A^{(1)}\ b^{(1)})$. Es sei $k \in \mathbb{N}_0$ so, daß genau die ersten k Zeilen von $A^{(1)}$ nicht verschwinden.

1. Fall: Sei $(b^{(1)}_{k+1}, ..., b^{(1)}_n) \neq 0$. Dann ist $\text{Lös}(A, b) = \emptyset$.

2. Fall: Sei $(b^{(1)}_{k+1}, ..., b^{(1)}_n) = 0$. Für $i \leq k$ sei

$$j_{min}(i) := \min(j \mid a^{(1)}_{ij} \neq 0),$$

Es ist $1 \leq j_{min}(1) < ... < j_{min}(k) \leq n$. Es sei

$$J := \{1, ..., n\} - \{j_{min}(1), ..., j_{min}(k)\}.$$

Skizzen in der Vorlesung

Mit Zeilenumformungen vom Typ II löscht man alle Einträge in den Spalten mit Spaltenindices $j_{min}(i)$, $i = 1, ..., k$ außer dem Eintrag $a^{(1)}_{ij_{min}(i)}$. Mit Zeilenumformungen vom Typ I normiert man alle Einträge $a^{(1)}_{ij_{min}(i)}$ zu 1. Man erhält eine Matrix $(A^{(2)}\ b^{(2)})$. Die i-te Zeile des neuen Gleichungssystems ist

$$x_{j_{min}(i)} + \sum_{j \in J} a^{(2)}_{ij} x_j = b^{(2)}_i.$$

Der Lösungsraum ist nun leicht beschreibbar:

$$\begin{aligned} \text{Lös}(A, b) = \{x \in M(n \times 1, K) \quad | \quad & x_j \text{ für } j \in J \text{ ist beliebig,} \\ & x_{j_{min}(i)} \text{ für } i = 1, ..., k \text{ ist durch} \\ & \text{die Gleichung oben bestimmt}\}. \end{aligned}$$

Eine besonders schöne Lösung $v_{inhom} \in \text{Lös}(A^{(2)}, b^{(2)})$ des inhomogenen Gleichungssystems erhält man nun, wenn man $x_j := 0$ für alle $j \in J$ setzt, sie ist

$$v_{inhom} = \sum_{i=1}^{k} b^{(2)}_i \cdot e_{j_{min}(i)} = \begin{pmatrix} 0 \\ \vdots \\ b^{(2)}_1 \\ \vdots \\ b^{(2)}_k \\ \vdots \\ 0 \end{pmatrix} \begin{matrix} \\ \\ \leftarrow j_{min}(1) \\ \\ \leftarrow j_{min}(k) \\ \\ \\ \end{matrix}$$

Und eine besonders schöne Basis $v_j, j \in J$ von Lösungen in $\text{Lös}(A^{(2)}, 0)$ (d.h. des homogenen Gleichungssystems) erhält man, indem man für v_j $x_j := -1$ setzt und $v_k := 0$ für $k \in J - \{j\}$, man erhält für $j \in J$

$$v_j = -e_j + \sum_{i=1}^{k} a^{(2)}_{ij} \cdot e_{j_{min}(i)} = \begin{pmatrix} 0 \\ \vdots \\ -1 \\ \vdots \\ \vdots \\ 0 \end{pmatrix} \leftarrow j + \begin{pmatrix} 0 \\ \vdots \\ a^{(2)}_{1j} \\ \vdots \\ a^{(2)}_{kj} \\ \vdots \\ 0 \end{pmatrix} \begin{matrix} \\ \\ \leftarrow j_{min}(1) \\ \\ \leftarrow j_{min}(k) \\ \\ \\ \end{matrix}.$$

Skizzen in der Vorlesung

In Prosa und etwas vage: Man erhält v_{inhom} aus dem Spaltenvektor b, indem man die ersten k Einträge von b auf die Stellen $j_{min}(1), ..., j_{min}(k)$ eines Spaltenvektors der Länge n verteilt und die anderen Stellen als 0 ansetzt.

Man erhält $v_j, j \in J$, als Summe des Spaltenvektors $-e_j$ und eines Spaltenvektors, den man analog zu v_{inhom} durch Verteilen der ersten k Einträge der j-ten Spalte von $A^{(3)}$ auf die Stellen $j_{min}(1), ..., j_{min}(k)$ erhält. (Man muss mit all den Indices aufpassen, aber man braucht nicht mehr zu rechnen für die Bestimmung von v_{inhom} und $v_j, j \in J$).
Vorsicht: Man *muß* nicht ganz genau so rechnen. In einfachen Fällen reicht es oft, die Matrix A irgendwie auf Zeilenstufenform zu bringen.

Beispiel 6.6

$$(A|b) = (A^{(3)}|b^{(3)}) = \left(\begin{array}{ccccccc|c} 1 & 2 & 0 & 3 & 5 & 0 & 7 & 10 \\ 0 & 0 & 1 & 4 & 6 & 0 & 8 & 11 \\ 0 & 0 & 0 & 0 & 0 & 1 & 9 & 12 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right) \in M(m \times (n+1), \mathbb{Q}),$$

mit $m = 5, n = 7$ und $k := \operatorname{rang} A = 3$, also $\dim \text{Lös}(A, 0) = n - k = 4$. Es sind $(j_{min}(1), j_{min}(2), j_{min}(3)) = (1, 3, 6)$ und $J := \{1, ..., n\} - \{j_{min}(1), j_{min}(2), j_{min}(3)\} = \{2, 4, 5, 7\}$. Hier sind die Lösung $v_{inhom} \in \text{Lös}(A, b)$ und die Basis $v_j \in \text{Lös}(A, 0)$, $j \in J$, von $\text{Lös}(A, 0)$

$$v_{inhom} = \begin{pmatrix} 10 \\ 0 \\ 11 \\ 0 \\ 0 \\ 12 \\ 0 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 2 \\ -1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad v_4 = \begin{pmatrix} 3 \\ 0 \\ 4 \\ -1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad v_5 = \begin{pmatrix} 5 \\ 0 \\ 6 \\ 0 \\ -1 \\ 0 \\ 0 \end{pmatrix}, \quad v_7 = \begin{pmatrix} 7 \\ 0 \\ 8 \\ 0 \\ 0 \\ 9 \\ -1 \end{pmatrix}.$$

Es ist

$$\begin{aligned} \text{Lös}(A, b) &= \{v_{inhom} + t_1 v_2 + t_2 v_4 + t_3 v_5 + t_4 v_7 \mid t_1, t_2, t_3, t_4 \in \mathbb{Q}\} \\ &= v_{inhom} + \operatorname{span}(v_2, v_4, v_5, v_7) = v_{inhom} + \text{Lös}(A, 0). \end{aligned}$$

Beispiel 6.7 Oft ist es schwerer, aus einer Textaufgabe ein lineares Gleichungssystem herauszudestillieren, als es zu lösen. Ein Beispiel:

"A famous puzzle of Sam Loyd: The combined ages of Mary and Ann are 44 years, and Mary is twice as old as Ann was when Mary was half as old as Ann will be when Ann ist three times as old as Mary was when Mary was three times as old as Ann. How old is Ann?"

1. Schritt: Geeignete Variablen einführen.
The combined ages of Mary (Alter jetzt: m) and Ann (Alter jetzt: a) are 44 years, and Mary is twice as old as Ann was (Alter zu dem Zeitpunkt: $a - t_1$) when Mary was (A.z.d.Z.: $m - t_1$) half as old as Ann will be (A.z.d.Z.: $a + t_2$)

when Ann ist three times as old as Mary was (A.z.d.Z.: $m - t_3$) when Mary was three times as old as Ann (A.z.d.Z.: $a - t_3$).

2. Schritt: Die Bedingungen als lineare Gleichungen schreiben.

$$\begin{aligned} &m + a = 44, \quad m = 2(a - t_1), \quad m - t_1 = \frac{1}{2}(a + t_2), \\ &a + t_2 = 3(m - t_3), \quad m - t_3 = 3(a - t_3). \end{aligned}$$

3. Schritt: Das lineare Gleichungssystem lösen. Angesichts seiner Gestalt wird es hier durch Zeilenumformungen von unten nach oben vereinfacht.

$$\left(\begin{array}{ccccc|c} 1 & 1 & 0 & 0 & 0 & 44 \\ 1 & -2 & 2 & 0 & 0 & 0 \\ 1 & -\frac{1}{2} & -1 & -\frac{1}{2} & 0 & 0 \\ -3 & 1 & 0 & 1 & 3 & 0 \\ 1 & -3 & 0 & 0 & 2 & 0 \end{array}\right) \rightarrow \left(\begin{array}{ccccc|c} 0 & \frac{8}{3} & 0 & 0 & 0 & 44 \\ -\frac{3}{2} & \frac{5}{2} & 0 & 0 & 0 & 0 \\ -\frac{5}{4} & \frac{9}{4} & -1 & 0 & 0 & 0 \\ -\frac{9}{2} & \frac{11}{2} & 0 & 1 & 0 & 0 \\ 1 & -3 & 0 & 0 & 2 & 0 \end{array}\right),$$

die eindeutige Lösung ist

$$(m, a, t_1, t_2, t_3)^{tr} = (\frac{55}{2}, \frac{33}{2}, \frac{11}{4}, 33, 11)^{tr}.$$