Albert-Ludwigs-Universität Freiburg

Vorlesungsskript (vorläufig)

Lineare Algebra I

Angelika Rohde

Wintersemester 2023/24

Inhaltsverzeichnis

1 Grundlagen

1.1 Mengen

Beispiel 1.1 (Zahlbereiche)**.**

- $\mathbb{N} = \{1, 2, 3, \dots\}$ *Menge der natürlichen Zahlen*
- $\mathbb{N}_0 = \{0, 1, 2, \dots\}$ *Menge der natürlichen Zahlen mit Null*
- $\mathbb{Z} = \{0, 1, -1, 2, -2, \dots\}$ *Menge der ganzen Zahlen*
- $\mathbb{Q} = \{\frac{p}{q} | \, p \in \mathbb{Z}, q \in \mathbb{N}\}$ *Menge der rationalen Zahlen*
- $\mathbb{R}$ *Menge der reellen Zahlen (→ Vorlesung Analysis)*
- $\mathbb{C}$ *Menge der komplexen Zahlen (→ Vorlesung Funktionentheorie)*

Wir möchten hier nicht formal den subtilen des Begriff der Menge erörtern, das ist Gegenstand der Mengenlehre. Für unsere Zwecke besteht eine Menge M wie in Beispiel 1.1 aus unterschiedlichen Elementen; wir schreiben $a \in M$ ("a Element M"), falls das Element a in M enthalten ist, andernfalls gilt $a \notin M$ ("a nicht Element M"). $\emptyset$ bezeichnet die leere Menge, die dadurch ausgezeichnet ist, dass sie keine Elemente enthält.

Notation 1.2 (Mengenangabe mit charakterisierender Eigenschaft)**.**

$$M = \{x \in A | \, x \text{ hat Eigenschaft } E\}$$

Beispiele. $\{x \in \mathbb{N} | \, 3 < x < 7\} = \{4, 5, 6\}$ *und* $\{x \in \mathbb{Z} | \, x^2 = -1\} = \emptyset$ *(leere Menge).*

Definition 1.3. *Seien M und N Mengen.*

M heißt Teilmenge von N ($M \subset N$), wenn gilt: $a \in M \Rightarrow a \in N$.

M heißt echte Teilmenge von N ($M \subsetneq N$), falls $M \subset N$ und $M \neq N$.

Beispiel 1.4. $\mathbb{N} \subsetneq \mathbb{N}_0 \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}$.

Definition 1.5. *Seien M, N Mengen. Wir definieren (":=" bedeutet "ist definiert als")*

$M \cup N := \{a | \, a \in M \text{ oder } a \in N\}$ *(Vereinigung)*

$M \cap N := \{a | \, a \in M \text{ und } a \in N\}$ *(Durchschnitt)*

$M \setminus N := \{a | \, a \in M \text{ und } a \notin N\}$ *(Differenz "M ohne N").*

Lemma 1.6. *Seien A, B, C Mengen. Dann gilt*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Für "=" müssen wir "$\subset$" und "$\supset$" beweisen. Wir zeigen eine Behauptung der Form $D \subset E$, indem wir für beliebiges $x \in D$ folgern, dass auch $x \in E$, also formal: $x \in D \Rightarrow x \in E$ ("$\Rightarrow$" bedeutet "daraus folgt").

Beweis.

"$\subset$": Sei $x \in A \cap (B \cup C)$.
$\Rightarrow x \in A$ und $x \in B \cup C$.
1. Fall: $x \in A$ und $x \in B \Rightarrow x \in A \cap B \subset (A \cap B) \cup (A \cap C)$
2. Fall: $x \in A$ und $x \in C \Rightarrow x \in A \cap C \subset (A \cap B) \cup (A \cap C)$.

"$\supset$": Sei $x \in (A \cap B) \cup (A \cap C)$.
($x \in A$ und $x \in B$) oder ($x \in A$ und $x \in C$)
$\Rightarrow x \in A$ und ($x \in B$ oder $x \in C$)
$\Rightarrow x \in A \cap (B \cup C)$. □

Bemerkung 1.7. *Wir haben hier die Pfeile "$\Rightarrow$" verwendet, wenn von einer Aussage auf eine andere geschlossen wurde. Im Folgenden wird "$\Leftrightarrow$" für eine Äquivalenzaussage verwendet, d.h., wenn beide Richtungen, "$\Rightarrow$" und "$\Leftarrow$", gelten.*

Lemma 1.8. *Seien A, B Mengen. Dann sind äquivalent:*

(i) $A \cup B = B$;

(ii) $A \subset B$.

In Kurzschreibweise: Es gilt $A \cup B = B \Leftrightarrow A \subset B$.

Beweis. Wir zeigen für die Äquivalenz "$\Leftrightarrow$" die beiden Richtungen "$\Rightarrow$" und "$\Leftarrow$".

"$\Rightarrow$": (D.h. wir nehmen an, dass $A \cup B = B$ gilt und müssen $A \subset B$ beweisen.)
Sei $x \in A$. $\Rightarrow x \in A \cup B \overset{(i)}{=} B$, d.h. $A \subset B$.

"$\Leftarrow$": (D.h. wir nehmen an, dass $A \subset B$ gilt und müssen $A \cup B = B$ beweisen, also $A \cup B \subset B$ sowie $B \subset A \cup B$.)
Sei $x \in A \cup B \Rightarrow x \in A$ oder $x \in B \overset{(ii)}{\Rightarrow} x \in B$, also haben wir $A \cup B \subset B$ gezeigt.
$B \subset A \cup B$ ist aber klar, womit $B = A \cup B$. □

Zusammenfassung 1.9 (Direkte Beweismethode)**.** *Die Aussage eines Satzes besteht immer aus einer (oder mehreren) Implikationen*

$$\textit{Aussage } A \Rightarrow \textit{Aussage } B$$

oder Äquivalenzen

$$\textit{Aussage } A \Leftrightarrow \textit{Aussage } B.$$

(Die Notation "⇔" bedeutet "genau dann wenn" und entspricht den beiden Implikationen Aussage A ⇒ Aussage B und Aussage B ⇒ Aussage A.) Die direkte Beweismethode besteht darin, eine Implikation durch eine Abfolge von direkten Schlüssen (Aussage A ⇒ Aussage A1 ⇒ Aussage A2 ⇒ ... ⇒ Aussage B) zu beweisen.

Beispiel 1.10. *Wir wollen zeigen:*

x_0 *ist eine Lösung von* $(x^2 - px + q) = 0$

$\Rightarrow$

$$x_0 = \frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q} \quad \textit{und} \quad \frac{p^2}{4} - q \geq 0.$$

Anfängerfehler: Forme $x_0 = \frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$ *so lange um, bis die erste Aussage dasteht:*

$$\begin{aligned} & x_0 - \frac{p}{2} = \pm\sqrt{\frac{p^2}{4} - q} \\ \Rightarrow \quad & \left(x_0 - \frac{p}{2}\right)^2 = \frac{p^2}{4} - q \\ \Rightarrow \quad & x_0^2 - px_0 + \frac{p^2}{4} = \frac{p^2}{4} - q \\ \Rightarrow \quad & x^2 - px + q = 0. \end{aligned}$$

Dies wäre als Beweis obiger Aussage falsch, weil die falsche Schlussrichtung gezeigt wird.

Richtig: x_0 *Lösung von* $x^2 - px + q = 0$

$$\begin{aligned} \Rightarrow \quad & x_0^2 - px_0 + \frac{p^2}{4} = \frac{p^2}{4} - q \\ \Rightarrow \quad & \left(x_0 - \frac{p}{2}\right)^2 = \frac{p^2}{4} - q \\ \Rightarrow \quad & \frac{p^2}{4} - q \geq 0 \quad \textit{und} \quad x_0 - \frac{p}{2} = \pm\sqrt{\frac{p^2}{4} - q} \\ \Rightarrow \quad & \frac{p^2}{4} - q \geq 0 \quad \textit{und} \quad x_0 = \frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}. \end{aligned}$$

□

1.2 Abbildungen

Definition 1.11. *Seien M und N Mengen. Eine Abbildung f von M nach N ist eine Vorschrift, die jedem Element* $m \in M$ *genau ein Element aus N zuordnet. Notation:*

$$\begin{aligned} f : M &\to N \\ m &\mapsto f(m). \end{aligned}$$

Beispiel. $f : \mathbb{R} \to \mathbb{R}^2,\ x \mapsto (x^2, x+1)$.

Bemerkung 1.12. *Seien M, M', N, N' Mengen.*

(i) Zwei Abbildungen $f : M \to N$ und $g : M' \to N'$ sind gleich, wenn $M = M'$, $N = N'$ und $f(m) = g(m)$ für alle $m \in M$.

(ii) $id_M : M \to M$, $m \mapsto m$, heißt Identität (oder identische Abbildung) auf M.

(iii) Für $A \subset M$ heißt $f_{|A} : A \to N$, $a \mapsto f(a)$, die Einschränkung von f auf A.

Bemerkung 1.13. *In obigem Beispiel haben wir die Notation $(x^2, x+1)$ verwendet. (m, n) heißt Tupel (geordnetes Paar). Formal: $M \times N = \{(m, n) | \, m \in M, n \in N\}$ heißt kartesisches Produkt von M und N. Es gilt $(m, n) = (m', n')$ genau dann, wenn $m = m'$ und $n = n'$.*

Beispiel. $\mathbb{R} \times \mathbb{R} = \{(a, b) | \, a \in \mathbb{R}, b \in \mathbb{R}\} = \mathbb{R}^2$ *(reelle Ebene).*

Analog definiert man $\mathbb{R}^n = \mathbb{R} \times \cdots \times \mathbb{R} := \{(a_1, \ldots, a_n) | \, a_i \in \mathbb{R} \text{ für } i = 1, \ldots, n\}$.

Definition 1.14. *Seien M, N Mengen, $f : M \to N$ eine Abbildung. f heißt*

- *injektiv, falls gilt: Für alle $m_1, m_2 \in M$ folgt aus $f(m_1) = f(m_2)$ stets $m_1 = m_2$ $\Leftrightarrow$ für alle $m_1, m_2 \in M$ folgt aus $m_1 \neq m_2$ stets $f(m_1) \neq f(m_2)$;*
- *surjektiv, falls gilt: Für jedes $n \in N$ existiert ein $m \in M$ mit $f(m) = n$;*
- *bijektiv, falls f injektiv und surjektiv ist.*

Beispiele 1.15.

(i) $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ ist nicht injektiv, denn $f(2) = f(-2)$, aber $2 \neq -2$. f ist auch nicht surjektiv, denn es existiert kein $x \in \mathbb{R}$ mit $f(x) = -1$.

(ii) $f : [0, \infty) \to \mathbb{R}$, $x \mapsto x^2$, ist injektiv, denn sind $x_1, x_2 \in [0, \infty)$ mit $x_1^2 = f(x_1) = f(x_2) = x_2^2$, so folgt $x_1 = x_2$. Es gibt aber weiterhin kein x mit $f(x) = -1$, d.h. f ist nicht surjektiv.

(iii) $f : [0, \infty) \to [0, \infty)$, $x \mapsto x^2$, ist injektiv (wie oben) und auch surjektiv, denn für alle $y \geq 0$ gilt $f(\sqrt{y}) = (\sqrt{y})^2 = y$. Damit ist f auch bijektiv.

Definition 1.16. *Seien L, M, N Mengen und $f : L \to M$, $g : M \to N$ Abbildungen. $g \circ f : L \to N$, $l \mapsto g(f(l))$, heißt die Verknüpfung (oder Hintereinanderschaltung, Verkettung, Komposition) von f und g.*

Beispiel 1.17. *Seien $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$ und $g : \mathbb{R} \to \mathbb{R}$, $x \mapsto x + 1$. Dann ist $g \circ f : \mathbb{R} \to \mathbb{R}$, $x \mapsto g(f(x)) = x^2 + 1$.*

Lemma 1.18. *Seien L, M, N, O Mengen, $f : L \to M$, $g : M \to N$, $h : N \to O$ Abbildungen. Dann gilt:*

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

d.h. die Verknüpfung von Abbildungen ist assoziativ.

Beweis. Für $x \in L$ gilt

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

□

Wir verwenden ab nun folgende *Abkürzung:* " $\forall$ " bedeutet "für alle".

Lemma und Definition 1.19. *Seien M, N Mengen, $f : M \to N$ eine Abbildung. Dann sind folgende Aussagen äquivalent:*

(i) *f ist bijektiv.*

(ii) *Zu jedem $n \in N$ gibt es genau ein $m \in M$ mit $f(m) = n$.*

(iii) *Es gibt genau eine Abbildung $g : N \to M$ mit $g \circ f = id_M$ und $f \circ g = id_N$. In diesem Fall bezeichnen wir die Abbildung g mit f^{-1} und nennen f^{-1} die Umkehrabbildung (oder inverse Abbildung) zu f, d.h. es gelten $f^{-1}(f(m)) = m \ \forall m \in M$ und $f(f^{-1}(n)) = n \ \forall n \in N$.*

Beweis. Statt (i) $\Leftrightarrow$ (ii) und (ii) $\Leftrightarrow$ (iii) zeigen wir (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (i).

(i) $\Rightarrow$ (ii): Sei f bijektiv.
Zu zeigen: Zu jedem $n \in N$ existiert genau ein $m \in M$ mit $f(m) = n$.

- "existiert" folgt aus der Surjektivität,
- "genau ein": Seien $m_1, m_2 \in M$ mit $f(m_1) = f(m_2) = n \Rightarrow m_1 = m_2$ wegen der Injektivität.

(ii) $\Rightarrow$ (iii): Angenommen, zu jedem $n \in N$ existiert genau ein $m \in M$ mit $f(m) = n$.
Zu zeigen: Es existiert genau eine Umkehrabbildung g mit $g \circ f = id_M$ und $f \circ g = id_N$.

- "existiert": Wir definieren

$$\begin{aligned} g : N &\to M, \\ n &\mapsto \text{ das eindeutig bestimmte } m \text{ mit } f(m) = n. \end{aligned}$$

  Dann gilt einerseits für $m \in M$: $(g \circ f)(m) = g(f(m)) = m$, d.h. $g \circ f = id_M$, andererseits für $n \in N$: $(f \circ g)(n) = f(g(n)) = n$, d.h. $f \circ g = id_N$.

- "genau eine": Seien $g_1, g_2 : N \to M$ mit $f \circ g_1 = f \circ g_2 = id_N$ und $g_1 \circ f = g_2 \circ f = id_M$. Zu zeigen: $g_1 = g_2$.
  Nach Lemma 1.18 ist $g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2$. Damit gilt

$$\begin{array}{rl} & g_1 \circ (f \circ g_2) = g_1 \circ id_N = g_1 \\ & \quad \| \\ & (g_1 \circ f) \circ g_2 = id_M \circ g_2 = g_2, \qquad \text{d.h. } g_1 = g_2. \end{array}$$

(iii) ⇒ (i): Wir setzen (iii) voraus. Zu zeigen: f ist bijektiv.

- "injektiv": Seien $m_1, m_2 \in M$ mit $f(m_1) = f(m_2)$.

$$\begin{array}{rl} \Rightarrow & f^{-1}(f(m_1)) = f^{-1}(f(m_2)) \\ \Rightarrow & (f^{-1} \circ f)(m_1) = (f^{-1} \circ f)(m_2) \\ & \quad \| \\ & \quad id_M \\ \Rightarrow & m_1 = m_2. \end{array}$$

- "surjektiv": Sei $n \in N \Rightarrow id_N(n) = n \;\Rightarrow\; (f \circ f^{-1})(n) = n \;\Rightarrow f(f^{-1}(n)) = n$. Mit $m = f^{-1}(n)$ ist dann $f(m) = n$.

[Bemerkung: Wir haben hier für die Implikation (iii) ⇒ (i) nicht die Eindeutigkeit von g verwendet und damit eine etwas stärkere Aussage bewiesen.] □

Beispiel 1.20. *$f : [0, \infty) \to [0, \infty)$, $x \mapsto x^2$, ist bijektiv (siehe oben). Die Umkehrabbildung f^{-1} ist gegeben durch $f^{-1}[0, \infty) \to [0, \infty)$, $x \mapsto \sqrt{x}$.*

Definition 1.21. *Seien M, N Mengen, $f : M \to N$ eine Abbildung, $A \subset M$, $B \subset N$.*

- *$f(A) := \{f(a) | \, a \in A\} \subset N$ heißt Bild von A (unter f).*
- *$f^{-1}(B) := \{m \in M | \, f(m) \in B\} \subset M$ heißt Urbild von B (unter f).*

Bemerkung. *Die Notation $f(A)$ bzw. $f^{-1}(B)$ ist zwar üblich, aber nicht unbedingt glücklich, weil einerseits f dabei quasi zu einer Abbildung auf Teilmengen von M "erweitert" wird, andererseits eine Bezeichnungskollision mit der inversen Abbildung f^{-1} besteht. Das Urbild ist immer definiert, auch dann, wenn die Abbildung f nicht bijektiv ist und die inverse Abbildung nicht existiert. Falls f aber invertierbar ist mit inverser Abbildung f^{-1}, dann gilt $f^{-1}(\{n\}) = \{f^{-1}(n)\}$, $n \in N$.*

1.3 Äquivalenzrelationen

Mitunter ist es zweckmäßg, Relationen zwischen zwei Elementen m_1, m_2 einer Menge M zu studieren. Notation: $m_1 \sim m_2$.

Beispiel 1.22.

(i) M *Menge der Freiburger Mathe-Studenten,* $m_1 \sim m_2 :\Leftrightarrow m_1$ *kennt* m_2.

(ii) $M = \mathbb{R}$, $m_1 \sim m_2 :\Leftrightarrow m_1 \leq m_2$.

(iii) $M = \mathbb{R}^2$, $x, y \in M$, *wobei* $x = (x_1, x_2)$, $y = (y_1, y_2)$. $x \sim y :\Leftrightarrow x_1^2 + x_2^2 = y_1^2 + y_2^2$.

Man kann eine Relation beschreiben durch ihren Graphen $R \subset M \times M$, wobei

$$(m_1, m_2) \in R \;\Leftrightarrow\; m_1 \sim m_2. \tag{1.1}$$

Entsprechend kann man eine Relation defnieren durch eine Teilmenge R von $M \times M$ und das Zeichen $\sim$ durch (1.1).

Definition 1.23. *Eine Relation* $\sim$ *auf einer Menge* M *heißt* Äquivalenzrelation, *wenn für beliebige* $m_1, m_2, m_3 \in M$ *gilt:*

(i) $m_1 \sim m_1$ *(Reflexivität)*

(ii) $m_1 \sim m_2 \Rightarrow m_2 \sim m_1$ *(Symmetrie)*

(iii) $m_1 \sim m_2$ *und* $m_2 \sim m_3 \Rightarrow m_1 \sim m_3$ *(Transitivität).*

Die Relation aus Beispiel 1.22 (iii) definiert eine Äquivalenzrelation, (i) und (ii) jedoch nicht.

Definition 1.24. *Ist eine Äquivalenzrelation* $\sim$ *auf einer Menge* M *gegeben, so heißt eine Teilmenge* $A \subset M$ Äquivalenzklasse *(bezüglich* $\sim$*), falls gilt:*

- $A \neq \emptyset$;
- $m, n \in A \Rightarrow m \sim n$;
- $m \in A$, $n \in M$, $m \sim n \Rightarrow n \in A$.

Lemma 1.25. *Ist* $\sim$ *eine Äquivalenzrelation auf einer Menge* M*, so gehört jedes Element* $a \in M$ *zu genau einer Äquivalenzklasse. Insbesondere gilt für zwei beliebige Äquivalenzklassen* A, A' *entweder* $A = A'$ *oder* $A \cap A' = \emptyset$.

Beweis. Für $a \in M$ sei $A \subset M$ definiert als $A := \{m \in M | \, m \sim a\}$. Wir zeigen, dass A eine Äquivalenzklasse ist, die a enthält. Wegen $a \sim a$ ist $a \in A \Rightarrow A \neq \emptyset$. Sind $m, n \in A$, also $m \sim a$ und $n \sim a$, so folgt $m \sim n$ nach Definition 1.23 (ii) und (iii). Ist $m \in A$, $n \in M$ und $m \sim n$, so ist wegen $m \sim a$ auch $n \sim a$ nach Definition 1.23 (ii) und (iii). Aber dann gilt $n \in A$. Damit ist A eine Äquivalenzklasse, die a enthält.

Es bleibt der Nachweis, dass für zwei beliebige Äquivalenzklassen A, A' entweder $A = A'$ oder $A \cap A' = \emptyset$ gilt. Angenommen, $A \cap A' \neq \emptyset$ und $a \in A \cap A'$. Ist $m \in A$, so ist $m \sim a$ und wegen $a \in A'$ auch $m \in A' \Rightarrow A \subset A'$. Genauso zeigt man $A' \subset A$, woraus $A = A'$ folgt. □

Eine Äquivalenzrelation $\sim$ auf einer Menge M liefert also eine Zerlegung von M in disjunkte Äquivalenzklassen. Diese Äquivalenzklassen kann man nun als Elemente einer neuen Menge auffassen.

Definition 1.26. *Sei M eine Menge, $\sim$ eine Äquivalenzrelation darauf. Die Menge der Äquivalenzklassen (bezüglich $\sim$) heißt Quotientenmenge von M nach der Äquivalenzrelation $\sim$ und wird mit $M/\sim$ bezeichnet.*

Indem man jedem Element $a \in M$ diejenige Äquivalenzklasse A_a zuordnet, in der es enthalten ist, erhält man eine kanonische Abbildung $M \to M/\sim$, $a \mapsto A_a$. Das Urbild der einelementigen Menge $\{A\}$ für ein *Element* A aus $M/\sim$ ist wieder A, aber diesmal aufgefasst als *Teilmenge* von M. Jedes $a \in A$ heißt Repräsentant der Äquivalenzklasse A.

Beispiel 1.27. *Wir betrachten noch einmal $\mathbb{R}^2$ mit der Äquivalenzrelation $\sim$ aus Beispiel 1.22 (iii). Die Äquivalenzklassen sind konzentrische Kreislinien um $(0,0)$ (die Äquivalenzklasse $\{(0,0)\}$ wird dabei als Kreislinie mit Radius Null aufgefasst).*

2 Algebraische Grundbegriffe

2.1 Gruppen und Gruppenhomomorphismen

Definition 2.1. *Sei M eine Menge. Eine (innere) Verknüpfung auf M ist eine Abbildung $* : M \times M \to M$, $(a,b) \mapsto a * b$.*

Beispiele 2.2.

$$+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}, \ (a,b) \mapsto a + b,$$
$$\cdot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}, \ (a,b) \mapsto a \cdot b.$$

Definition 2.3. *Eine Gruppe $(G, *)$ besteht aus einer Menge G und einer Verknüpfung $* : G \times G \to G$, $(a, b) \mapsto a * b$, mit folgenden Eigenschaften:*

(i) Die Verknüpfung $*$ ist assoziativ, d.h. $a * (b * c) = (a * b) * c$ für alle $a, b, c \in G$.

(ii) Es existiert ein neutrales Element $e \in G$, d.h. ein Element $e \in G$ mit $e*a = a*e = a$ für alle $a \in G$.

(iii) Für jedes $a \in G$ existiert ein inverses Element a', d.h. ein Element $a' \in G$ mit $a' * a = a * a' = e$.

Die Gruppe heißt abelsch (oder kommutativ), wenn für alle $a, b \in G$ gilt $a * b = b * a$.

Lemma 2.4. *Sei $(G, *)$ eine Gruppe. Dann gilt:*

(i) Es gibt genau ein neutrales Element in G.

(ii) Für jedes $a \in G$ gibt es ein eindeutig bestimmtes inverses Element.

Beweis. (i) Die Existenz folgt aus der Definition der Gruppe. Eindeutigkeit: Sind e und $\tilde{e}$ neutrale Elemente von G, dann folgt $e = e * \tilde{e} = \tilde{e}$ aus Definition 2.3 (ii).

(ii) Die Existenz folgt aus der Definition der Gruppe. Eindeutigkeit: Seien $b \in G$ und $\tilde{b} \in G$ inverse Elemente zu $a \in G$. Dann gilt

$$b \overset{2.3(ii)}{=} e * b \overset{2.3(iii)}{=} (\tilde{b} * a) * b \overset{2.3(i)}{=} \tilde{b} * (a * b) \overset{2.3(iii)}{=} \tilde{b} * e \overset{2.3(ii)}{=} \tilde{b}. \qquad \square$$

Bemerkung 2.5 (Quantoren)**.** *Vor allem in Beweisen, aber oft auch in Formulierungen von Aussagen, verwendet man die Quantoren $\forall$ ("für alle"), $\exists$ ("es existiert"), $\exists!$ ("es gibt genau ein") - häufig in Verbindung mit einem ":".*

Beispielsweise:

- Assoziativität Gruppe: $\forall\, a, b, c \in G$: $a * (b * c) = (a * b) * c$
- inverses Element: $\forall\, a \in G\ \exists!\, a' \in G$ mit $a' * a = a * a' = e$.

Beispiele 2.6.

(i) $(\mathbb{R}, +)$ ist eine abelsche Gruppe:

- *Assoziativgesetz: $a + (b + c) = (a + b) + c\ \forall\, a, b, c \in \mathbb{R}$*
- *neutrales Element: $e = 0$, denn $a + 0 = 0 + a = a\ \forall\, a \in \mathbb{R}$*
- *inverses Element: $a + (-a) = (-a) + a = 0\ \forall a \in \mathbb{R}$*
- *Kommutativgesetz: $a + b = b + a\ \forall\, a, b \in \mathbb{R}$.*

(ii) $(\mathbb{R} \setminus \{0\}, \cdot)$ *ist eine abelsche Gruppe*

- *Assoziativgesetz:* $a \cdot (b \cdot c) = (a \cdot b) \cdot c \; \forall a, b, c \in \mathbb{R} \setminus \{0\}$
- *neutrales Element:* $e = 1$*, denn* $a \cdot 1 = 1 \cdot a = a \; \forall a \in \mathbb{R} \setminus \{0\}$
- *inverses Element:* $a \cdot a^{-1} = a^{-1} \cdot a = 1 \; \forall a \in \mathbb{R} \setminus \{0\}$
- *Kommutativgesetz:* $a \cdot b = b \cdot a \; \forall a, b \in \mathbb{R} \setminus \{0\}$.

Lemma 2.7. $(\mathbb{R}, \cdot)$ *ist keine Gruppe.*

Beweis. Angenommen, $(\mathbb{R}, \cdot)$ sei eine Gruppe. Dann wäre 1 das neutrale Element, da $a \cdot 1 = 1 \cdot a = a \; \forall a \in \mathbb{R}$. Sei nun n' das inverse Element zu 0, dann folgt $n' \cdot 0 = 0 \cdot n' = 1$. Das ist aber falsch, d.h. wir erhalten einen Widerspruch. Deshalb ist $(\mathbb{R}, \cdot)$ keine Gruppe. □

Bemerkung 2.8 (Widerspruchsbeweis)**.** *Wir haben hier einen Widerspruchsbeweis geführt. Dabei nehmen wir an, dass eine zu beweisende Aussage falsch ist und zeigen, dass das zu einem Widerspruch führt. Hat man den Widerspruch hergeleitet, verwendet man häufig das Symbol* $\lightning$ *.*

Bemerkung 2.9 (Negation von Aussagen mit Quantoren)**.** *Aussagen mit Quantoren sind manchmal von der Form*

$$\forall x \; \exists y \; : \; \textit{Aussage } A(x, y) \textit{ gilt.}$$

Die Negation dieser Aussage ist:

$$\exists x \; \forall y \; : \; \textit{Aussage } A(x, y) \textit{ gilt nicht.}$$

Beispiel (inverses Element bei der Gruppe)**.** *Sei* G *eine Menge und* $* : G \times G \to G$ *eine Verknüpfung mit neutralem Element* $e \in G$*. (iii) aus Definition 2.3 bedeutet*

$$\forall a \in G \; \exists a' \in G \; : \; a' * a = e$$

Die Negation ist

$$\exists a \in G \; \forall a' \in G \; : \; a' * a \neq e.$$

Genau das haben wir in Lemma 2.7 für $(G, *) = (\mathbb{R}, \cdot)$ *gezeigt.*

Analog ist die Negation von

$$\exists x \; \forall y \; : \; \text{Aussage } A(x, y) \text{ gilt.}$$

$$\forall x \; \exists y \; : \; \text{Aussage } A(x, y) \text{ gilt nicht.}$$

Lemma 2.10 (Kürzungsregel)**.** *Sei $(G, *)$ eine Gruppe, $a, b, c \in G$. Gilt $a * b = a * c$ oder $b * a = c * a$, so folgt $b = c$.*

Beweis. Gelte $a * b = a * c$.

$$\begin{aligned} &\Rightarrow && a' * (a * b) = a' * (a * c) \\ &\Rightarrow && (\underbrace{a' * a}_{=e}) * b = (a' * a) * c \\ &\Rightarrow && b = c. \end{aligned}$$

Die Aussage für $b * a = c * a$ folgt analog. □

Lemma und Definition 2.11 (Symmetrische Gruppe)**.** *Sei M eine Menge und*

$$S(M) := \{f : M \to M | \, f \text{ ist bijektiv}\}.$$

(i) Dann gilt: $(S(M), \circ)$ ist eine Gruppe, die sogenannte symmetrische Gruppe.

(ii) Ist $M = \{1, \ldots, n\}$, so heißt

$$(S(\{1, \ldots, n\}), \circ) := (S_n, \circ)$$

symmetrische Gruppe auf n Ziffern. Die Elemente von S_n heißen Permutationen und werden mit π bezeichnet (d.h. $\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$).

Beweis von (i). Die Verknüpfung $\circ$ ist als Abbildung von $S(M) \times S(M)$ nach $S(M)$ *wohldefiniert*, denn die Komposition bijektiver Abbildungen ist wieder bijektiv. Zudem gilt für $f, g, h \in S(M)$ das Assoziativgesetz $f \circ (g \circ h) = (f \circ g) \circ h$ nach Lemma 1.18; wegen $id_M \circ f = f \circ id_M = f \; \forall f \in S(M)$ ist id_M neutrales Element und für jedes $f \in S(M)$ ist die zugehörige Umkehrabbildung f^{-1} inverses Element: $f \circ f^{-1} = f^{-1} \circ f = id_M$. □

Bemerkung 2.12. *(i) Die Gruppe $(S(M); \circ)$ ist in der Regel nicht abelsch, da die Verknüpfung $f \circ g$ nicht kommutativ ist.*

(ii) Der Begriff "wohldefiniert" wird bei der Definition einer Abbildung $f : M \to N$ verwendet und bedeutet, dass die Zuordnung $m \mapsto f(m)$ eindeutig ist und alle Funktionswerte $f(m)$ im Wertebereich N der Abbildung liegen.

(iii) Die Elemente $\pi \in S_n$ kann man in der Form

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \pi(1) & \pi(2) & \ldots & \pi(n) \end{pmatrix}$$

schreiben (Permutationsschreibweise).

Beispiele.

$$S_1 = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$$

$$S_2 = \left\{ \underbrace{\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}}_{=id_{\{1,2\}}}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$$

$$S_3 = \left\{ \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}}_{=id_{\{1,2,3\}}}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \right.$$
$$\left. \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

Es gilt

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

d.h. $(S_3, \circ)$ *ist nicht abelsch.*

Bemerkung 2.13 (Zyklenschreibweise von S_n)**.**
Setze $\pi^j = \underbrace{\pi \circ \cdots \circ \pi}_{j-mal}$ *und* $\pi^{-j} = \underbrace{\pi^{-1} \circ \cdots \circ \pi^{-1}}_{j-mal}$*. Sei* $m \in \{1, \ldots, n\}$ *fest. Es gilt*

$$\{\pi(m), \pi^2(m), \pi^3(m), \ldots\} \subset \{1, \ldots, n\}.$$

$\Rightarrow \exists\, i, j, i \neq j,$ *mit* $\pi^i(m) = \pi^j(m)$*. Sei OE ("ohne Einschränkung")* $i > j$*.*

$$\Rightarrow \quad \underbrace{\pi^{-j}(\pi^i(m))}_{=\pi^{i-j}(m)} = \pi^{-j}(\pi^j(m)) = m$$

Sei nun $k \in \mathbb{N}$ *die kleineste natürliche Zahl mit* $\pi^k(m) = m$*. Wir stellen die Elemente* $m, \pi(m), \ldots, \pi^{k-1}(m)$ *in einem* Zyklus *dar:*

$$\underset{\longleftarrow}{\overset{\longrightarrow}{\Big(m}} \quad \overset{\longrightarrow}{\pi(m)} \quad \overset{\longrightarrow}{\pi^2(m)} \quad \overset{\longrightarrow}{\ldots} \quad \overset{\longrightarrow}{\pi^{k-1}(m)}\Big)$$

Die Elemente in einem Zyklus sind alle unterschiedlich (sonst wäre obiges k nicht das kleinste $k \in \mathbb{N}$ mit $\pi^k(m) = m$).

Beispiel:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 1 & 2 & 6 & 3 & 7 \end{pmatrix}$$
$$= (\ 1\ \ 5\ \ 6\ \ 3\ )(\ 2\ \ 4\ )(\ 7\ )$$

Die Elemente, die auf sich selbst abgebildet werden, lässt man dann noch weg und erhält

$$\pi = (\ 1\ \ 5\ \ 6\ \ 3\ )(\ 2\ \ 4\ ).$$

Konvention: $id = (\ )$.

Beispiel.

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \right.$$
$$\left. \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$
$$= \{(\ ), (\ 2\ \ 3\ ), (\ 1\ \ 2\ ), (\ 1\ \ 2\ \ 3\ ), (\ 1\ \ 3\ \ 2\ ), (\ 1\ \ 3\ )\}$$

Wir zeigen noch (mithilfe eines Widerspruchsbeweises), dass die Zyklen disjunkt sind:

Angenommen, die Zyklen sind nicht disjunkt.
$\Rightarrow \exists\, \bar{m} \notin \{m, \ldots, \pi^{k-1}(m)\}$ und $\exists\, i, j \in \mathbb{N}$ mit $\pi^i(\bar{m}) = \pi^j(m)$.
$\Rightarrow \underbrace{\pi^{-i}(\pi^i(\bar{m}))}_{=\bar{m}} = \pi^{-i+j}(m)$. $\Rightarrow \bar{m}$ ist Element des Zyklus' von m. $\lightning$
Der letzte Schluss gilt auch, wenn $j - i < 0$ ist, da $\pi^{-1}(m) = \pi^{k-1}(m)$ (mit $\pi^{-1}(m), \pi^{-2}(m)$, ... durchläuft man den Zyklus rückwärts).

Definition 2.14 (Gruppenhomomorphismus)**.** *Seien $(G, *)$, $(H, \circledast)$ Gruppen. Eine Abbildung $\varphi : G \to H$ heißt Gruppenhomomorphismus, wenn für alle $a, b \in G$ gilt*

$$\varphi(a * b) = \varphi(a) \circledast \varphi(b).$$

Ein Gruppenhomomorphismus heißt Gruppenisomorphismus, wenn er bijektiv ist.

Wir verwenden nachfolgend die Bezeichnung $\mathbb{R}_{>0} := \{x \in \mathbb{R} | \, x > 0\} = (0, \infty)$.

Beispiele 2.15. *(i) $\varphi : \mathbb{Z} \to \mathbb{Z}$, $a \mapsto 2a$, ist ein Gruppenhomomorphismus von $(\mathbb{Z}, +)$ nach $(\mathbb{Z}, +)$, denn $\varphi(a + b) = 2(a + b) = 2a + 2b = \varphi(a) + \varphi(b)$ $\forall\, a, b \in \mathbb{Z}$. φ ist aber kein Gruppenisomorphismus, denn φ ist nicht surjektiv ($1 \notin \varphi(\mathbb{Z})$).*

(ii) $\varphi : \mathbb{Z} \to \mathbb{Z}$, $a \mapsto a+1$, *ist kein Gruppenhomomorphismus von* $(\mathbb{Z}, +)$ *nach* $(\mathbb{Z}, +)$, *denn* $\varphi(2) = 3 \neq \varphi(1) + \varphi(1) = 4$.

(iii) $\varphi : \mathbb{R} \to \mathbb{R}_{>0}$, $x \mapsto e^x$, *ist ein Gruppenisomorphismus von* $(\mathbb{R}, +)$ *nach* $(\mathbb{R}_{>0}, \cdot)$. *Denn einerseits gilt* $\phi(x+y) = e^{x+y} = e^x \cdot e^y = \phi(x) \cdot \phi(y)$ $\forall\, x, y \in \mathbb{R}$, *andererseits ist* $\varphi : \mathbb{R} \to \mathbb{R}_{>0}$ *bijektiv.*

Lemma und Definition 2.16. *Seien* $(G, *)$ *und* $(H, \circledast)$ *Gruppen mit neutralen Elementen* $e_G \in G$ *bzw.* $e_H \in H$ *sowie* $\varphi : G \to H$ *ein Gruppenhomomorphismus. Dann gilt:*

(i) $\varphi(e_G) = e_H$.

(ii) Für alle $a \in G$ *ist* $\varphi(a') = \varphi(a)'$.

(iii) Ist φ *ein Gruppenisomorphismus, dann ist auch* $\varphi^{-1} : H \to G$ *ein Gruppenisomorphismus.*

$(G, *)$ *und* $(H, \circledast)$ *heißen* <u>isomorph</u> *(*$(G, *) \cong (H, \circledast)$*), wenn es einen Gruppenisomorphismus* $\varphi : G \to H$ *gibt.*

Beweis. (i) $e_H \circledast \varphi(e_G) = \varphi(e_G) = \varphi(e_G * e_G) = \varphi(e_G) \circledast \varphi(e_G) \overset{\text{Lemma } 2.10}{\Rightarrow} e_H = \varphi(e_G)$.

(ii) Es gilt $\varphi(a) \circledast \varphi(a') = \varphi(a * a') = \varphi(e_G) \overset{(i)}{=} e_H$, analog $\varphi(a') \circledast \varphi(a) = e_H$.
$\Rightarrow \varphi(a') = \varphi(a)'$.

(iii) φ ist bijektiv, d.h. φ^{-1} existiert und ist ebenfalls bijektiv. Zu zeigen: φ^{-1} ist Gruppenhomomorphismus.
Seien $c, d \in H$. Dann gilt

$$\begin{aligned}
\varphi^{-1}(c \circledast d) &= \varphi^{-1}\Big(\varphi\big(\varphi^{-1}(c)\big) \circledast \varphi\big(\varphi^{-1}(c)\big)\Big) \\
&= \varphi^{-1}\Big(\varphi\big(\varphi^{-1}(c) * \varphi^{-1}(d)\big)\Big) \qquad \text{(da } \varphi \text{ Gruppenhomomorphismus ist)} \\
&= \varphi^{-1}(c) * \varphi^{-1}(d).
\end{aligned}$$

□

Bemerkung. *Insbesondere gilt* $(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot)$ *nach Beispiel 2.15 (iii).*

Definition 2.17 (Untergruppe)**.** *Sei* $(G, *)$ *eine Gruppe und* $G' \subset G$ *eine nichtleere Teilmenge.* $(G', *)$ *heißt* <u>Untergruppe</u> *von* $(G, *)$*, wenn* $(G', *)$ *selbst eine Gruppe ist.*

In jeder Gruppe $(G, *)$ bildet die einelementige Teilmenge, die nur aus dem neutralen Element besteht, mit $*$ eine Untergruppe. Wir nennen sie die triviale Untergruppe. Ebenso ist natürlich die ganze Gruppe stets eine Untergruppe von sich selber.

Bemerkung 2.18. *Ist* $(G, *)$ *eine Gruppe und* $G' \subset G$ *eine nichtleere Teilmenge, so ist* $(G', *)$ *genau dann eine Untergruppe von* $(G, *)$*, wenn für beliebige* $a, b \in G'$ *auch* $a * b \in G'$ *sowie* $a' \in G'$ *gilt (Übungsblatt 4, Aufgabe 1 (i)).*

2.2 Ringe und Körper

Kurze Übersicht. Ringe und Körper sind Mengen mit zwei Verknüpfungen – einer Addition mit Gruppenstruktur und einer Multiplikation. Dabei gibt es im Ring bei der Multiplikation nicht zwangsläufig ein inverses Element der Multiplikation (wie in $\mathbb{Z}$, wo $3^{-1} = 1/3 \notin \mathbb{Z}$), während beim Körper $(K \setminus \{0\}, \cdot)$, d.h. die Menge K ohne das neutrale Element 0 der Addition zusammen mit der Multiplikation, auch eine Gruppe ist.

Definition 2.19 (Ring)**.** *Ein Ring ist ein Tripel $(R, +, \cdot)$ bestehend aus einer Menge R und zwei Verknüpfungen $+$ und $\cdot$,*

$$+ : R \times R \to R,\ (a, b) \mapsto a + b \quad \text{“Addition”}$$
$$\cdot : R \times R \to R,\ (a, b) \mapsto a \cdot b \quad \text{“Multiplikation”},$$

welche den folgenden drei Bedingungen genügen:

(i) $(R, +)$ *ist eine abelsche Gruppe. Das neutrale Element der Addition wird mit* $0 = 0_R$ *bezeichnet. Das inverse Element der Addition zu* a *wird mit* $-a$ *bezeichnet.*

(ii) Die Multiplikation ist assoziativ, d.h. für alle $a, b, c \in R$ *gilt*

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

(iii) Es gelten die Distributivgesetze, d.h. für alle $a, b, c \in R$ *gelten*

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{und}$$
$$(b + c) \cdot a = b \cdot a + c \cdot a.$$

Ein Ring heißt kommutativ, wenn $a \cdot b = b \cdot a$ *für alle* $a, b \in R$*. Ein Ring mit Einselement ist ein Ring, in dem ein Element* $1 = 1_R$ *existiert mit* $1_R \cdot a = a \cdot 1_R = a$ *für alle* $a \in R$*.*

Ohne Klammerung gilt die Konvention “$\cdot$” vor “$+$”.

Bemerkung. *Ist aus dem Zusammenhang klar, welche Verknüpfungen gemeint sind, werden diese bei der Angabe von Gruppen oder Ringen oft weggelassen. Man schreibt dann bspw. kurz “Sei R ein Ring.” statt “Sei $(R, +, \cdot)$ ein Ring.”.*

Lemma 2.20. *Sei $(R, +, \cdot)$ ein Ring. Dann gilt:*

(i) $0 \cdot a = a \cdot 0 = 0$ *für alle* $a \in R$ *und*

(ii) $a \cdot (-b) = -a \cdot b = (-a) \cdot b$ *für alle* $a, b \in R$*.*

Beweis. (i) Da 0 das neutrale Element der Ringaddition ist, gilt

$$0 \cdot a + 0 = 0 \cdot a = (0+0) \cdot a \overset{2.19(iii)}{=} 0 \cdot a + 0 \cdot a \overset{\text{Lemma } 2.10}{\Rightarrow} 0 = 0 \cdot a.$$

(ii) Da $-a$ das Inverse der Ringaddition zu a ist, gilt

$$0 \overset{\text{Lemma } 2.20(i)}{=} 0 \cdot b = (a + (-a)) \cdot b \overset{2.19(iii)}{=} a \cdot b + (-a) \cdot b \;\Rightarrow\; -a \cdot b = (-a) \cdot b.$$

Analog zeigt man $-a \cdot b = a \cdot (-b)$. □

Beispiel 2.21. *$(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit Einselement. Ebenso sind $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ kommutative Ringe mit Einselement. In $\mathbb{Q} \setminus \{0\}$ und $\mathbb{R} \setminus \{0\}$ gibt es darüberhinaus auch jeweils das inverse Element der Multiplikation ($\rightarrow$ Körper (s.u.)).*

Restklassenringe. Wir wollen jetzt noch ein weiteres Beispiel diskutieren: Sei $m \in \mathbb{N}$ beliebig. Zu jedem $a \in \mathbb{Z}$ gibt es dann bekanntlich eindeutig bestimmte ganze Zahlen q und r mit

$$a = qm + r \quad \text{und} \quad 0 \leq r < m \quad \text{(Übungsblatt 4, Aufgabe 3)}.$$

Setze $r_m(a) := r$ (Rest von a bei Division durch m). Sei $F_m := \{0, 1, 2, \ldots, m-1\}$. Wir definieren eine Addition $+_m$ sowie eine Multiplikation $\cdot_m$ auf F_m durch

$$a +_m b := r_m(a + b) \tag{2.1}$$

$$a \cdot_m b := r_m(a \cdot b). \tag{2.2}$$

Lemma 2.22. *(i) Es gelten folgende Rechenregeln. Für $a, b \in F_m$ ist*

$$r_m(a+b) = r_m(r_m(a) + b) = r_m(a + r_m(b)) = r_m(r_m(a) + r_m(b))$$
$$r_m(a \cdot b) = r_m(r_m(a) \cdot b) = r_m(a \cdot r_m(b)) = r_m(r_m(a) \cdot r_m(b)).$$

(ii) $(F_m, +_m, \cdot_m)$ ist ein kommutativer Ring mit Einselement. Er wird als Restklassenring modulo m bezeichnet.

Beweis. Übungsblatt 4, Aufgabe 2. □

Definition 2.23. *Sei $(R, +, \cdot)$ ein Ring. Er heißt nullteilerfrei, wenn für alle $a, b \in R$ gilt: Aus $a \cdot b = 0_R$ folgt $a = 0_R$ oder $b = 0_R$.*

Satz 2.24. *Sei $m \in \mathbb{N}$, $m > 1$. Dann sind äquivalent:*

(i) $(F_m, +_m, \cdot_m)$ ist nullteilerfrei.

(ii) m ist eine Primzahl.

Beweis. (i) $\Rightarrow$ *(ii)*: Wir zeigen die Umkehrung $\neg$(ii) $\Rightarrow \neg$(i) (dies ist äquivalent zur Implikation (i) $\Rightarrow$ (ii) – ein sogenannter indirekter Beweis). Sei m keine Primzahl. Dann gibt es $a, b \in \mathbb{N}$ mit $1 < a$, $b < m$ und $m = a \cdot b$. Es folgt $a \cdot_m b = r_m(a \cdot b) = r_m(m) = 0$, d.h. F_m ist nicht nullteilerfrei.

(ii) $\Rightarrow$ (i): Seien m eine Primzahl und $a, b \in F_m$ mit $a \cdot_m b = 0$. Zz: $a = 0$ oder $b = 0$. Wegen $a \cdot_m b = r_m(a \cdot b) = 0$ gibt es ein $q \in \mathbb{Z}$ mit $a \cdot b = q \cdot m$. $\overset{m \text{ Primzahl}}{\Rightarrow}$ m teilt a oder m teilt b. $\overset{a,b<m}{\Rightarrow}$ $a = 0$ oder $b = 0$. □

Definition 2.25 (Körper)**.** *Ein Körper ist ein kommutativer Ring $(K, +, \cdot)$ mit Einselement, in dem zusätzlich gilt: $(K \setminus \{0_K\}, \cdot)$ ist eine abelsche Gruppe mit neutralem Element 1_K. Damit besitzt jedes von 0_K veschiedene Element $a \in K$ ein Inverses bzgl. der Verknüpfung "$\cdot$", welches wir mit a^{-1} (oder auch $1/a$) bezeichnen.*

Bemerkung. *Per definitionem gilt $0_K \neq 1_K$.*

Beispiele 2.26. *(i) $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind Körper.*

(ii) $(\mathbb{Z}, +, \cdot)$ ist kein Körper, da es zu $a \notin \{-1, 1\}$ kein inverses Element der Multiplikation gibt.

Satz 2.27. *Sei K ein Körper. Dann ist K nullteilerfrei.*

Beweis (durch Widerspruch). Angenommen, K ist nicht nullteilerfrei.
Dann gibt es $a, b \in K$ mit $a \neq 0$, $b \neq 0$ und $a \cdot b = 0$.
$\Rightarrow \exists\, a^{-1}$ mit $a \cdot a^{-1} = 1$ und $\exists\, b^{-1}$ mit $b \cdot b^{-1} = 1$.
$\Rightarrow \underbrace{a \cdot b}_{=0} \cdot a^{-1} \cdot b^{-1} \overset{\text{Kommutativität}}{=} a \cdot a^{-1} \cdot b \cdot b^{-1} = 1 \cdot 1 = 1$. ↯

□

Satz 2.28. *Sei $(F_m, +_m, \cdot_m)$ wie oben der Restklassenring modulo m. F_m ist genau dann ein Körper, wenn m eine Primzahl ist.*

Beweis.

"$\Rightarrow$": Sei F_m ein Körper. $\overset{\text{Satz } 2.27}{\Rightarrow}$ F_m ist nullteilerfrei. $\overset{\text{Satz } 2.24}{\Rightarrow}$ m ist eine Primzahl.

"$\Leftarrow$": Sei nun m eine Primzahl.

$\overset{\text{Lemma } 2.22 \text{ und Satz } 2.24}{\Rightarrow}$ F_m ist nullteilerfreier, kommutativer Ring mit Einselement.

Zz: F_m ist ein Körper. Dafür fehlt nur die Existenz des Inversen a^{-1} zu $a \neq 0$.

Sei nun $a \in F_m \setminus \{0\}$. Betrachte die Abbildung

$$\begin{aligned} F_m &\to F_m \\ x &\mapsto x \cdot_m a. \end{aligned}$$

Die Abbildung ist injektiv, da aus $x \cdot_m a = y \cdot_m a$ folgt, dass $(x-y) \cdot_m a = 0$ (nach dem Distributivgesetz und Lemma 2.20 (ii)) und somit wegen der Nullteilerfreiheit $x - y = 0$, d.h. $x = y$. Damit sind die Elemente $0 \cdot_m a, \ldots, (m-1) \cdot_m a$ alle verschieden. Da F_m nur m Elemente enthält, ist die Abbildung folglich surjektiv und es existiert insbesondere ein $x \in F_m$ mit $x \cdot_m a = 1$.

□

Bemerkung 2.29. *In unserem Beispiel besteht F_m aus den Zahlen $\{0, 1, \ldots, m-1\}$ und $+_m$ sowie $\cdot_m$ sind Verknüpfungen darauf. Der sogenannte Restklassenring F_m wird aber häufig anders eingeführt. Und zwar definiert man auf $\mathbb{Z}$ die Äquivalenzrelation $\sim_m$ durch*

$$x \sim_m y :\Leftrightarrow \; r_m(x) = r_m(y).$$

Die m-elementige Quotientenmenge $\mathbb{Z}/\sim_m$ wird mit $\mathbb{Z}/m\mathbb{Z}$ bezeichnet; ihre Elemente – die Äquivalenzklassen – sind Teilmengen ganzer Zahlen, die jeweils bei Division mit m denselben Rest besitzen. D.h. zwei Zahlen $x, y \in \mathbb{Z}$ liegen genau dann in derselben Äquivalenzklasse, wenn ihre Differenz $x-y$ durch m teilbar ist. Auf der Quotientenmenge $\mathbb{Z}/\sim_m$ definiert man nun die Verknüpfungen $+$ und $\cdot$ von Äquivalenzklassen mithilfe ihrer Repräsentanten durch $+_m$ aus (2.1) und $\cdot_m$ aus (2.2) (wobei hier die Wohldefiniertheit zu prüfen ist!) → Übungsblatt 4, Aufgabe 2. Da aber die m Elemente von F_m gerade Repräsentanten der m verschiedenen Äquivalenzklassen von $\mathbb{Z}/\sim_m$ sind, gelten alle obigen Ergebnisse für F_m entsprechend dann auch für $\mathbb{Z}/m\mathbb{Z}$. Für eine Primzahl p ist $\mathbb{Z}/p\mathbb{Z}$ nach Satz 2.28 ein Körper und heißt Primkörper der Charakteristik p.

2.2.1 Der Körper $\mathbb{C}$ der komplexen Zahlen

In $\mathbb{R}$ kann man Wurzeln aus allen positiven Zahlen ziehen, nicht jedoch aus negativen. Das bringt die Idee auf, die reellen Zahlen zu erweitern.

Definition 2.30. *Die komplexen Zahlen sind definiert als $\mathbb{C} = \mathbb{R}^2$ mit den Verknüpfungen*

$$(a,b) + (c,d) := (a+c, b+d) \quad \text{und} \tag{2.3}$$

$$(a,b) \cdot (c,d) := (ac - bd, ad + bc) \tag{2.4}$$

für alle $a, b, c, d \in \mathbb{R}$.

Satz 2.31. *$\mathbb{C}$ bildet mit der Addition (2.3) und der Multiplikation (2.4) einen Körper.*

Beweis. Dass $(\mathbb{C}, +)$ eine abelsche Gruppe mit neutralem Element $(0,0)$ ist, ist klar. Dass $\mathbb{C}\setminus\{(0,0)\}$ eine abelsche Gruppe bezüglich der Multiplikation ist, wurde auf Übungsblatt 3, Aufgabe 1c) gezeigt. Die Distributivgesetze rechnet man unmittelbar nach. □

Das neutrale Element der Addition ist $0_{\mathbb{C}} = (0,0)$, das neutrale Element der Multiplikation $1_{\mathbb{C}} = (1,0)$. Für (a,b) ist das additive Inverse $-(a,b) = (-a,-b)$, für $(a,b) \neq 0_{\mathbb{C}}$ das multiplikative Inverse

$$(a,b)^{-1} = \left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right).$$

Die Abbildung $\mathbb{R} \to \mathbb{C}$, $a \mapsto (a,0)$, definiert einen Körperhomomorphismus (Übungsblatt 4, Aufgabe 4). Wir können folglich $\mathbb{R}$ mit komplexen Zahlen identifizieren, deren zweite Komponente gleich Null ist. Definieren wir schließlich $i = (0,1)$ (die sogenannte imaginäre Einheit), erhalten wir die Darstellung $(a,b) = (a,0) + b \cdot (0,1) = a + bi$ für alle $a, b \in \mathbb{R}$. Insbesondere können wir damit 0 und 1 für $0_{\mathbb{C}}$ und $1_{\mathbb{C}}$ schreiben. Für die imaginäre Einheit i gilt $i^2 = (0,1) \cdot (0,1) = (-1,0) = -1_{\mathbb{C}} = -1$, d.h. -1 besitzt nun eine Wurzel in $\mathbb{C}$.

2.2.2 Der Polynomring $R[t]$

Sei R ein Ring und t eine sogenannte Unbestimmte. Unter einem Polynom über R in der Unbestimmten t versteht man einen Ausdruck der Form

$$P(t) = a_0 + a_1 \cdot t + \cdots + a_n \cdot t^n$$

mit $a_0, \ldots, a_n \in R$ und $n \in \mathbb{N}_0$. Dabei kann als Unbestimmte t all das eingesetzt werden, für was die rechte Seite sinnvoll ist (insbesondere müssen Vielfache und Potenzen definiert sein). $a_0, a_1, \ldots, a_n$ heißen Koeffizienten des Polynoms. Die Menge dieser Polynome wird mit $R[t]$ bezeichnet. Oft lässt man bei einem Polynom die Angabe der Unbestimmten weg und schreibt kurz P. Sind alle Koeffizienten des Polynoms gleich Null, nennt man es Nullpolynom ($P = 0$). Der Grad des Polynoms P wird definiert als

$$deg(P) := \begin{cases} \infty & \text{falls } P = 0, \\ \max\{\nu \in \mathbb{N}_0 |\, a_\nu \neq 0\} & \text{sonst,} \end{cases}$$

wobei die Festlegung für den Grad des Nullpolynoms in der Literatur nicht einheitlich ist. Natürlich kann man für die Unbestimmte t ein Element von R selbst einsetzen. Ist $\lambda \in R$, so ist auch $P(\lambda) = a_0 + a_1 \cdot \lambda + \cdots + a_n \cdot \lambda^n \in R$. Damit erhält man eine Abbildung

$$\begin{aligned} \tilde{P}: \; & R \to R \\ & \lambda \mapsto P(\lambda). \end{aligned}$$

Warum man zwischen P und $\tilde{P}$ so penibel unterscheidet, demonstriert folgendes Beispiel.

Beispiel 2.32. *Sei $F_2 = \{0,1\}$ der Restklassenring modulo 2 und $P(t) = 1 \cdot_m t +_m 1 \cdot_m t^2$.*

Dann gelten

$$P(0) = 0 +_m 0 \cdot_m 0 \overset{\text{Lemma } 2.20}{=} 0 +_m 0 = 0,$$
$$P(1) = 1 +_m 1 \cdot_m 1 = 1 +_m 1 = 0.$$

Damit ist zwar $\tilde{P}$ die Nullabbildung, d.h. $\tilde{P}(x) = 0 \ \forall x \in F_2$, aber P ist nicht das Nullpolynom, d.h. $P \neq 0$.

Auf $R[t]$ kann man nun zwei Verknüpfungen, eine Addition und eine Multiplikation, einführen. Um die Notation zu vereinfachen, verwenden wir auch für die Polynomring-Addition und -Multiplikation die Zeichen $+$ und $\cdot$. Seien

$$P(t) = a_0 + a_1 \cdot t + \cdots + a_n \cdot t^n \quad \text{und} \quad Q(t) = b_0 + b_1 \cdot t + \cdots + b_m \cdot t^m$$

zwei Elemente aus $R[t]$. Ohne Einschränkung gelte für die nachfolgenden Definitionen $m = n$ (andernfalls ergänzen wir $b_{m+1} = \cdots = b_n = 0$ falls $m < n$ und $a_{n+1} = \ldots a_m = 0$ falls $m > n$). Wir definieren

$$P(t) + Q(t) := (a_0 + b_0) + (a_1 + b_1) \cdot t + \cdots + (a_n + b_n) \cdot t^n$$
$$P(t) \cdot Q(t) := c_0 + c_1 \cdot t + \cdots + c_{m+n} \cdot t^{n+m} \quad \text{mit} \quad c_k = \sum_{\substack{i,j \in \{0,\ldots,n\}: \\ i+j=k}} a_i \cdot b_j.$$

Satz und Definition 2.33. *Sei R ein Ring. Dann gelten folgende Aussagen:*

(i) *$(R[t], +, \cdot)$ ist ein Ring; er heißt Polynomring über R.*

(ii) *Ist R kommutativ, so auch $R[t]$.*

(iii) *Ist R nullteilerfrei, so gilt $deg(P \cdot Q) = deg(P) + deg(Q)$.*
(Hier gilt die Konvention $n + \infty = \infty + m = \infty + \infty = \infty \ \forall m, n \in \mathbb{N}_0$.)

Beweis. Übungsblatt 5, Aufgabe 1. □

In Analogie zur Division mit Rest bei ganzen Zahlen verfährt man beim Polynomring $K[t]$ über einem Körper K.

Satz 2.34. *Seien K ein Körper und $K[t]$ der Polynomring über K. Dann gibt es zu $P, Q \in K[t]$ eindeutig bestimmte Polynome $q, r \in K[t]$ mit folgenden Eigenschaften:*

(i) *$P = Q \cdot q + r$ sowie*

(ii) *$deg(r) < deg(Q)$, falls $r \neq 0$.*

Beweis. Eindeutigkeit: Seien $q, r, q', r' \in K[t]$ mit

$$P = Q \cdot q + r \quad \text{und } deg(r) < deg(Q), \text{ falls } r \neq 0$$
$$P = Q \cdot q' + r' \quad \text{und } deg(r') < deg(Q), \text{ falls } r' \neq 0.$$

Dann gilt nach Lemma 2.20 (ii) und dem Distributivgesetz $Q \cdot (q + (-q')) = (r' + (-r))$. Sind $r \neq 0$ und $r' \neq 0$, folgt

$$deg(r' + (-r)) \leq \max\big(deg(r), deg(-r')\big) < deg(Q) \text{ falls } r \neq r'.$$

Aber $q + (-q') \neq 0$ impliziert

$$deg(r' + (-r)) = deg\big(Q \cdot (q + (-q'))\big) = deg(Q) + deg\big(q + (-q')\big) \geq deg(Q),$$

was nicht sein kann, womit $q + (-q') = 0$ und damit $r' + (-r) = 0$.

Sind $r = 0$ und $r' \neq 0$, ist einerseits $deg(r') < deg(Q)$, andererseits folgt wie oben $deg(r') \geq deg(Q)$, was unmöglich ist, womit auch $r' = 0$. Aber mit $r = r' = 0$ folgt aus $\infty = deg(Q \cdot (q + (-q')) = deg(Q) \cdot deg(q + (-q'))$ auch $q - q' = 0$.

Existenz: Existiert ein $q \in K[t]$ mit $P = Q \cdot q$, folgt die Aussage mit $r = 0$. Andernfalls gilt $P + (-Q \cdot p) \neq 0$ für alle Polynome $p \in K[t]$, insbesondere $deg(P + (-Q \cdot p)) \geq 0$. Wir wählen nun ein $q \in K[t]$ mit der Eigenschaft

$$deg\big(P + (-Q \cdot q)\big) \leq deg\big(P + (-Q \cdot p)\big) \quad \text{für alle } p \in K[t].$$

Mit $r := P + (-Q \cdot q)$ gilt dann (i). Zu zeigen bleibt hierfür (ii), was wir nachfolgend durch Widerspruch beweisen. Angenommen, $deg(r) \geq deg(Q)$. Ist

$$Q = b_0 + b_1 \cdot t + \cdots + b_m \cdot t^m \quad \text{und} \quad r = c_0 + c_1 \cdot t + \cdots + c_k \cdot t^k$$

mit $b_m \neq 0$ und $c_k \neq 0$ für $k \geq m$, definieren wir $p := q + \frac{c_k}{b_m} \cdot t^{k-m}$. Aber dann folgt

$$r + \Big(- Q \cdot \Big[\frac{c_k}{b_m} \cdot t^{k-m}\Big]\Big) = P + \Big(- Q \cdot q + Q \cdot \Big[\frac{c_k}{b_m} \cdot t^{k-m}\Big]\Big) = P + (-Q \cdot p).$$

Da r und $Q \cdot [\frac{c_k}{b_m} \cdot t^{k-m}]$ denselben höchsten (von Null verschiedenen) Koeffizienten haben, ergibt sich weiter

$$deg\Big(r + \Big(- Q \cdot \Big[\frac{c_k}{b_m} \cdot t^{k-m}\Big]\Big)\Big) < deg(r),$$

also $deg(P + (-Q \cdot p)) < deg(r)$. ↯ □

Nach diesen Überlegungen kommen wir nun zu einer wesentlichen Frage – nämlich der nach der Existenz von Nullstellen.

Das nächste Lemma zeigt, dass man bei einem Polynom den Linearfaktor $(t - \lambda)$ abspalten kann, wenn λ eine Nullstelle ist.

Lemma 2.35. *Ist $\lambda \in K$ eine Nullstelle von $P \in K[t]$, $P \neq 0$, so existiert ein eindeutiges Polynom $Q \in K[t]$ mit*

$$P = (t - \lambda) \cdot Q \quad \text{und} \quad deg(Q) = deg(P) - 1.$$

Beweis. Nach Satz 2.34 gibt es eindeutig bestimmte $Q, r \in K[t]$ mit $P = (t - \lambda) \cdot Q + r$ und $deg(r) < deg(t - \lambda) = 1$ falls $r \neq 0$. Damit ist $r = a_0$ mit $a_0 \in K$. Wegen $P(\lambda) = 0$ folgt

$$0 = P(\lambda) = (\lambda - \lambda) \cdot Q(\lambda) + a_0 = a_0,$$

d.h. $r = 0$ und $P = (t - \lambda) \cdot Q$ ist gezeigt. $deg(Q) = deg(P) - 1$ folgt dann aus

$$deg(P) = deg((t - \lambda) \cdot Q) = deg(t - \lambda) + deg(Q) = 1 + deg(Q). \qquad \square$$

Korollar 2.36. *Seien K ein Körper, $P \in K[t]$ ein Polynom und k die Anzahl der Nullstellen von P. Ist $P \neq 0$, so gilt $k \leq deg(P)$.*

Beweis. Wir beweisen die Aussage durch vollständige Induktion nach dem Grad des Polynoms.

Induktionsanfang: Ist $deg(P) = 0$, so ist $P = a_0 \neq 0$ ein konstantes Polynom. Dieses hat aber keine Nullstelle, also ist die Behauptung korrekt.

Induktionsschritt: Sei die Aussage für Polynome $Q \in K[t]$ mit $deg(Q) \leq n - 1$, $n \in \mathbb{N}$, bereits bewiesen. Sei $P \in K[t]$ mit $deg(P) = n$. Besitzt P keine Nullstelle, so ist die Behauptung richtig. Ist andernfalls $\lambda \in K$ Nullstelle von P, so existiert nach Lemma 2.35 $Q \in K[t]$ mit $P = (t-\lambda)\cdot Q$ und $deg(Q) = n-1$. Alle von λ verschiedenen Nullstellen von P müssen folglich auch welche von Q sein. Nach Induktionsannahme besitzt Q aber höchstens $n - 1$ Nullstellen, womit $k \leq (n - 1) + 1 = n$ ist. $\square$

Über dem Körper $K = \mathbb{R}$ gibt es Polynome P mit $deg(P) > 0$, die keine Nullstelle besitzen.

Beispiel 2.37. *Sei $K = \mathbb{R}$ und $P(t) = t^2 + 1$ für $t \in \mathbb{R}$, so ist $P(t) \geq 1$ für alle $t \in \mathbb{R}$ und P besitzt insbesondere in $\mathbb{R}$ keine Nullstelle.*

Über dem Körper $\mathbb{C}$ gibt es ein solches Beispiel jedoch nicht.

Satz 2.38 (Fundamentalsatz der Algebra)**.** *Jedes Polynom $P \in \mathbb{C}[t]$ mit $deg(P) > 0$ hat mindestens eine Nullstelle.*

Beweis. Später. $\square$

3 Vektorräume

Hier wird noch eine Zeichnung eingefügt.

Definition 3.1. *Sei K ein Körper. Eine Menge V mit einer Addition*

$$+ : V \times V \to V,\ (v, w) \mapsto v + w$$

und einer skalaren Multiplikation

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

heißt <u>K-Vektorraum</u> (K-VR), falls Folgendes gilt:

(i) $(V,)$ *ist eine abelsche Gruppe. Das neutrale Element wird mit* $0 = 0_V$*, das zu* $v \in V$ *inverse Element mit* $-v$ *bezeichnet.*

(ii) Für die skalare Multiplikation gelten folgende Axiome: Für alle $\lambda, \mu \in K$ *und alle* $v, w \in V$ *gilt*

$$\begin{aligned}
&(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v \\
&\lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w \\
&\lambda \cdot (\mu \cdot v) = (\lambda \cdot \mu) \cdot v \\
&1 \cdot v = v.
\end{aligned}$$

Konventionen: "+" vor "·", $\lambda v := \lambda \cdot v$.

Bemerkung. *Es ist wichtig, zwischen skalarer Multiplikation und Multiplikation in K sowie zwischen Addition in V und Addition in K zu unterscheiden.*

Beispiele 3.2. *(i) K Körper, $n \in \mathbb{N}$, $K^n = \{(x_1, \ldots, x_n) |\ x_1, \ldots, x_n \in K\}$ mit*

Addition $(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$ *und*

Skalarmultiplikation $\lambda \cdot (x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n)$

ist ein Vektorraum über K (der sog. <u>Standard-Vektorraum</u>). Es gelten $0 = (0, \ldots, 0)$ *und* $-(x_1, \ldots, x_n) = (-x_1, \ldots, -x_n)$.

[Die Axiome aus der obigen Definition muss man nachrechnen.]

(ii) Seien M eine Menge und K ein Körper. Wir definieren

$$\begin{aligned}
Abb(M, K) :=& \{f |\ f \text{ ist eine Abbildung } f : M \to K\} \\
=& \{f : M \to K\} \text{ (Kurzschreibweise)}
\end{aligned}$$

$V = Abb(M, K)$ wird mit folgenden Verknüpfungen zu einem Vektorraum:

$$(f+g)(x) := f(x) + g(x) \ \forall\, x \in M \quad \textit{(Addition)}$$
$$(\lambda \cdot f)(x) := \lambda \cdot f(x) \ \forall\, x \in M \quad \textit{(Skalarmultiplikation).}$$

Bemerkung 3.3 (Notation). *(i) Vektoren (die Elemente) eines Vektorraums V werden oft besonders gekennzeichnet, bspw. mit einem Pfeil $\vec{v}$ oder fett gedruckt $\mathbf{v}$. Wir verzichten auf weitere Kennzeichnungen und verwenden vor allem die Buchstaben u, v, w.*

(ii) Vektoren (vor allem) aus dem K^n werden oft als Spalten geschrieben, d.h.

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \quad \textit{anstelle der Zeilenform} \quad (x_1, \ldots, x_n).$$

Lemma 3.4. *Sei K ein Körper, V ein K-VR. Dann gilt:*

(i) $0_K \cdot v = 0_V \ \forall\, v \in V$

(ii) $\lambda \cdot 0_V = 0_V \ \forall\, \lambda \in K$

(iii) $\lambda \cdot v = 0 \Rightarrow \lambda = 0_K$ *oder* $v = 0_V$

(iv) $(-1) \cdot v = -v \ \forall\, v \in V$.

Beweis. (i) und (ii) folgen mit der Kürzungsregel (Lemma 2.10), (iv) ist einfach. (iii): Seien $\lambda \in K, v \in V$ mit $\lambda \cdot v = 0$. Ist $\lambda \neq 0_K$, so folgt $v = 1 \cdot v = (\lambda^{-1}\lambda) \cdot v = \lambda^{-1} \cdot (\lambda \cdot v) = \lambda^{-1} \cdot 0_V \overset{(ii)}{=} 0_V$. □

3.1 Untervektorräume und lineare Hülle

Definition 3.5. *Seien K ein Körper und V ein K-Vektorraum. $W \subset V$ mit $W \neq \emptyset$ heißt Untervektorraum (kurz UVR) von V, falls W mit den eingeschränkten Verknüpfungen selbst ein Vektorraum ist.*

Lemma 3.6. *Eine Teilmenge $W \neq \emptyset$ eines K-VRs V ist genau dann ein Untervektorraum von V, falls gilt:*

(i) $u, v \in W \Rightarrow u + v \in W$
(d.h. W ist abgeschlossen unter der Addition)

(ii) $\lambda \in K,\ w \in W \Rightarrow \lambda \cdot w \in W$
(d.h. W ist abgeschlossen unter der skalaren Multiplikation).

Beweis. "⇒": Ist W selbst ein K-VR, so gelten natürlich die beiden Bedingungen (i) und (ii).

"⇐": Wir nehmen an, dass (i) und (ii) gelten. Für die Aussage "W ist K-VR" müssen wir die Existenz des inversen Elements und des neutralen Elements der Addition zeigen:

- Sei $w \in W$. $\Rightarrow -w \overset{\text{Lemma } 3.4(iv)}{=} (-1) \cdot w \in W$ nach (ii).
- Sei w ein beliebiges Element aus $W \Rightarrow -w \in W \Rightarrow 0_V = w + (-w) \in W$ nach (i). 0_V ist aber auch das neutrale Element in W, da ja $w + 0_V = w$. $0_V + w = w$ $\forall\, w \in W$.

□

Beispiele 3.7. *Was sind Untervektorräume von $V = \mathbb{R}^2$?*

(i) $W = \{(0,0)\}$,

(ii) $W = V = \mathbb{R}^2$,

(iii) alle Geraden durch den Ursprung.

Beweis von (iii). Bis auf die senkrechte Gerade kann man alle Geraden durch den Ursprung als Menge

$$W = \{(x, mx) |\, x \in \mathbb{R}\}$$

schreiben mit $m \in \mathbb{R}$. Hier gilt für alle $v = (x, mx)$ und $w = (y, my) \in W$:

$(x, mx) + (y, my) = (x + y, m(x + y)) \in W$ sowie

$\lambda \cdot (x, mx) = (\lambda x, m \cdot (\lambda x)) \in W$, womit nach Lemma 3.6 W UVR von $\mathbb{R}^2$ ist.

Für die senkrechte Gerade durch den Ursprung $\{(0, y) | y \in \mathbb{R}\}$ geht der Beweis analog.

□

Der nächste Satz sagt, dass $\mathbb{R}^2$ neben diesen Beispielen keine weiteren Untervektorräume besitzt.

Satz 3.8. *Sei $V = \mathbb{R}^2$ und $W \subset V$ mit $W \neq \emptyset$. Dann ist W ein UVR von V genau dann, wenn $W = \{(0,0\}$, $W = \mathbb{R}^2$ oder W eine Gerade durch den Ursprung ist, d.h. entweder $W = \{(x, \lambda_0 x) |\, x \in \mathbb{R}\}$ für ein $\lambda_0 \in \mathbb{R}$ oder $W = \{(0, y) |\, y \in \mathbb{R}\}$.*

Beweis. "⇐": Haben wir gezeigt.

"⇒": Sei W ein anderer Vektorraum als $W = \{(0,0)\}$, $W = \mathbb{R}^2$ oder $W = \{(0, y) |\, y \in \mathbb{R}\}$ und $(w_2^*, w_2^*) \in W$ ein Punkt mit $w_1^* \neq 0$. Ein solcher muss existieren, denn außer $\{(0,0)\}$ bildet keine echte Teilmenge von $\{(0, y) |\, y \in \mathbb{R}\}$ einen UVR. Setze $\lambda_0 := w_2^*/w_1^*$.

Wir zeigen: $W = \{(x, \lambda_0 x) |\, x \in \mathbb{R}\}$.

"$\supset$": Sei $x \in \mathbb{R}$.

$$\Rightarrow \qquad (x, \lambda_0 x) = \left(x, \frac{w_2^*}{w_1^*} x\right) = \frac{x}{w_1^*}(w_1^*, w_2^*) \in W,$$

da W ein UVR ist.

"$\subset$": Sei nun (w_1, w_2) ein beliebiges anderes Element aus W. Wir müssen zeigen, dass (w_1, w_2) auf der Geraden liegt, d.h., dass $w_2 = \lambda_0 w_1$ gilt.

Widerspruchsbeweis:

Annahme: Gelte $w_2 \neq \lambda_0 w_1$. Wir zeigen, dass dann bereits $W = \mathbb{R}^2$ gelten muss, d.h., dass dann jedes $(z_1, z_2) \in \mathbb{R}^2$ in W liegt.

Sei dafür $(z_1, z_2) \in \mathbb{R}^2$ beliebig. Wir setzen

$$a = \frac{\lambda_0 z_1 - z_2}{w_1 \lambda_0 - w_2}, \quad \text{und} \quad b = \frac{w_1 z_2 - w_2 z_1}{w_1 \lambda_0 - w_2}$$

(der Nenner ist $\neq 0$ wegen $w_2 \neq \lambda_0 w_1$). Damit ist aber

$$(z_1, z_2) = \underbrace{a \cdot (w_1, w_2)}_{\in W} + \underbrace{b \cdot (1, \lambda_0)}_{\in W},$$

also $(z_1, z_2) \in W$. $\lightning$ Somit gilt $w_2 = \lambda_0 w_1$. □

Bemerkung 3.9. *Die Frage "Wie kommt man auf obiges a und b?" ist für die Gültigkeit des Beweises nicht relevant – wohl aber für das "Finden" des Beweises: Man muss dafür das Gleichungssystem*

$$z_1 = a w_1 + b$$
$$z_2 = a w_2 + b \lambda_0$$

mit a, b unbekannt bei bekannten w_1, w_2, z_1, z_2 lösen (z. Bsp. indem man $b = z_1 - a w_1$ in die zweite Gleichung einsetzt).

Bemerkung 3.10. *Für Abbildungen $f : \mathbb{R} \to \mathbb{R}$ haben wir damit gezeigt:*

$$\{(x, f(x)) | \, x \in \mathbb{R}\} \quad \textit{ist UVR von } \mathbb{R}^2 \;\Leftrightarrow\; f(x) = \lambda_0 x \quad \textit{für ein } \lambda_0 \in \mathbb{R}.$$

Satz 3.11. *Sei K ein Körper, V ein K-VR, I eine Indexmenge und $(W_i)_{i \in I}$ eine Familie von Untervektorräumen von V (d.h. für jedes $i \in I$ ist W_i ein UVR von V). Dann gilt*

$$W = \bigcap_{i \in I} W_i = \{w \in V | \, w \in W_i \textit{ für alle } i \in I\}$$

ist ein UVR von V.
("Beliebige Durchschnitte von Untervektorräumen sind wieder Untervektorräume").

Beweis. $0_V \in W$, d.h. $W \neq \emptyset$. Wir weisen (i) und (ii) aus Lemma 3.6 nach.

(i) Seien $v, w \in W$.
$\Rightarrow v, w \in W_i \ \forall\, i \in I$
$\Rightarrow u + v \in W_i \ \forall\, i \in I$
$\Rightarrow v + w \in \cap_{i \in I} W_i = W$.

(ii) Seien $\lambda \in K$, $v \in W$.
$\Rightarrow v \in W_i \ \forall\, i \in I$
$\Rightarrow \lambda v \in W_i \ \forall\, i \in I$
$\Rightarrow \lambda v \in \cap_{i \in I} W_i = W$. □

Um die Notation weiter zu vereinfachen, lassen wir nachfolgend (wie gerade bereits im Beweis) den Punkt $\cdot$ bei der Skalarmultiplikation meistens weg.

Beispiel 3.12. *Die Vereinigung von UVRs ist im Allgemeinen kein UVR. Man betrachte z.Bsp.* $K = \mathbb{R}$, $V = \mathbb{R}^2$

$$W_1 = \{(x_1, x_2) \in \mathbb{R}^2 | \, x_1 = x_2\}$$
$$W_2 = \{(x_1, x_2) \in \mathbb{R}^2 | \, x_1 = 0\}.$$

W_1 und W_2 sind UVRs. Aber $W_1 \cup W_2$ ist kein UVR, da bspw. $(1,1) \in W_1 \subset W_1 \cup W_2$ *und* $(0,1) \in W_2 \subset W_1 \cup W_2$, *aber* $(1,1) + (0,1) = (1,2) \notin W_1 \cup W_2$.

Dass $W_1 \cup W_2$ kein UVR sein kann, folgt natürlich auch bereits aus Satz 3.8.

Definition 3.13. *Seien K ein Körper und V ein K-VR.*

(i) Seien $r \in \mathbb{N}$, $v_1, \ldots, v_r \in V$ und $a_1, \ldots, a_r \in K$. Der Ausdruck

$$v = a_1 v_1 + \cdots + a_r v_r$$

heißt Linearkombination von $v_1, \ldots, v_r$. Es gilt $v \in V$.

(ii) Ist $M = \{v_1, \ldots, v_r\} \subset V$ für ein $r \in \mathbb{N}$, so heißt

$$\mathrm{Lin}(M) := \{a_1 v_1 + \cdots + a_r v_r | \, a_1, \ldots, a_r \in K\}$$

lineare Hülle von M.

(iii) Ist $M \subset V$ beliebig, $M \neq \emptyset$, so heißt

$$\mathrm{Lin}(M) := \bigcup_{\substack{L \subset M: \\ L \text{ endlich}}} \mathrm{Lin}(L)$$

die lineare Hülle von M. Wir setzen $\mathrm{Lin}(\emptyset) = \{0\}$.

Bemerkung 3.14. *Für unendliche Mengen M (d.h. Mengen M mit mehr als endlich vielen Elementen) gilt damit:*

$$v \in \mathrm{Lin}(M)$$

$$\Leftrightarrow$$

$\exists$ *endliche Teilmenge* $\{v_1, \ldots, v_s\} \subset M$ *und* $\exists\, a_1, \ldots, a_s \in K$ *mit* $v = a_1 v_1 + \cdots + A_s v_s$.

D.h. die lineare Hülle von unendlich vielen Vektoren besteht aus allen Linearkombinationen von je endlich vielen.

Beispiele 3.15. *(i) In Satz 3.8 haben wir die Gerade* $W = \{(x, \lambda_0 x) | x \in \mathbb{R}\}$ *betrachtet und dann im Beweis den Vektor* $(1, \lambda_0) \in W$. *Wegen* $(x, \lambda_0 x) = x(1, \lambda_0)$ *gilt* $W = \mathrm{Lin}(\{(1, \lambda_0)\})$.

(ii) Im Beweis von Satz 3.8 wurde dann gezeigt, dass jeder beliebige Vektor $(z_1, z_2) \in \mathbb{R}^2$ *als Linearkombination der beiden Vektoren* (w_1, w_2) *und* $(1, \lambda_0)$ *dargestellt werden kann, d.h. dass gilt*

$$\mathrm{Lin}(\{(1, \lambda_0), (w_1, w_2)\}) = \mathbb{R}^2.$$

Voraussetzung war, dass (w_1, w_2) *nicht auf der Geraden* $\{(x, \lambda_0 x) | x \in \mathbb{R}\}$ *liegt* ($w_2 \neq \lambda_0 w_1$), *d.h. dass* $(w_1, w_2) \notin \mathrm{Lin}(\{(1, \lambda_0)\})$.

(iii) Wegen $(x_1, x_2) = x_1(1, 0) + x_2(0, 1)\ \forall\, x_1, x_2 \in \mathbb{R}$ *gilt* $\mathrm{Lin}(\{(1, 0), (0, 1)\}) = \mathbb{R}^2$.

(iv) Im $\mathbb{R}^n$ *gilt*

$$(x_1, \ldots, x_n) = x_1 \underbrace{(1, 0, \ldots, 0)}_{=:e_1} + x_2 \underbrace{(0, 1, 0, \ldots, 0)}_{=:e_2} + \cdots + x_n \underbrace{(0, \ldots, 0, 1)}_{=:e_n}.$$

Hier ist $e_i \in \mathbb{R}^n$ *für* $i \in \{1, \ldots, n\}$ *derjenige Vektor, dessen i-ter Eintrag eine* 1 *ist und der sonst überall den Eintrag Null hat.* $e_1, \ldots, e_n$ *heißen die Einheitsvektoren im* $\mathbb{R}^n$. *Damit ist* $\mathbb{R}^n = \mathrm{Lin}(\{e_1, \ldots, e_n\})$.

Satz 3.16. *Sei K ein Körper, V ein K-VR und $M \subset V$. Dann gilt:*

(i) $\mathrm{Lin}(M)$ *ist ein UVR von V.*

(ii) Ist W ein UVR von V mit $M \subset W$, dann gilt $\mathrm{Lin}(M) \subset W$.

(iii) Es gilt

$$\mathrm{Lin}(M) = \bigcap_{\substack{W \text{ UVR von } V \\ \text{mit } M \subset V}} W,$$

d.h. $\mathrm{Lin}(M)$ *ist der kleinste UVR von V, der alle Vektoren v aus M enthält.*

Beweis. (i) Heuristisch (und auch inhaltlich) ist der Beweis klar: Wenn man zwei Linearkombinationen addiert bzw. mit einem Skalar multipliziert, erhält man wieder eine Linearkombination. Das Problem ist, den Beweis formal korrekt aufzuschreiben:

Wir wollen Lemma 3.6 verwenden, müssen also entsprechend die Voraussetzungen überprüfen. Es gilt

- $\mathrm{Lin}(M) \neq \emptyset$.
- Seien $u_1, u_2 \in \mathrm{Lin}(M)$.

  $\Rightarrow$ Es existieren endliche Mengen $L_1, L_2 \subset M$ mit $u_i \in \mathrm{Lin}(L_i)$, $i = 1, 2$.

  Mit $L^* = L_1 \cup L_2$ gilt $u_1.u_2 \in \mathrm{Lin}(L^*)$. Sei nun $L^* = \{v_1, \ldots, v_r\}$ für ein $r \in \mathbb{N}$.

  $\Rightarrow$ $u_1 = \alpha_1 v_1 + \cdots + \alpha_r v_r$ mit $\alpha_i \in K$
  $u_2 = \beta_1 v_1 + \cdots + \beta_r v_r$ mit $\beta_i \in K$

  $\Rightarrow$ $u_1 + u_2 = (\alpha_1 + \beta_1)v_1 + \cdots + (\alpha_n + \beta_n)v_n \in \mathrm{Lin}(L^*) \subset \mathrm{Lin}(M)$.
- Seien $\lambda \in K$, $u \in \mathrm{Lin}(M)$, d.h. es existiert eine endliche Menge $L = \{v_1, \ldots, v_r\}$, $L \subset M$, mit $u = \alpha_1 v_1 + \cdots + \alpha_r v_r$ für $\alpha_1, \ldots, \alpha_r \in K$.

  $\Rightarrow$ $\lambda u = (\lambda\alpha_1)v_1 + \cdots + (\lambda\alpha_r)v_r \in \mathrm{Lin}(L) \subset \mathrm{Lin}(M)$.

(ii) Sei $W \subset V$ ein UVR mit $M \subset W$. Es gilt

$$\mathrm{Lin}(M) = \bigcup_{\substack{L \subset M: \\ L \text{ endlich}}} \mathrm{Lin}(L),$$

d.h. wir müssen zeigen: $\mathrm{Lin}(L) \subset W$ für alle endlichen Teilmengen L von M. Aber für endliches $L = \{v_1, \ldots, v_r\}$ ist

$$\mathrm{Lin}(L) = \{\alpha_1 v_1 + \cdots + \alpha_r v_r | \alpha_1, \ldots, \alpha_r \in K\} \in W,$$

da W Vektorraum ist und alle $v_i \in L \subset M \subset W$, $i = 1, \ldots, r$.

(iii) Nach (i) ist $\mathrm{Lin}(M)$ ein UVR von V und damit einer der UVRs, über die der Durchschnitt gebildet wird, also

$$\bigcap_{\substack{W \text{ UVR von } V \\ \text{mit } M \subset V}} W \subset \mathrm{Lin}(M).$$

Andererseits folgt für alle $M \subset W$ nach (ii) auch $\mathrm{Lin}(M) \subset W$, womit

$$\mathrm{Lin}(M) \subset \bigcap_{\substack{W \text{ UVR von } V \\ \text{mit } M \subset V}} W.$$

□

Wir wollen abschließend noch einige Eigenschaften der linearen Hülle festhalten.

Lemma 3.17. *Seien K ein Körper, V ein K-Vektorraum, $M \subset V$. Dann gelten folgende Aussagen:*

(i) $M \subset \mathrm{Lin}(M)$.

(ii) $M \subset M' \subset V \Rightarrow Lin(M) \subset \mathrm{Lin}(M')$.

(iii) $M = \mathrm{Lin}(M) \Leftrightarrow M$ *ist UVR von* V.

(iv) $\mathrm{Lin}(\mathrm{Lin}(M)) = \mathrm{Lin}(M)$.

Beweis. (i) folgt unmittelbar aus der Definition der linearen Hülle.

(ii) $M \subset M' \Rightarrow M \subset \mathrm{Lin}(M')$. $\mathrm{Lin}(M')$ ist damit einer der UVRs W in der Darstellung

$$\mathrm{Lin}(M) = \bigcap_{\substack{W \text{ UVR von } V \\ \text{mit } M \subset V}} W$$

aus Satz 3.16 (iii). $\Rightarrow \mathrm{Lin}(M) \subset \mathrm{Lin}(M')$.

(iii) "$\Rightarrow$": Klar. "$\Leftarrow$": Da M ein UVR ist, ist er einer der Ws im Durchschnitt aus Satz 3.16 (iii). $\Rightarrow M = \mathrm{Lin}(M)$.

(iv) Es gilt $\mathrm{Lin}(M) \subset \mathrm{Lin}(\mathrm{Lin}(M))$. Außerdem ist $\mathrm{Lin}(M)$ einer der Vektorräume W bei der $\cap$-Bildung von $\mathrm{Lin}(\mathrm{Lin}(M))$ aus Satz 3.16 (iii). $\Rightarrow$ Behauptung.
Alternativ: Nach Satz 3.16 (i) ist $\mathrm{Lin}(M)$ UVR und nach Satz 3.16 (iii) ist $\mathrm{Lin}(\mathrm{Lin}(M))$ der kleinste UVR, der $\mathrm{Lin}(M)$ enthält. □

3.2 Lineare Unabhängigkeit, Basis und Dimension

Notation 3.18 (Summenzeichen)**.** *Wir verwenden ab jetzt das Symbol "$\sum$" als Abkürzung für eine Summe von endlich vielen Elementen, z. Bsp.*

$$\sum_{i=1}^{n} x_i = x_1 + \cdots + x_n$$

oder für $I = \{i_1, \ldots, i_r\} \subset \mathbb{N}$ (Indexmenge)

$$\sum_{i \in I} y_i = y_{i_1} + \cdots + y_{i_r}.$$

Nimmt man aus einer endlichen Indexmenge I ein Element i_0 heraus und summiert über $I \setminus \{i_0\}$, kennzeichnet man dies häufig mit $\sum_{i \neq i_0}$ anstelle von $\sum_{i \in I \setminus \{i_0\}}$.

Bemerkung 3.19. *Bei Vektorräumen ist es üblich, von einer "Familie" oder einem "System" $(v_1, \dots, v_r)$ von Vektoren zu sprechen. Für eine beliebige Indexmenge I ist eine Familie $(v_i)_{i\in I}$ formal gegeben durch eine Abbildung $I \to V$, $i \mapsto v_i$. Eine Familie muss nicht endlich sein – grundsätzlich studieren wir auch Familien mit unendlich (abzählbar) vielen Vektoren $(v_1, v_2, \dots)$ oder allgemeiner $(v_i)_{i\in I}$ mit einer beliebigen Indexmenge I. Im Spezialfall $I = \mathbb{N}$ nennt man eine Familie "Folge" – der Begriff ist aus der Analysis I bereits bekannt. Im Gegensatz zur Menge der Mitglieder der Familie $\{v_i | i \in I\}$ ist bei einer Familie die Zuordnung $i \mapsto v_i$ fest, also insbesondere $(v_1, \dots, v_r) \neq (v_{\pi(1)}, \dots, v_{\pi(r)})$ für jede Permutation $\pi \in S_r \setminus \{id\}$ (sofern die v_is alle verschieden sind).*

Definition 3.20. *Sei V ein K-Vektorraum.*

(i) Eine endliche Familie von Vektoren $(v_1, \dots, v_r)$ heißt linear unabhängig, falls aus

$$\sum_{i=1}^{r} \lambda_i v_i = 0 \quad \text{mit } \lambda_1, \dots, \lambda_r \in K$$

folgt $\lambda_1 = \cdots = \lambda_r = 0$.

(ii) Eine unendliche Familie von Vektoren $(v_i)_{i\in I}$ heißt linear unabhängig, wenn für jede endliche Teilmenge $J \subset I$ die Familie $(v_i)_{i\in J}$ linear unabhängig ist.

(iii) Eine Familie von Vektoren heißt linear abhängig, falls sie nicht linear unabhängig ist.

Zum besseren Verständnis halten wir fest:

Lemma 3.21. *Ist $r \geq 2$, so gilt: $(v_1, \dots, v_r)$ ist linear abhängig*

$$\Leftrightarrow$$

$\exists\, i_0 \in \{1, \dots, r\}$, so dass v_{i_0} eine Linearkombination aus $\{v_j | \, j \in \{1, \dots, r\} \setminus \{i_0\}\}$ ist.

Beweis. "$\Rightarrow$": $(v_1, \dots, v_r)$ linear abhängig $\Rightarrow \exists\ \lambda_1, \dots, \lambda_r \in K$ (nicht alle $= 0$) mit

$$\sum_{i=1}^{r} \lambda_i v_i = 0.$$

Ist nun aber i_0 ein Index mit $\lambda_{i_0} \neq 0$, folgt

$$v_{i_0} = -\lambda_0^{-1} \sum_{i\in\{1,\dots,r\}\setminus\{i_0\}} \lambda_i v_i = \sum_{i\in\{1,\dots,r\}\setminus\{i_0\}} (\lambda_{i_0}^{-1}\lambda_i) v_i.$$

"$\Leftarrow$": Gelte

$$v_{i_0} = \sum_{i\in\{1,\dots,r\}\setminus\{i_0\}} \lambda_i v_i.$$

für ein $i_0 \in \{1, \ldots, r\}$. Setze $\lambda_{i_0} = -1$. $\Rightarrow \sum_{i=1}^{r} \lambda_i v_i = 0 \Rightarrow (v_1, \ldots, v_r)$ sind linear abhängig. $\square$

Beispiele 3.22. *(i) Sei V der $\mathbb{R}$-VR $\mathbb{R}^n$. Die Familie der Einheitsvektoren $(e_1, \ldots, e_n)$ ist linear unabhängig, denn sind $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$ mit $\sum_{i=1}^{n} \lambda_i e_i = 0$, d.h.*

$$0 = \lambda_1(1, 0, \ldots, 0) + \cdots + \lambda_n(0, \ldots, 0, 1) = (\lambda_1, \ldots, \lambda_n),$$

so folgt $\lambda_1 = \cdots = \lambda_n = 0$.

(ii) Sei $V = \mathbb{R}^2$. Die Familie $((1,1), (1,0), (0,1))$ ist linear abhängig, denn

$$1 \cdot (1,1) + (-1) \cdot (0,1) + (-1) \cdot (1,0) = 0.$$

(iii) Enthält die Familie $(v_1, \ldots, v_r)$ die 0 (d.h. das neutrale Element $0 = 0_V$ der Addition in V), so ist sie linear abhängig (weil $1 \cdot 0_V = 0_V$ mit $1 \neq 0 = 0_K$ gilt).

(iv) Enthält die Familie $(v_1, \ldots, v_r)$ zweimal denselben Vektor, so ist sie linear abhängig (weil $1 \cdot v + (-1) \cdot v = 0$ ist).

Zur Vereinfachung der Notation setzen wir $\mathrm{Lin}\big((v_i)_{i \in I}\big) := \mathrm{Lin}(\{v_i | i \in I\})$ und für endliche Familien $(v_1, \ldots, v_r)$ auch $\mathrm{Lin}(v_1, \ldots, v_r) := \mathrm{Lin}(\{v_1, \ldots, v_r\})$.

Satz 3.23. *Sei V ein K-VR, $(v_i)_{i \in I}$ eine Familie von Vektoren. Dann sind äquivalent:*

(i) $(v_i)_{i \in I}$ ist linear unabhängig.

(ii) Jeder Vektor $v \in \mathrm{Lin}\big((v_i)_{i \in I}\big)$ lässt sich in eindeutiger Weise als Linearkombination aus Vektoren der Familie $(v_i)_{i \in I}$ linear darstellen.

Beweis. (i) $\Rightarrow$ (ii): Sei $(v_i)_{i \in I}$ linear unabhängig und $v \in \mathrm{Lin}\big((v_i)_{i \in I}\big)$.
$\Rightarrow$ Es existieren $J \subset I$, J endlich, und $\lambda_i \in K$ für $i \in J$ mit

$$v = \sum_{i \in J} \lambda_i v_i \quad \text{(Existenz einer Darstellung)}.$$

Eindeutigkeit: Angenommen, es gibt eine weitere Darstellung, d.h. es existieren $H \subset I$, H endlich, und $\mu_i \in K$ für $i \in H$ mit

$$v = \sum_{i \in H} \mu_i v_i.$$

Bilde $G := H \cup J$ und setze $\lambda_i = 0$ für $i \in G \setminus J$ sowie $\mu_i = 0$ für $i \in G \setminus H$.

$$\Rightarrow \qquad 0 = v - v = \sum_{i \in G} (\lambda_i - \mu_i) v_i.$$

Da $(v_i)_{i\in I}$ linear unbahängige Familie ist, folgt $\lambda_i = \mu_i \ \forall\, i \in G$ und die Darstellung ist damit eindeutig.

(ii) $\Rightarrow$ (i): Gelte (ii). Zu zeigen: $(v_i)_{i\in I}$ ist linear unabhängig. (Beweisidee: Man nutzt die Eindeutigkeit der Darstellung für $v \in \mathrm{Lin}\big((v_i)_{i\in I}\big)$ für $v = 0$.)

Angenommen, $(v_i)_{i\in I}$ ist linear abhängig.
$\Rightarrow \exists\ J \subset I$, J endlich mit $(v_i)_{i\in J}$ ist linear abhängig
$\Rightarrow \forall\, i \in J\ \exists\, \lambda_i \in K$ (nicht alle $= 0$) mit

$$\sum_{i\in J} \lambda_i v_i = 0.$$

$\Rightarrow$ Die Darstellung der 0 als Element von $\mathrm{Lin}\big((v_i)_{i\in I}\big)$ ist nicht eindeutig (die andere Darstellung ist $0 = \sum_{i\in J} 0 \cdot v_i$). $\lightning$

Damit ist $(v_i)_{i\in I}$ linear unabhängig. □

Definition 3.24. *Sei V ein K-VR und $(v_i)_{i\in I}$ eine Familie von Vektoren.*

(i) $(v_i)_{i\in I}$ *heißt* Erzeugendensystem *(kurz: ES) von V, wenn $V = \mathrm{Lin}\big((v_i)_{i\in I}\big)$.*

(ii) V *heißt endlich erzeugt, wenn V ein endliches Erzeugendensystem besitzt.*

(iii) $(v_i)_{i\in I}$ *heißt Basis von V, wenn $(v_i)_{i\in I}$ ein linear unabhängiges Erzeugendensystem von V ist.*

(iv) Ist $B = (v_1, \ldots, v_r)$ eine endliche Basis von V, dann heißt r die Länge von B.

Bemerkung. *Jeder Vektorraum besitzt ein Erzeugendensystem, da $V = \mathrm{Lin}(V)$.*

Frage: Besitzt auch jeder Vektorraum eine Basis?
Wir wollen das zunächst für Vektorräume mit endlichem ES untersuchen.

Satz 3.25. *Sei $V \neq \{0\}$, $M = (v_1, \ldots, v_n)$ sei eine endliche Familie von Vektoren aus V. Dann sind äquivalent:*

(i) M ist eine Basis von V.

(ii) M ist ein unverkürzbares ES von V, d.h. M ist ein ES und für jedes $i \in \{1, \ldots, n\}$ ist $(v_j)_{j\in\{1,\ldots,n\}\setminus i}$ kein ES von V.

(iii) Zu jedem $v \in V$ gibt es eindeutig bestimmte $\lambda_1, \ldots, \lambda_n \in K$ mit

$$v = \sum_{i=1}^{n} \lambda_i v_i.$$

(iv) *M ist unverlängerbar linear unabhängig, d.h. M ist linear unabhängig und für jedes $v \in V$ ist die Familie $(v_1, \ldots, v_n, v)$ linear abhängig.*

Beweis. (i) $\Rightarrow$ (ii): Sei M Basis von V. Angenommen, M ist verkürzbar.
$\Rightarrow \exists\, v_i \in M$ mit $v_i = \sum_{j \neq i} \lambda_j v_j$
$\Rightarrow (v_1, \ldots, v_n)$ ist linear abhängig. $\lightning$

(ii) $\Rightarrow$ (iii): Sei $v \in V$. M Erzeugendensystem $\Rightarrow \exists\, \lambda_1, \ldots, \lambda_n :\ v = \sum_{i=1}^n \lambda_i v_i$.
Angenommen, die λ_i sind nicht eindeutig.
$\Rightarrow \exists\, \mu_1, \ldots, \mu_n :\ v = \sum_{i=1}^n \mu_i v_i$ und für mindestens ein $i_0 \in \{1, \ldots, n\}$ ist $\mu_{i_0} \neq \lambda_{i_0}$.
$\Rightarrow 0 = \sum_{i=1}^n (\mu_i - \lambda_i) v_i = \sum_{i \neq i_0} (\mu_i - \lambda_i) v_i + (\mu_{i_0} - \lambda_{i_0}) v_{i_0}$.
$\Rightarrow v_{i_0} = -(\mu_{i_0} - \lambda_{i_0})^{-1} \sum_{i \neq i_0} (\mu_i - \lambda_i) v_i$.
$\Rightarrow v_{i_0}$ kann weggelassen werden, d.h. M ist verkürzbar. $\lightning$

(iii) $\Rightarrow$ (iv): Nach Satz 3.23 ist die Familie $(v_1, \ldots, v_n)$ linear unabhängig. Sei $v \in V$.
$\Rightarrow \exists$ (eindeutige) $\lambda_1, \ldots, \lambda_n :\ v = \sum_{i=1}^n \lambda_i v_i$.
$\Rightarrow (v_1, \ldots, v_n, v)$ ist linear abhängig.
$\Rightarrow M$ ist unverlängerbar linear unabhängig.

(iv) $\Rightarrow$ (i): Sei M unverlängerbar linear unabhängig und sei $v \in V$.
$\Rightarrow (v_1, \ldots, v_n, v)$ ist linear abhängig.
$\Rightarrow$ Es existieren $\lambda_1, \ldots, \lambda_n, \lambda \in K$, nicht alle gleich 0, mit

$$\lambda v + \sum_{i=1}^n \lambda_i v_i = 0.$$

Es folgt $\lambda \neq 0$, andernfalls wäre $\sum_{i=1}^n \lambda_i v_i = 0$ und damit auch $\lambda_1 = \cdots = \lambda_n = 0$, denn M ist linear unabhängig. $\Rightarrow v = -\lambda^{-1} \sum_{i=1}^n \lambda_i v_i$. Aber damit ist M eine Basis. □

Korollar 3.26 (Korollar bedeutet "Folgerung"). *Seien K ein Körper und $V \neq \{0\}$ ein K-VR. Sei $M = (v_1, \ldots, v_n)$ eine endliche, linear unabhängige Familie von Vektoren aus V. Ist M keine Basis, so ist M verlängerbar linear unabhängig, d.h. es gibt ein $v \in V$, so dass $(v_1, \ldots, v_n, v)$ linear unabhängig ist.*

Beweis. Nach Satz 3.25 gilt (iv) $\Rightarrow$ (i). Die Umkehrung ergibt $\neg$(i) $\Rightarrow \neg$(iv). □

Eine weitere Folgerung ist der

Satz 3.27 (Basisauswahlsatz). *Besitzt V ein endliches Erzeugendensystem, dann kann man daraus eine Basis auswählen, d.h. zu einem ES $(v_1, \ldots, v_n)$ gibt es eine Teilmenge $\{i_1, \ldots, i_r\} \subset \{1, \ldots, n\}$, so dass $(v_{i_1}, \ldots, v_{i_r})$ eine Basis ist.*

Beweis. Man entferne von dem ES nacheinander solange Elemente, bis die resultierende Familie ein unverkürzbares ES und somit nach Satz 3.25 auch eine Basis ist. □

Bemerkung. *Beim "Verkürzen" des ES' kann man im Allgemeinen nicht beliebige Elemente entfernen, sondern muss sukzessive überprüfen, ob das ES ohne jeden einzelnen der Vektoren noch ein ES ist. Insofern sagt der Satz nichts über die beste Strategie aus, aus einem gegebenen ES eine Basis zu finden.*

Korollar 3.28. *Jeder endlich erzeugte K-VR besitzt eine Basis von endlicher Länge.*

Fragen: Ist V ein endlich erzeugter K-VR.

- Ist dann jede Basis von endlicher Länge?
- Sind verschiedene Basen von V gleich lang?

Lemma 3.29 (Basisaustauschlemma)**.** *Sei V ein endlich erzeugter K-VR, $B = (v_1, \dots, v_r)$ eine Basis von V, $w = \sum_{i=1}^{r} \lambda_i v_i$. Dann gilt: Ist $\lambda_k \neq 0$ für ein $k \in \{1, \dots, r\}$, so ist*

$$B' = (v_1, \dots, v_{k-1}, w, v_{k+1}, \dots, v_r)$$

ebenfalls eine Basis von V (d.h. man kann v_k gegen w austauschen).

Beweis. Damit die Formulierung des Beweises nicht zu technisch wird, nehmen wir OE ("ohne Einschränkung" – man schreibt manchmal auch OBdA = "ohne Beschränkung der Allgemeinheit") an, dass $k = 1$ ist. Wegen $\lambda_1 \neq 0$ gilt dann

$$v_1 = -\frac{1}{\lambda_1} \sum_{i=2}^{r} \lambda_i v_1 + \frac{1}{\lambda_1} w. \tag{3.1}$$

Wir zeigen jetzt, dass auch $B' = (w, v_2, \dots, v_r)$ eine Basis ist.

- B' ist ein ES von V:

  Sei $v \in V$. Da $(v_1, \dots, v_r)$ Basis von V ist, existieren $\mu_1, \dots, \mu_r \in K$ mit

  $$v = \sum_{i=1}^{r} \mu_i v_i \overset{(3.1)}{=} \frac{\mu_1}{\lambda_1} w + \sum_{i=2}^{r} \Big(\mu_i - \mu_1 \frac{\lambda_i}{\lambda_1}\Big) v_i,$$

  also ist $v \in \mathrm{Lin}(w, v_2, \dots, v_r)$.

- B' ist linear unabhängig:

  Seien μ und $\mu_2, \dots, \mu_r \in K$ mit $\mu w + \sum_{i=2}^{r} \mu_i v_i = 0$. Wegen $w = \sum_{i=1}^{r} \lambda_i v_i$ mit $\lambda_1 \neq 0$ folgt $\mu\lambda_1 v_1 + \sum_{i=2}^{r} (\mu_i + \mu\lambda_i) v_i = 0$.
  $\overset{B \text{ Basis}}{\Rightarrow} \mu\lambda_1 = 0$ und $\mu_i + \mu\lambda_i = 0 \ \forall\, i \in \{2, \dots, r\}$.
  $\overset{\lambda_1 \neq 0}{\Rightarrow} \mu = 0$ und $\mu_i = 0 \ \forall\, i \in \{2, \dots, r\}$.
  $\Rightarrow B'$ ist Basis. □

Satz 3.30 (Basisaustauschsatz)**.** *Seien V ein endlich erzeugter K-VR, $(w_1, \dots, w_m)$ eine linear unabhängige Familie in V. Dann gilt:*

(i) Ist $B = (v_1, \dots, v_r)$ eine Basis, dann ist $r \geq m$.

(ii) Es gibt Indizes $i_{m+1}, \dots, i_r \in \{1, \dots, r\}$, so dass $B^* = (w_1, \dots, w_m, v_{i_{m+1}}, \dots, v_{i_r})$ wieder eine Basis von V ist, d.h. man kann m Elemente der Basis B gegen die $w_1, \dots, w_m$ austauschen.

Beweisidee: Wende das Austauschlemma 3.29 sukzessive auf $w_1, \dots, w_m$ an. Formal machen wir das mit einem Induktionsbeweis nach $n = 1, \dots, m$.

Beweis. Wir zeigen (ii) per Induktion nach n. Aus dem Beweis ergibt sich dann auch (i).

Wir halten zunächst fest, dass aus $(w_1, \dots, w_m)$ linear unabhängig auch $(w_1, \dots, w_n)$ linear unabhängig für alle $n \leq m$ folgt.

Induktionsanfang: Da B Basis ist, gibt es $\lambda_1, \dots, \lambda_r \in K$ mit $w_1 = \sum_{i=1}^{r} \lambda_i v_i$. Da $w_1 \neq 0$ gibt es ein $k \in \{1, \dots, r\}$ mit $\lambda_k \neq 0$. Nach dem Austauschlemma kann man v_k durch w_1 ersetzen und erhält eine neue Basis.

Induktionsschritt $n - 1 \to n$ für $n \leq m$: Sei die Behauptung für $n - 1$ bereits bewiesen, d.h. per Induktionsvoraussetzung gibt es Indizes $i_n, \dots, i_r \in \{1, \dots, r\}$, so dass $B^* = (w_1, \dots, w_{n-1}, v_{i_n}, \dots, v_{i_r})$ eine Basis von V ist. Im Falle $n - 1 = r$ wäre $\tilde{B} = (w_1, \dots, w_{n-1})$ eine Basis von V, d.h. nach Satz 3.25 (iv) unverlängerbar linear unabhängig. $\lightning$ (zu $(w_1, \dots, w_n)$ linear unabhängig), d.h. $n - 1 < r$. Da B^* eine Basis ist, gibt es $\lambda_1, \dots, \lambda_r \in K$ mit

$$w_n = \sum_{k=1}^{n-1} \lambda_k w_k + \sum_{k=n}^{r} \lambda_k v_{i_k}.$$

Falls $\lambda_n = \dots = \lambda_r = 0$, dann wäre $(w_1, \dots, w_n)$ linear abhängige Familie $\lightning$. Also gibt es ein $\lambda_k \neq 0$ mit $k \in \{n, \dots, r\}$. Nach dem Austauschlemma kann man das v_{i_k} gegen das w_n austauschen und erhält, dass $\tilde{B}^* := (w_1, \dots, w_n, v_{j_{n+1}}, \dots, v_{j_r})$ mit $j_{n+1}, \dots, j_r \in \{i_n, \dots, i_r\} \backslash \{i_k\} \subset \{1, \dots, r\}$ eine Basis von V ist. Aus dem letzten Schritt der Induktion für $n = m$ folgt auch $r \geq m$, d.h. (i). □

Satz 3.31. *Seien K ein Körper und V ein K-VR. Dann gilt:*

(i) Ist V endlich erzeugt, so ist jede Basis von V von endlicher Länge, und alle Basen von V haben dieselbe Länge.

(ii) Ist V nicht endlich erzeugt, dann existert von V keine Basis endlicher Länge.

Beweis. (i) Sei V endlich erzeugt. $\overset{\text{Korollar 3.28}}{\Rightarrow}$ $\exists$ endliche Basis $(v_1, \dots, v_r)$ von V.
Sei $(w_i)_{i \in I}$ eine beliebige Basis von V.
Ist I unendlich oder endlich mit Länge $s \geq r+1$, so existieren $i_1, \dots, i_{r+1} \in I$, so dass $(v_{i_1}, \dots, v_{i_{r+1}})$ linear unabhängige Familie ist.
$\overset{\text{Austauschsatz}}{\Rightarrow}$ Länge der Basis $(= r) \geq$ Anzahl der unabhängigen Vektoren $(= r+1)$ $\lightning$
$\Rightarrow I$ endlich mit Länge $s \leq r$.
Vertauscht man die Basen im obigen Argument, erhält man $r \leq s$ und damit $s = r$.

(ii) Angenommen, es existiert eine Basis endlicher Länge. Dann ist diese insbesondere ein endliches Erzeugendensystem. $\lightning$ □

Definition 3.32. *Die Dimension eines K-Vektorraums V ist definiert als*

$$\dim_K V := \begin{cases} \text{Länge einer Basis} & \text{falls } V \text{ endlich erzeugt ist} \\ \infty & \text{falls } V \text{ nicht endlich erzeugt ist.} \end{cases}$$

Wir setzen $\dim_K \{0\} := 0$.

Wegen Satz 3.31 (i) ist $\dim_K V$ wohldefiniert. Falls keine Verwechslungsgefahr besteht, lässt man den Körper K auch weg und schreibt kurz $\dim V$.

Beispiele 3.33. *(i) Die Standardbasis $(e_1, \dots, e_n)$ von K^n hat die Länge n, also ist* $\dim_K K^n = n$.

(ii) Die von einem Vektor $(1, \lambda_0)$ erzeugte Gerade V im $\mathbb{R}^2$ ist ein $\mathbb{R}$-VR mit Dimension $\dim V = 1$.

(iii) Seien v_1 und v_2 zwei linear unabhängige Vektoren in $\mathbb{R}^3$. Dann ist der UVR $U =$ $\mathrm{Lin}(v_1, v_2)$ *eine Ebene durch den Nullpunkt mit* $\dim U = 2$.

Korollar 3.34. *Seien V ein endlichdimensionaler K-VR und $U \subset V$ ein UVR. Dann gilt:*

(i) U ist endlichdimensional.

(ii) $\dim_K U \leq \dim_K V$.

(iii) Es gilt $U = V \Leftrightarrow \dim_K U = \dim_K V$.

Beweis. Sei $\dim V = r \in \mathbb{N}$. Es existiert also eine Basis der Länge r.

(i) Angenommen, U ist nicht endlichdimensional (insbesondere $U \neq \{0\}$). Wir zeigen per Induktion: $\forall\, m \in \mathbb{N}$ gibt es dann linear unabhängige $(u_1, \dots, u_m)$ in U.

Induktionsanfang $m = 1$: Wegen $U \neq \{0\}$ $\exists\, u_1 \in U \setminus \{0\}$ und (u_1) ist linear unabhängige Familie.

Induktionsschritt $m \to m+1$: Seien $(u_1, \ldots, u_m)$ linear unabhängig. $(u_1, \ldots, u_m)$ kann keine Basis sein, andernfalls wäre U endlichdimensional. $\overset{\text{Korollar 3.26}}{\Rightarrow}$ $(u_1, \ldots, u_m)$ ist verlängerbar linear unabhängig, d.h. $\exists\, u_{m+1} \in U$: $(u_1, \ldots, u_{m+1})$ ist linear unabhängig.

$\Rightarrow (u_1, \ldots, u_{r+1})$ linear unabhängig in V. $\lightning$ zum Austauschsatz.

(ii) Seien $s = \dim_K U$ und $(u_1, \ldots, u_s)$ eine Basis von U. $\Rightarrow (u_1, \ldots, u_s)$ linear unabhängig $\overset{\text{Austauschsatz}}{\Rightarrow}$ $s \leq r = \dim_K V$.

(iii) "$\Rightarrow$": klar. "$\Leftarrow$": Angenommen, $U \subset V$, aber $U \neq V$. Sei $(u_1, \ldots, u_r)$ eine Basis von U. Wegen $U \neq V$ ist $(u_1, \ldots, u_r)$ zwar linear unabhängig, aber keine Basis von V. Nach Korollar 3.26 ist $(u_1, \ldots, u_r)$ dann in V verlängerbar linear unabhängig, d.h. $\exists\, v \in V$, so dass $(u_1, \ldots, u_r, v)$ linear unabhängig ist. $\overset{\text{Austauschsatz}}{\Rightarrow}$ $r+1 \leq \dim V = \dim U = r$. $\lightning$ □

Satz 3.35 (Basisergänzungssatz)**.** *Seien K ein Körper, V ein endlichdimensionaler K-VR mit $r = \dim_K V$ und $(u_1, \ldots, u_n)$ eine linear unabhängige Familie in V. Dann existieren $u_{n+1}, \ldots, u_r \in V$, so dass $(u_1, \ldots, u_r)$ eine Basis von V ist, d.h. $(u_1, \ldots, u_n)$ kann zu einer Basis ergänzt werden.*

Beweis. Nach Korollar 3.28 und Satz 3.31 besitzt V eine Basis $(v_1, \ldots, v_r)$. Die Behauptung folgt nun aus dem Basisaustauschsatz (d.h. die $u_{n+1}, \ldots, u_r$ sind $n-r$ Vektoren von $(v_1, \ldots, v_r)$). □

3.3 Auswahlaxiom, Zornsches Lemma und Basisexistenzsatz allgemein

Zu einer Menge M bezeichnen wir mit $\mathcal{P}(M)^\times = \{S \subset M | S \neq 0\}$ die Menge der nicht-leeren Teilmengen von M, d.h. die Potenzmenge von M ohne die leere Menge.

Definition 3.36. *Eine Auswahlfunktion auf einer Menge M ist eine Abbildung $f : \mathcal{P}(M)^\times \to M$ mit der Eigenschaft, dass $f(A) \in A$ für alle $A \in \mathcal{P}(M)^\times$.*

Die Funktion f "wählt" also für jede nicht-leere Teilmenge A von M ein Element aus A "aus".

Auswahlaxiom: Zu jeder Menge gibt es eine Auswahlfunktion.

Wenngleich die Existenz einer Auswahlfunktion plausibel erscheint und in Einzelfällen auch ohne axiomatische Forderung eine Auswahlfunktion schlicht angegeben werden kann, muss ihre Existenz im Allgemeinen tatsächlich axiomatisch gefordert werden.

Es gibt mehrere zum Auswahlaxiom logisch äquivalente Postulierungen – eine ist das Zornsche Lemma. Um dieses formulieren zu können, benötigen wir noch die Klärung einiger Begriffe.

Definition 3.37. *Eine (partielle) Ordnung auf einer Menge M ist eine Relation $\preceq$ auf der Menge M, so dass für alle $x, y, z \in M$ gilt:*

(i) $x \preceq y$ *und* $y \preceq z \Rightarrow x \preceq z$ *(Transitivität)*

(ii) $x \preceq y$ *und* $y \preceq x \Rightarrow x = y$ *(Antisymmetrie)*

(iii) $x \preceq x$ *(Reflexivität).*

Eine totale Ordnung auf einer Menge ist eine partielle Ordnung auf M*, so dass für alle* $x, y \in M$ *zusätzlich*

(iv) $x \preceq y$ *oder* $y \preceq x$ *gilt,*

also zwei Elemente aus M *immer zueinander in Relation stehen.*

Eine Menge mit partieller bzw. totaler Ordnung bezeichnet man als partiell bzw. total geordnete Menge.

Beispiele 3.38. *(i) Die Potenzmenge einer Menge* M *ist durch die Inklusionsrelation* $\subset$ *partiell geordnet.*

(ii) Die ganzen Zahlen $\mathbb{Z}$ *sind mit der* $\leq$*-Relation total geordnet.*

Definition 3.39. *(i) Sei* M *eine bezüglich* $\preceq$ *partiell geordnete Menge. Ein Element* $x \in M$ *heißt obere Schranke für die Teilmenge* $S \subset M$*, wenn* $y \preceq y$ *für alle* $y \in S$ *gilt.*

(ii) Die Menge M *heißt bezüglich der Ordnung* $\preceq$ *induktiv geordnet, wenn jede total geordnete Teilmenge* $S \subset M$ *eine obere Schranke in* M *besitzt.*

(iii) Ein Element $x \in M$ *einer bezüglich* $\preceq$ *partiell geordneten Menge* M *heißt maximales Element, wenn für alle* $y \in M$ *mit* $x \preceq y$ *bereits* $x = y$ *gilt.*

Für eine Menge M ist beispielsweise die Potenzmenge bezüglich der Inklusion induktiv geordnet. Mithilfe eines Fixpunktsatzes von Bourbaki kann man beweisen, dass folgende Aussage aus dem Auswahlaxiom folgt – tatsächlich ist letzteres dazu sogar äquivalent.

Lemma von Zorn: Eine nicht-leere induktiv geordnete Menge besitzt ein maximales Element.

Satz 3.40 (Basisergänzungssatz für unendlichdimensionale VR)**.** *Seien* K *ein Körper,* V *ein* K*-VR und* $(u_j)_{j \in J}$ *eine linear unabhängige Familie in* V*. Dann kann* $(u_j)_{j \in J}$ *zu einer Basis von* V *ergänzt werden, d.h. es existiert* I *mit* $J \subset I$ *und eine Familie* $(v_i)_{i \in I}$ *mit* $v_j = u_j$ *für alle* $j \in J$*, so dass* $(v_i)_{i \in I}$ *eine Basis von* V *ist. Insbesondere besitzt jeder* K*-VR eine Basis.*

Zum Beweis muss man zeigen, dass es eine maximal linear unabhängige Familie gibt, die $(u_j)_{j \in J}$ enthält. Dazu verwenden wir das Zornsche Lemma.

Beweis. Sei $\mathcal{M}$ das System aller Teilmengen $A \subset V$, die $\{u_j | j \in J\}$ enthalten und selbst eine linear unabhängige Familie von Vektoren bilden:

$$\mathcal{M} = \{A \subset V | A \text{ ist linear unabhängig und } \{u_j | j \in J\} \subset A\}.$$

$\mathcal{M}$ ist partiell geordnet durch die Inklusion $\subset$. Diese Ordnung ist aber induktiv, denn bei einer total geordneten Teilmenge $\mathcal{M}' \subset \mathcal{M}$ ist auch $\cup_{A \in \mathcal{M}'} A$ linear unabhängig. Sind nämlich sind $v_1, \ldots, v_r \in \cup_{A \in \mathcal{M}'} A$ paarweise verschieden, so gibt es ein $A \in \mathcal{M}'$ mit $v_1, \ldots, v_r \in A$. Nach dem Lemma von Zorn besitzt $\mathcal{M}$ ein maximales Element. Aber jedes solche ist eine Basis: Wäre ein maximales Element M keine Basis, gäbe es ein $v \in V \setminus \mathrm{Lin}(M)$. Aber dann wäre $M \cup \{v\}$ linear unabhängig, im Widerspruch zur Maximalität von M. □

3.4 Matrizen

Das Arbeiten mit Matrizen spielt eine zentrale Rolle in der linearen Algebra. Nach einer Einführung werden wir als erste Anwendung eine Basis von einem UVR $U = \mathrm{Lin}(v_1, \ldots, v_n)$ bestimmen.

Definition 3.41. *Sei K ein Körper, $m, n \in \mathbb{N}$. Eine $m \times n$-Matrix A (mit Elementen aus K) ist eine Familie*

$$A = (a_{ij})_{\substack{1 \le i \le m \\ 1 \le k \le n}} = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix} \quad \textit{(oder kurz } (a_{ij})\textit{).}$$

Die Menge aller $m \times n$-Matrizen mit Einträgen aus K wird mit $M(m \times n, K)$ bezeichnet.

Bemerkung 3.42. *Wir schreiben ab jetzt die Elemente aus K^n immer als Spaltenvektoren, also*

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in K^n.$$

Definition 3.43 (Verknüpfungen auf $M(m \times n, K)$)**.**

(i) Für $(a_{ij}), (b_{ij}) \in M(m \times n, K)$ definieren wir die Addition durch

$$(a_{ij}) + (b_{ij}) := (a_{ij} + b_{ij}) \tag{3.2}$$

und die skalare Multiplikation durch

$$\lambda \cdot (a_{ij}) := (\lambda \cdot a_{ij}) \quad \textit{für } \lambda \in K.$$

(ii) Wir definieren die Multiplikation von Matrizen durch

$$\begin{aligned} \cdot : M(m \times n, K) \times M(n \times r, K) &\to M(m \times r, K) \\ (a_{ij})_{\substack{1 \le i \le m \\ 1 \le k \le n}} \cdot (b_{jk})_{\substack{1 \le j \le n \\ 1 \le k \le t}} &\mapsto (c_{ik})_{\substack{1 \le i \le m \\ 1 \le k \le r}} \end{aligned} \tag{3.3}$$

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

$$i\text{-te Zeile} \begin{pmatrix} & * & \\ a_{i1} & \dots & a_{in} \\ & * & \end{pmatrix} \cdot \begin{pmatrix} & b_{1k} & \\ * & \vdots & * \\ & b_{nk} & \end{pmatrix} = \begin{pmatrix} & c_{ik} & \end{pmatrix}$$

k-te Spalte

Bemerkung. *Es ist leicht nachzurechnen, dass $M(m \times n, K)$ mit den Verknüpfungen aus (i) ein K-Vektorraum mit Dimension $\dim_K M(m \times n, K) = m \cdot n$ ist. Für den Nachweis der Dimension verwendet man, dass die $m \times n$-Matrizen E_{ij}, $i, = 1, \dots, m$, $j = 1, \dots, n$, mit*

$$(E_{ij})_{i'j'} = \ (i', j')\text{-ter Eintrag von } E_{ij} \ = \begin{cases} 1 & \text{falls } (i', j') = (i, j) \\ 0 & \text{andernfalls} \end{cases}$$

eine Basis bilden.

Lemma 3.44. *Seien K ein Körper, $m, n, r, s \in \mathbb{N}$, $A, A_1, A_2 \in M(m \times n, K)$, $B, B_1, B_2 \in M(n \times r, K)$, $C \in M(r \times s, K)$.*

(i) Es gelten folgende Rechenregeln:

$$\begin{aligned} A \cdot (B_1 + B_2) &= A \cdot B_1 + A \cdot B_2 \\ (A_1 + A_2) \cdot B &= A_1 \cdot B + A_2 \cdot B \\ A \cdot (\lambda \cdot B) &= \lambda \cdot (A \cdot B) = (\lambda \cdot A) \cdot B \\ A \cdot (B \cdot C) &= (A \cdot B) \cdot C \end{aligned}$$

aber in der Regel <u>nicht</u>: $A \cdot B = B \cdot A$.

(ii) Mit der <u>Einheitsmatrix</u>

$$E_n := \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in M(n \times n, K)$$

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

Beweis. Nachrechnen! □

Der Fall $m = n$ von "quadratischen" Matrizen ist besonders wichtig.

Lemma 3.45. *$M(n \times n, K)$ ist mit den inneren Veerknüpfungen $+$ aus (3.2) und $\cdot$ aus (3.3) ein Ring mit Einselement E_n. Für $n > 1$ ist dieser Ring nicht kommutativ, d.h. im Allgemeinen ist $A \cdot B \neq B \cdot A$.*

Beweis. Einfaches Nachrechnen der Eigenschaften (Übungsaufgabe)! Für den Nachweis der fehlenden Kommutativität muss man ein Beispiel angeben:

$$\left(\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 0 & \\ \hline 0 & & 0 \end{array}\right) \cdot \left(\begin{array}{cc|c} 0 & 1 & 0 \\ 0 & 0 & \\ \hline 0 & & 0 \end{array}\right) = \left(\begin{array}{cc|c} 0 & 1 & 0 \\ 0 & 0 & \\ \hline 0 & & 0 \end{array}\right),$$

aber

$$\left(\begin{array}{cc|c} 0 & 1 & 0 \\ 0 & 0 & \\ \hline 0 & & 0 \end{array}\right) \cdot \left(\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 0 & \\ \hline 0 & & 0 \end{array}\right) = \left(\begin{array}{cc|c} 0 & 0 & 0 \\ 0 & 0 & \\ \hline 0 & & 0 \end{array}\right).$$

□

Definition 3.46. *$A \in M(n \times n, K)$ heißt invertierbar, wenn es $B \in M(n \times n, K)$ gibt mit $A \cdot B = B \cdot A = E_n$.*

Lemma 3.47. *Es gilt*

$$GL(n, K) := \left\{ A \in M(n \times n, K) \,\middle|\, A \text{ ist invertierbar} \right\}$$

ist bezüglich der Matrizenmultiplikation eine Gruppe, die allgemeine lineare Gruppe. Das neutrale Element ist E_n. Das zu $A \in GL(n, K)$ inverse Element bezeichnen wir mit A^{-1}. Für $A, B \in GL(n, K)$ gilt $(AB)^{-1} = B^{-1}A^{-1}$.

Beweis. Wir müssen zunächst zeigen, dass für $A_1, A_2 \in GL(n, K)$ das Produkt $A_1 \cdot A_2$ wieder in $GL(n, K)$ liegt, d.h. auch invertierbar ist. Betrachte $A_2^{-1} \cdot A_1^{-1}$. Es gilt nach dem Assoziativgesetz der Matrizenmultiplikation (Lemma 3.44 (i))

$$(A_1 \cdot A_2)(A_2^{-1} \cdot A_1^{-1}) = A_1 \cdot A_1^{-1} = E_n$$

und

$$(A_2^{-1}A_1^{-1}) \cdot (A_1 \cdot A_2) = A_2^{-1} \cdot A_2 = E_n,$$

d.h. $A_1 \cdot A_2$ ist invertierbar mit Inversem $A_2^{-1} \cdot A_1^{-1}$. Damit gilt $A_1 \cdot A_2 \in GL(n, K)$. Das neutrale Element ist E_n. Mit $A \in GL(n, K)$ liegt auch A^{-1} in $GL(n, K)$, da A^{-1} das Inverse A besitzt: $A^{-1} \cdot A = A \cdot A^{-1} = E_n$. □

Definition 3.48. *Sei $A = (a_{ij}) \in M(m \times n, K)$. Dann heißt*

$$A^t := \begin{pmatrix} a_{11} & \dots & a_{m1} \\ \vdots & & \vdots \\ a_{1n} & \dots & a_{mn} \end{pmatrix}$$

die zu A transponierte Matrix (Transponierte von A). Wir schreiben oft A' anstelle von A^t.

Für $n = m$ ensteht A^t aus A durch "Spiegelung" an der Diagonalen $(a_{11}, a_{22}, \dots, a_{nn})$.

Beispiel 3.49.

$$A = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix} \quad \Rightarrow \quad A^t = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}.$$

Lemma 3.50. *Seien $A, A_1, A_2 \in M(m \times n, K)$, $B \in M(n \times r, K)$, $\lambda \in K$. Dann gilt*

(i) $(A_1 + A_2)^t = A_1^t + A_2^t$

(ii) $(\lambda \cdot A)^t = \lambda \cdot A^t$

(iii) $(A^t)^t = A$

(iv) $(A \cdot B)^t = B^t \cdot A^t$.

Beweis. Wir beweisen nur (iv), (i) – (iii) sind klar. Mit $(a_{ij}^t) := A^t$ und $(b_{ij}^t) := B^t$ ist

$$(B^t \cdot A^t)_{ki} = \sum_{j=1}^{n} b_{kj}^t a_{ji}^t = \sum_{j=1}^{n} b_{jk} a_{ij} = \sum_{j=1}^{n} a_{ij} b_{jk} = (A \cdot B)_{ik} = ((A \cdot B)^t)_{ki}.$$

Also ist $(A \cdot B)^t = B^t \cdot A^t$. □

3.4.1 Zeilenstufenform und Gaußalgorithmus

Beispiel 3.51. *Wir wollen folgendes Gleichungssystem lösen:*

$$\begin{array}{rcrcrcl} x & - & y & + & 2z & = & 4 \\ 3x & - & 3y & + & z & = & 2 \\ 2x & + & y & - & z & = & 5. \end{array}$$

Man kann das Gleichungssystem auch in Matrizenform schreiben

$$\begin{pmatrix} 1 & -1 & 2 \\ 3 & -3 & 1 \\ 2 & 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 4 \\ 2 \\ 5 \end{pmatrix}. \tag{3.4}$$

$$
\begin{array}{rcrcrcrl}
x & - & y & + & 2z & = & 4 & \\
3x & - & 3y & + & z & = & 2 & \mid \textit{ Zeile 2 - 3 } \cdot \textit{ Zeile 1} \\
2x & + & y & - & z & = & 5 & \mid \textit{ Zeile 3 - 2 } \cdot \textit{ Zeile 1} \\
\hline
x & - & y & + & 2z & = & 4 & \\
 & & & - & 5z & = & -10 & \mid \textit{ Vertauschen der 2.} \\
 & & 3y & - & 5z & = & -3 & \mid \textit{ und 3. Zeile} \\
\hline
x & - & y & + & 2z & = & 4 & \\
 & & 3y & - & 5z & = & -3 & \mid \cdot 1/3 \\
 & & & - & 5z & = & -10 & \mid \cdot(-1/5) \\
\hline
x & - & y & + & 2z & = & 4 & \\
 & & y & - & \frac{5}{3}z & = & -1 & \\
 & & & & z & = & 2 &
\end{array}
$$

In der Matrizenformschreibweise (3.4) können wir die gleichen Operationen an den Zeilen von

$$
A := \begin{pmatrix} 1 & -1 & 2 \\ 3 & -3 & 1 \\ 2 & 1 & -1 \end{pmatrix}
$$

durchführen. Die Zeilenoperationen wollen wir in diesem Abschnitt untersuchen. Wir halten noch die Matrixschreibweise als vorletzten Schritt fest:

$$
\underbrace{\begin{pmatrix} 1 & -1 & 2 \\ 0 & 3 & -5 \\ 0 & 0 & -5 \end{pmatrix}}_{\textit{Zeilenstufenform von } A} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 4 \\ -3 \\ -10 \end{pmatrix}.
$$

Definition 3.52. *Sei $A \in M(m \times n, K)$ mit Zeilen (!) $a_1, \ldots, a_m \in K^m$. Wir definieren folgende elementaren Zeilenumformungen von A:*

(I) Multiplikation $ZM(i, \lambda)$ der i-ten Zeile mit $\lambda \in K \setminus \{0\}$

$$
\begin{pmatrix} \cdots \\ a_i \\ \cdots \end{pmatrix} \to \begin{pmatrix} \cdots \\ \lambda \cdot a_i \\ \cdots \end{pmatrix}
$$

(II) Addition $ZA(i, j, \lambda)$ des λ-fachen der j-ten Zeile zur i-ten Zeile($i \neq j$)

$$
\begin{pmatrix} \cdots \\ a_i \\ \cdots \\ a_j \\ \cdots \end{pmatrix} \to \begin{pmatrix} \cdots \\ a_i + \lambda \cdot a_j \\ \cdots \\ a_j \\ \cdots \end{pmatrix}
$$

(III) Vertauschen $ZV(i,j)$ der i-ten mit der j-ten Zeile ($i \neq j$)

$$\begin{pmatrix} \dots \\ a_i \\ \dots \\ a_j \\ \dots \end{pmatrix} \to \begin{pmatrix} \dots \\ a_j \\ \dots \\ a_i \\ \dots \end{pmatrix}$$

.

Bemerkung 3.53. *(III) kann man auch durch mehrfache Hintereinanderausführung von (I) und (II) erhalten.*

$$\begin{pmatrix} \dots \\ a_i \\ \dots \\ a_j \\ \dots \end{pmatrix} \xrightarrow{(II)} \begin{pmatrix} \dots \\ a_i + a_j \\ \dots \\ a_j \\ \dots \end{pmatrix} \xrightarrow{(I)} \begin{pmatrix} \dots \\ a_i + a_j \\ \dots \\ -a_j \\ \dots \end{pmatrix} \xrightarrow{(II)} \begin{pmatrix} \dots \\ a_i + a_j \\ \dots \\ a_i \\ \dots \end{pmatrix}$$

$$\downarrow (I)$$

$$\begin{pmatrix} \dots \\ a_j \\ \dots \\ a_i \\ \dots \end{pmatrix} \xleftarrow{(I)} \begin{pmatrix} \dots \\ a_j \\ \dots \\ -a_i \\ \dots \end{pmatrix} \xleftarrow{(II)} \begin{pmatrix} \dots \\ a_i + a_j \\ \dots \\ -a_i \\ \dots \end{pmatrix}$$

Lemma 3.54. *Elementare Zeilenumformungen von $A \in M(m \times n, K)$ erhält man durch Multiplikation von A von links mit den zugehörigen $M(m \times m, K)$-Elementarmatrizen, die wir mit $ZM(i,\lambda)$, $ZA(i,j,\lambda)$ und $ZV(i,j)$ bezeichnen. Es gilt:*

$$ZV(i,j) = \begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array} \begin{array}{c} \downarrow i\text{-te Spalte} \quad \downarrow j\text{-te Spalte} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array} \begin{pmatrix} 1 & & & & & & & & & & \\ & \ddots & & & & & & & 0 & & \\ & & 1 & & & & & & & & \\ & & & 0 & & & 1 & & & & \\ & & & & 1 & & & & & & \\ & & & & & \ddots & & & & & \\ & & & & & & & 1 & & & \\ & & & 1 & & & & 0 & & & \\ & & & & & & & & 1 & & \\ & & & & & & & & & \ddots & \\ & 0 & & & & & & & & & \\ & & & & & & & & & & 1 \end{pmatrix} \begin{array}{l} \\ \\ \\ \leftarrow\ i\text{-te Zeile} \\ \\ \\ \\ \\ \leftarrow\ j\text{-te Zeile} \\ \\ \\ \\ \end{array}$$

$$ZM(i,\lambda) = \begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \end{array} \begin{array}{c} \downarrow i\text{-te Spalte} \\ \left(\begin{array}{ccccccc} 1 & & & & & & \\ & \ddots & & & 0 & & \\ & & 1 & & & & \\ & & & \lambda & & & \\ & & & & 1 & & \\ & 0 & & & & \ddots & \\ & & & & & & 1 \end{array}\right) \end{array} \leftarrow i\text{-te Zeile}$$

$$ZA(i,j,\lambda) = \begin{array}{c} \\ \\ \\ \\ \end{array} \begin{array}{c} \downarrow j\text{-te Spalte} \\ \left(\begin{array}{ccccc} 1 & & & & 0 \\ & \ddots & \lambda & & \\ & 0 & \ddots & & \\ & & & 1 & \end{array}\right) \end{array} \leftarrow i\text{-te Zeile}$$

.

Beweis. Nachrechnen, dass $ZM(i,\lambda)\cdot A$, $ZA(i,j,\lambda)\cdot A$ und $ZV(i,j)\cdot A$ zu der entsprechenden Zeilenumformumg führt. □

Bemerkung 3.55. *In Beispiel 3.51 gilt*

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

.

Definition 3.56. *Sei $A \in M(m\times n, K)$ mit Zeilen $a_1,\dots,a_m$. Man sagt, A sei in Zeilenstufenform (ZSF), falls folgende Bedingungen erfüllt sind:*

(i) Es gibt ein $r\in\mathbb{N}_0$, $r\le m$, so dass für die Zeilen $a_1,\dots,a_m$ gilt:

$$a_i \neq 0 \text{ für } i=1,\dots,r \text{ und } a_{r+1}=\dots=a_m=0.$$

(ii) Setzen wir $j_i := \min\{j \in \{1,\dots,n\} | \, a_{ij} \neq 0\}$ *für* $i = 1,\dots,r$*, so gilt*

$$j_1 < j_2 < \cdots < j_r \quad \textit{(Stufenbedingung).}$$

Die Elemente $a_{1j_1},\dots,a_{rj_r}$ *heißen Pivots.*

Wir wollen jetzt den von den Zahlen $a_1,\dots,a_m$ aufgespannten Vektorraum betrachten und beweisen, dass die r Zeilen der Zeilenstufenform eine Basis bilden. Können wir dann noch ein Konstruktionsverfahren für die Zeilenstufenform angeben, haben wir eine Methode gefunden, um aus einem Erzeugendensystem eine Basis zu konstruieren.

Definition 3.57. *Sei* $A \in M(m \times n, K)$ *mit Zeilen* $a_1,\dots,a_m$*.*

$$ZR(A) := \mathrm{Lin}(a_1,\dots,a_m) \subset K^n$$

heißt der Zeilenraum von A*.* $SR(A) := ZR(A^t) \subset K^m$ *wird als Spaltenraum von* A *bezeichnet.*

Lemma 3.58. *Seien* $A, B \in M(m \times n, K)$*. Dann gilt: Ist* B *aus* A *durch eine endliche Folge von elementaren Zeilenumformungen entstanden, dann ist* $ZR(B) = ZR(A)$*.*

Beweis. Wir müssen die Aussage für die Zeilenumformungen (I) und (II) beweisen. Für (I) ist für $\lambda \neq 0$ und $i \in \{1,\dots,m\}$ zu zeigen:

$$\mathrm{Lin}(a_1,\dots,a_m) = \mathrm{Lin}(a_1,\dots,a_{i-1},\lambda a_i, a_{i+1},\dots,a_m).$$

Wegen der Implikation $M \subset \mathrm{Lin}(M') \Rightarrow \mathrm{Lin}(M) \subset \mathrm{Lin}(M')$ nach Lemma 3.17 muss gezeigt werden, dass alle Vektoren aus dem linken Erzeugendensystem in der linearen Hülle auf der rechten Seite enthalten sind und umgekehrt. Das ist aber unmittelbar klar. Für (II) folgt mit demselben Argument

$$\mathrm{Lin}(a_1,\dots,a_m) = \mathrm{Lin}(a_1,\dots,a_{i-1},a_i + \lambda a_j, a_{i+1},\dots,a_m).$$

D.h. die Aussage $ZR(A) = ZR(B)$ gilt nach jeweils einer Umformung vom Typ (I) oder (II) und damit auch für jede endliche Abfolge von elementaren Zeilenumformungen. □

Wir zeigen nun, dass man wie in Beispiel 3.51 jede $m \times n$-Matrix A durch endlich viele elementare Zeilenumformungen in eine Matrix B von ZSF bringen kann.

Gaußalgorithmus (oder gaußsches Eliminationsverfahren) Sei $A \in M(m \times n, K)$ mit $A \neq 0$. Wir wenden in jedem der r Schritte ($r \in \mathbb{N}$, $r \leq \min(n,m)$) die folgenden drei Teilschritte bestehend aus elementaren Zeilenumformungen an, um eine Matrix B in ZFS zu erhalten.

Start: Setze $A_1 = A$.

1. Teilschritt: Sei j_1 die erste Spalte von A_1, die nicht nur Nullen enthält, d.h.

$$j_1 := \min\big\{j \in \{1,\dots,n\} \,\big|\, \exists\, i \in \{1,\dots,m\} \text{ mit } a_{ij} \neq 0\big\}.$$

Wähle ein i_1 aus mit $a_{i_1 j_1} \neq 0$.

2. Teilschritt: Vertausche die i_1-te Zeile mit der ersten Zeile (Umformung vom Typ (III)). Man erhält das erste Pivot

$$\tilde{a}_{1j_1} = a_{i_1 j_1} \neq 0$$

und die transformierte Matrix

$$\tilde{A}_1 = \begin{pmatrix} 0 & \dots & 0 & \tilde{a}_{1j_1} & * & \dots & * \\ & & & * & & & \\ & 0 & & \vdots & & * & \\ & & & * & & & \end{pmatrix}$$

3. Teilschritt: Durch Umformungen vom Typ II können alle Einträge der j-ten Spalte unterhalb der obersten Zeile zu 0 gemacht werden. Man erhält

$$\bar{A}_1 = \left(\begin{array}{cccc|ccc} 0 & \dots & 0 & \tilde{a}_{1j_1} & * & \dots & * \\ \hline & & & 0 & & & \\ & 0 & & \vdots & & A_2 & \\ & & & 0 & & & \end{array}\right).$$

Man wende dann diese drei Teilschritte auf A_2 an. Dabei kann man die Zeilenumformungen von A_2 auf die ersten Spalten von $\bar{A}_1$ ausdehnen, da diese nur Nullen enthalten.

Iteriere dieses Verfahren. Das Verfahren bricht ab, weil die Folge $j_1 < j_2 \dots$ streng monoton wachsend ist und entweder nach r Schritten $j_r = n$ oder $A_{r+1} = 0$ gilt.

Wir bezeichnen mit B die resultierende Matrix in ZSF. Wegen des 1. Teilschrittes ("Wähle ein i_1 aus ...") ist die Matrix B nicht eindeutig.

Lemma 3.59. *Die ersten r Zeilen $b_1, \dots, b_r$ von B bilden eine Basis von $ZR(A)$. Es gilt $ZR(A) = ZR(B) = \mathrm{Lin}(b_1, \dots, b_r)$ und $\dim ZR(A) = \dim ZR(B) = r$.*

Beweis. $ZR(A) = ZR(B)$ und $\dim ZR(A) = \dim ZR(B) = r$ sind klar. Wir müssen nur die lineare Unabhängigkeit von $b_1, \dots, b_r$ zeigen. Seien $\lambda_1, \dots, \lambda_r \in K$ mit $\lambda_1 b_1 + \dots \lambda_r b_r = 0$. In der j_1-ten Komponente von $\lambda_1 b_1 + \dots + \lambda_r b_r$ steht $\lambda_1 b_{1j_1} = 0$. Wegen $b_{1j_1} \neq 0$ folgt $\lambda_1 = 0$. In der zweiten Komponente von $\lambda_1 b_1 + \dots \lambda_r b_r = \lambda_2 b_2 + \dots \lambda_r b_r$

steht $\lambda_2 b_{2j_2} = 0$ und wegen $b_{2j_2} \neq 0$ folgt $\lambda_2 = 0$. Man erhält so iterativ $\lambda_1 = \lambda_2 = \cdots = \lambda_r = 0$. □

Fazit: Wir haben damit eine Methode gefunden, um zu einem endlichen Erzeugendensystem eine Basis und die Dimension des erzeugten Vektorraums zu bestimmen.

Beispiel 3.60. *Sei* $W = \operatorname{Lin}\big((0,0,3,-1),(0,1,2,0),(0,3,0,2)\big) \subset \mathbb{R}^4$.

$$\begin{pmatrix} 0 & 0 & 3 & -1 \\ 0 & 1 & 2 & 0 \\ 0 & 3 & 0 & 2 \end{pmatrix} \overset{ZV(1,2)}{\longrightarrow} \begin{pmatrix} 0 & 1 & 2 & 0 \\ 0 & 0 & 3 & -1 \\ 0 & 3 & 0 & 2 \end{pmatrix} \overset{ZA(3,1,-3)}{\longrightarrow} \begin{pmatrix} 0 & 1 & 2 & 0 \\ 0 & 0 & 3 & -1 \\ 0 & 0 & -6 & 2 \end{pmatrix}$$

$$\downarrow ZA(3,2,2)$$

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

$\Longrightarrow \big((0,1,2,0),(0,0,3,-1)\big)$ *ist eine Basis von* W *mit* $\dim W = 2$.

Definition 3.61. *Sei* $A \in M(m \times n, K)$.
Zeilenrang(A)$:= \dim ZR(A)$ *heißt Zeilenrang von* A.
Spaltenrang(A)$:= \dim SR(A)$ *heißt Spaltenrang von* A.

Beispiel 3.62. *Wir setzen Beispiel 3.60 mit*

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

fort. Mithilfe elementarer Zeilenumformungen hatten wir die ZSF

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

erreicht, d.h. Zeilenrang(A)$= 2$. *Analog der Spaltenrang:*

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 3 \\ 3 & 2 & 0 \\ -1 & 0 & 2 \end{pmatrix} \longrightarrow \begin{pmatrix} -1 & 0 & 2 \\ 0 & 1 & 3 \\ 3 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} -1 & 0 & 2 \\ 0 & 1 & 3 \\ 0 & 2 & 6 \\ 0 & 0 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} -1 & 0 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

d.h. Spaltenrang(A)$= 2 =$ *Zeilenrang(A).*

Wir werden später zeigen, dass generell Zeilenrang = Spaltenrang gilt.

3.5 Die Summe von Untervektorräumen

Definition 3.63. *Seien $U, W \subset V$ Untervektorräume (UVRs).*

$$U + W := \{u + w \mid u \in U, w \in W\}$$

heißt die Summe von U und W.

Achtung: $U + W$ ist nicht (!) die Vereinigung von U und W als Mengen!

Lemma 3.64. *Seien $U, W \subset V$ UVRs. Dann gilt*

(i) $U + W = \mathrm{Lin}(U \cup W)$, d.h. $U + W$ ist der kleinste UVR, der U und W enthält.

(ii) Sind U und W endlichdimensional, dann ist auch $U + W$ endlichdimensional mit $\dim(U + W) \leq \dim U + \dim W$.

Beweis. (i) "$\subset$": $U + W \subset \mathrm{Lin}(U \cup W)$ ist klar.
"$\supset$": Sei $v \in \mathrm{Lin}(U \cup W) \Rightarrow \exists\, s \in \mathbb{N}$, $\lambda_1, \ldots, \lambda_s \in K$ und $w_1, \ldots, w_s \in U \cup W$ mit

$$v = \sum_{j=1}^{s} \lambda_j w_j.$$

Seien OE für ein $r \leq s$ die Vektoren $w_1, \ldots, w_r \in U$ und $w_{r+1}, \ldots, w_s \in W$. Dann ist

$$v \;=\; \underbrace{\sum_{j=1}^{s} \lambda_j w_j}_{\in U} \;+\; \underbrace{\sum_{j=r+1}^{s} \lambda_j w_j}_{\in W} \;\in\; U + W.$$

(ii) Sind $(u_1, \ldots, u_r)$ eine Basis von U und $(w_1, \ldots, w_s)$ eine Basis von W, so ist die Familie $(u_1, \ldots, u_r, w_1, \ldots, w_s)$ ein Erzeugendensystem von $U + W$.
$\Rightarrow \dim(U + W) \leq r + s = \dim U + \dim W$. □

Beispiele 3.65. *(i)* $K = \mathbb{R}$, $V = \mathbb{R}^2$, $U = \mathrm{Lin}((-1, 1))$, $W = \mathrm{Lin}((1, 1))$.
$\Rightarrow U + W = \mathrm{Lin}((1, -1)) + \mathrm{Lin}((1, 1)) = \mathrm{Lin}\big((-1, 1), (1, 1)\big) = \mathbb{R}^2$.

(ii) $K = \mathbb{R}$, $U = \mathrm{Lin}(e_1, e_2)$, $V = \mathrm{Lin}(e_2, e_3)$.
$\Rightarrow U + W$ *enthält* e_1, e_2, e_3, *d.h.* $U + W = \mathbb{R}^3$.

Satz 3.66. *Seien $U, W \subset V$ endlichdimensionale UVRs. Dann gilt*

$$\dim(U + W) = \dim(U) + \dim(W) - \dim(U \cap W).$$

Beweis. (i) Sei $(v_1, \dots, v_m)$ eine Basis von $U \cap W$. Nach dem Basisergänzungssatz gibt es $u_1, \dots, u_k \in U$ und $w_1, \dots, w_l \in W$, so dass $B_1 = (v_1, \dots, v_m, u_1, \dots, u_k)$ eine Basis von U ist und $B_2 = (v_1, \dots, v_m, w_1, \dots, w_l)$ eine Basis von W ist.

(ii) Behauptung: $B = (v_1, \dots, v_m, u_1, \dots, u_k, w_1, \dots, w_l)$ ist eine Basis von $U + W$. Klar: B ist eine Erzeugendensystem. Wir zeigen, dass B linear unabhängig ist. Sei

$$\underbrace{\lambda_1 v_1 + \dots + \lambda_m v_m + \mu_1 u_1 + \dots + \mu_k u_k}_{=:u \in U} + \nu_1 w_1 + \dots + \nu_l w_l = 0$$

$\Rightarrow u = -\nu_1 w_1 - \dots - \nu_l w_l \in W$
$\Rightarrow u \in U \cap W$
$\Rightarrow \mu_1 = \dots = \mu_k = 0$ (wegen Eindeutigkeit der Darstellung in B_1)
$\Rightarrow \lambda_1 v_1 + \dots + \lambda_m v_m + \nu_1 w_1 + \dots + \nu_l w_l = 0$
$\Rightarrow \lambda_1 = \dots = \lambda_m = \nu_1 = \dots = \nu_l = 0$ (da B_2 Basis).

(iii) Aus (i) und (ii) folgt

$$\begin{array}{ccccc} \dim(U+W) & = & \dim(U) & + \dim(W) & - \dim(U \cap W). \\ \| & & \| & \| & \| \\ m+k+l & & m+k & m+l & m \end{array}$$

□

Definition 3.67. *Seien $U, W \subset V$ UVRs. V heißt direkte Summe von U und W, wenn gilt: $V = U + W$ und für jedes $v \in V$ gibt es eine eindeutige Darstellung $v = u + w$ mit $u \in U$ und $w \in W$. Man schreibt $V = U \oplus W$.*

Bemerkung 3.68. *(i) In Beispiel 3.65 (i) gilt $V = U \oplus W$ und in Beispiel 3.65 (ii) ist $U + V = \mathbb{R}^3$ keine direkte Summe.*

(ii) Die Definition gilt auch für unendlichdimensionale UVRs.

Lemma 3.69. *Seien $U, W \subset V$ UVRs. Dann sind äquivalent:*

(i) $V = U \oplus W$

(ii) $V = U + W$ *und* $U \cap W = \{0\}$.

Beweis. (i) $\Rightarrow$ (ii): Aus (i) folgt sofort $V = U + W$. Angenommen, $U \cap V \neq \{0\}$. Seien $z \in U \cap W$, $z \neq 0$, und

$$v = u + w = \underbrace{(u - z)}_{\in U} + \underbrace{(w + z)}_{\in W},$$

d.h. die Darstellung ist nicht eindeutig. ↯
$\Rightarrow U \cap W = \{0\}$ und $V = U \oplus W$.

(ii) $\Rightarrow$ (i): Sei $v \in V$. $\Rightarrow \exists\, u \in U$, $w \in W$ mit $v = u + w$. Wir zeigen die Eindeutigkeit der Darstellung. Sei $v = u + w = \tilde{u} + \tilde{w}$ eine weitere Darstelllung mit $\tilde{u} \in U$, $\tilde{w} \in W$.

$$\Rightarrow \quad \underbrace{u - \tilde{u}}_{\in U} = \underbrace{\tilde{w} - w}_{\in W} = 0,$$

da $U \cap W = \{0\}$. Es folgen $u = \tilde{u}$, $w = \tilde{w}$ und die Darstellung ist eindeutig. □

Satz 3.70. *Seien V endlichdimensionaler K-VR, $U, W \subset V$ UVRs. Dann sind äquivalent:*

(i) $V = U \oplus W$

(ii) Für alle Basen $(u_1, \ldots, u_k)$ von U und $(w_1, \ldots, w_l)$ von W ist $(u_1, \ldots, u_k, w_1, \ldots, w_l)$ eine Basis von V.

(iii) Es gibt Basen $(u_1, \ldots, u_k)$ von U und $(w_1, \ldots, w_l)$ von W, so dass die Familie $(u_1, \ldots, u_k, w_1, \ldots, w_l)$ eine Basis von V ist.

(iv) $V = U + W$ *und* $\dim V = \dim U + \dim W$.

Beweis. (i)$\Rightarrow$(ii): Erzeugendensystem ist klar. Die behauptete lineare Unabhängigkeit folgt aus Satz 3.23 oder analog zum zweiten Beweisteil von Satz 3.66.

(ii)$\Rightarrow$(iii) ist klar.

(iii)$\Rightarrow$(iv) ist klar.

(iv)$\Rightarrow$(i) folgt aus Satz 3.66 und Lemma 3.69. □

Satz und Definition 3.71. *Seien V ein VR, $U \subset V$ ein UVR. Dann existiert ein UVR $W \subset V$ mit $V = U \oplus W$. W heißt Komplement zu U in V.*

Man beachte, das V nicht als endlichdimensional vorausgesetzt wurde.

Beweis. Wir wenden den Baisergänzungssatz 3.40 an.; Sei $(u_j)_{j \in J}$ eine Basis von U.
$\Rightarrow \exists\, I$ mit $J \subset I$ und eine Basis $(v_i)_{i \in I}$ von V mit $v_j = u_j \;\forall\, j \in J$. Insbesondere gilt

$$U = \operatorname{Lin}\big((v_i)_{i \in J}\big).$$

Setze $W := \operatorname{Lin}\big((v_i)_{i \in I \setminus J}\big)$. Wir wollen zeigen: $U \cap W = \{0\}$.
Sei $v \in U \cap W$. $\Rightarrow$ Es existieren Darstellungen $v = \lambda_{j_1} v_{j_1} + \cdots + \lambda_{j_k} v_{j_k} = \mu_{i_1} v_{i_1} + \cdots + \mu_{i_l} v_{i_l}$ mit $j_1, \ldots, j_k \in J$ und $i_1, \ldots, i_l \in I \setminus J$.

$$\Rightarrow \quad 0 = \sum_{m=1}^{k} \lambda_{j_m} v_{j_m} - \sum_{m=1}^{l} \mu_{i_m} v_{i_m}.$$

Da $(v_i)_{i\in I}$ Basis von V ist und somit insebseondere der Nullvektor eine eindeutige Darstellung als Linearkombination besitzt, folgt $\lambda_{j_1} = \cdots = \lambda_{j_k} = \mu_{i_1} = \cdots = \mu_{i_l} = 0$.
$\Rightarrow v = 0$. Lemma 3.69 impliziert dann die Behauptung. □

Bemerkung 3.72. *Das Komplement ist nicht eindeutig bestimmt. Beispielsweise gilt für $K = \mathbb{R}$, $V = \mathbb{R}^2$ und $U = \mathrm{Lin}(e_1)$*

$$V = U \oplus \mathrm{Lin}(e_2) = U \oplus \mathrm{Lin}((1,1)).$$

Definition 3.73 (Summe von r Vektorräumen)**.** *Sind $2 \leq r \in \mathbb{N}$ und $U_1, \ldots, U_r \subset V$ UVRs, so definieren wir*

$$U_1 + \ldots U_r := \left\{ u_1 + \cdots + u_r \;\middle|\; u_i \in U_i \text{ für } i = 1, \ldots, r \right\}.$$

Die Summe heißt direkte Summe, falls die Darstellung

$$v = u_1 + \cdots + u_r \quad \text{mit } u_i \in U_i,\ i = 1, \ldots r,$$

für alle $v \in U_1 + \cdots + U_r$ eindeutig ist. Man schreibt dann

$$U_1 \oplus \cdots \oplus U_r = \bigoplus_{i=1}^{r} U_i.$$

Bemerkung 3.74. *(i) Die Definition ist im Falle $r = 2$ identisch mit Definition 3.67.*

(ii) Außerdem ist offensichtlich, dass für $r = 3$ gilt

$$U_1 + U_2 + U_3 = (U_1 + U_2) + U_3$$
$$U_1 \oplus U_2 \oplus U_3 = (U_1 \oplus U_2) \oplus U_3$$

bzw. für allgemeine $r \in \mathbb{N}$, $r \geq 2$, entsprechend

$$U_1 + \cdots + U_r = (\ldots((U_1 + U_2) + U_3) + \ldots) + U_r$$
$$U_1 \oplus \cdots \oplus U_r = (\ldots((U_1 \oplus U_2) \oplus U_3) \oplus \ldots) \oplus U_r.$$

Damit übertragen sich die Ergebnisse des Falls $r = 2$ iterativ auf den allgemeinen Fall, z. Bsp. gilt für einen K-VR V:

Satz 3.75. *Seien $U_1, \ldots, U_r \subset V$ endlich erzeugte UVRs. Dann sind äquivalent:*

(i) $V = U_1 \oplus \cdots \oplus U_r$.

(ii) Für alle Basen $\left(u_1^{(i)}, \ldots, u_{k_i}^{(i)}\right)$ *von* U_i *(*$i = 1, \ldots, r$*) ist*

$$\left(u_1^{(1)}, \ldots, u_{k_1}^{(1)}, u_1^{(2)}, \ldots, u_{k_2}^{(2)}, \ldots, u_1^{(r)}, \ldots, u_{k_r}^{(r)}\right)$$

eine Basis von V*.*

(iii) $v = u_1 + \cdots + u_r$ *mit* $u_i \in U_i$*,* $i = 1, \ldots, r$*, und* $\dim V = \dim U_1 + \cdots + \dim U_r$*.*

Beweis. Der Beweis erfolgt durch iterative Anwendung von Satz 3.70. □

Das nächste Lemma beinhaltet für allgemeines $r \geq 2$ das Analogon der Bedingung (ii) aus Lemma 3.69.

Lemma 3.76. *Seien* $r \geq 2$ *und* $U_1, \ldots, U_r$ *UVRs mit* $V = U_1 + \cdots + U_r$*. Dann gilt* $V = U_1 \oplus \cdots \oplus U_r$ *genau dann, wenn*

$$U_i \cap \sum_{\substack{j=1 \\ j \neq i}}^{r} U_j = \{0\} \quad \forall\, i = 1, \ldots, r.$$

Beweis. "⇒": Angenommen, es existiert $i \in \{1, \ldots, r\}$ mit

$$U_i \cap \sum_{\substack{j=1 \\ j \neq i}}^{r} U_j \neq \{0\}.$$

$\Rightarrow \exists\, u_j \in U_j$, $j = 1, \ldots, r$, $u_i \neq 0$ mit $u_i = u_1 + \cdots + u_{i-1} + u_{i+1} + \cdots + u_r$, womit $0 = u_1 + \cdots + u_{i-1} - u_i + u_{i+1} + \cdots + u_r$. ↯ (zur Eindeutigkeit der Darstellung der 0)

"⇐": Sei $v \in V$, besitzt also eine Darstellung $v = u_1 + \cdots + u_r$ mit $u_i \in U_i$, $i = 1, \ldots, r$. Zu zeigen: Die Darstellung ist eindeutig. Seien $\tilde{u}_j \in U_j$, $j = 1, \ldots, r$, mit $v = u_1 + \cdots + u_r = \tilde{u}_1 + \cdots + \tilde{u}_r$, so dass nicht $u_j = \tilde{u}_j$ für alle j gilt. Es existiert folglich $i_0 \in \{1, \ldots, r\}$ mit $u_{i_0} \neq \tilde{u}_{i_0}$.

$$\Rightarrow \quad 0 \neq u_{i_0} - \tilde{u}_{i_0} = -\sum_{\substack{j=1 \\ j \neq i_0}}^{r} (u_j - \tilde{u}_j) \quad \Rightarrow \quad U_{i_0} \cap \sum_{\substack{j=1 \\ j \neq i_0}}^{r} U_j \neq \{0\}. \text{ ↯}$$

□

Bemerkung 3.77. *(i) Für den Nachweis einer direkten Summe* $U_1 \oplus \cdots \oplus U_r$ $(r \geq 3)$ *reicht es nicht, paarweise* $U_i \cap U_j = \{0\}$ *für alle* $i \neq j$*,* $1 \leq i, j \leq r$ *zu fordern. Ein Gegenbeispiel für* $r = 3$*:* $K = \mathbb{R}$*,* $V = \mathbb{R}^2$*,*

$$U_1 = \mathrm{Lin}(e_1),\ U_2 = \mathrm{Lin}(e_2),\ U_3 = \mathrm{Lin}((1,1)).$$

Dann gilt $V = U_1 + U_2 + U_3 = \mathbb{R}^2$ *mit* $U_1 \cap U_2 = \{0\}$, $U_2 \cap U_3 = \{0\}$ *und* $U_1 \cap U_3 = \{0\}$, *aber*

$$U_1 \cap \underbrace{(U_2 + U_3)}_{=\mathbb{R}^2} = U_1 \neq \{0\},$$

d.h. die Summe ist nicht direkt.

(ii) Zur Warnung vor Rechenfehlern sei bemerkt, dass für die Summe von UVRs kein Distributivgesetz gilt. Mit den Bezeichnungen aus (i) ist bspw.

$$\underbrace{(U_1 \cap U_2)}_{=\{0\}} + \underbrace{(U_1 \cap U_3)}_{=\{0\}} = \{0\} \neq U_1 = U_1 \cap (U_2 + U_3).$$

Der Vollständigkeit halber sei nach angemerkt, dass ja gilt

$$U_1 \oplus \cdots \oplus U_r = (\dots((U_1 \oplus U_2) \oplus U_3) \oplus \dots) \oplus U_r. \tag{3.5}$$

Die Bedingung, dass alle Summen direkt sind, wäre

$$U_i \cap \sum_{j=1}^{i-1} U_j = \{0\} \quad \forall\, i \in \{1, \dots, r\}.$$

Wegen der Gleichheit in (3.5) folgt aus Lemma 3.76, dass dies äquivalent ist zu

$$U_i \cap \sum_{\substack{j=1 \\ j \neq i}}^{r} U_j = \{0\} \quad \forall\, i \in \{1, \dots, r\}.$$

Das ist nicht ganz offensichtlich. Man kann diese Äquivalenz aber trotzdem direkt nachrechnen (Übungsblatt 11, Aufgabe 1).

4 Lineare Abbildungen

In diesem Kapitel sind U, V und W stets K-Vektorräume.

Definition 4.1. *Sei* $f : V \to W$ *eine Abbildung.* f *heißt (*K*-)lineare Abbildung oder (Vektorraum-)Homomorphismus, wenn folgende Bedingungen erfüllt sind:*

(L1) $f(u + v) = f(u) + f(v)$ *für alle* $u, v \in V$

(L2) $f(\lambda v) = \lambda f(v)$ *für alle* $v \in V$ *und für alle* $\lambda \in K$.

Beispiele 4.2. *(i) Sei $A = (a_{ij}) \in M(m \times n, K)$. Wir betrachten die Abbildung*

$$\tilde{A} : K^n \to K^m,\ x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto A \cdot x.$$

Es gelten für $u, v \in K^n$, $\lambda \in K$:

$$\tilde{A}(u+v) = A \cdot (u+v) = A \cdot u + A \cdot v = \tilde{A}(u) + \tilde{A}(v) \text{ sowie}$$
$$\tilde{A}(\lambda v) = A \cdot (\lambda v) = \lambda \cdot (A \cdot v) = \lambda \cdot \tilde{A}(v).$$

Wegen

$$\tilde{A}(e_i) = A \cdot e_i = \begin{pmatrix} a_{i1} \\ \vdots \\ a_{im} \end{pmatrix}$$

stehen in den Spalten von A die Bilder der Basisvektoren $e_1, \ldots, e_n$ von K^n unter $\tilde{A}$. Sind $A \in M(m \times n, K)$ und $B \in M(n \times r, K)$, $x \in K^r$, dann gilt

$$\widetilde{AB}(x) = (AB)x = A(Bx) = A \cdot \tilde{B}(x) = \tilde{A}\big(\tilde{B}(x)\big) = \big(\tilde{A} \circ \tilde{B}\big)(x),$$

d.h. die Verknüpfung $\tilde{A} \circ \tilde{B} = \widetilde{AB}$ entspricht der Matrix-Multiplikation.

(ii) Sei $f : \mathbb{R}^2 \to \mathbb{R}^2$, $\binom{x_1}{x_2} \mapsto \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)\binom{x_1}{x_2} = \binom{x_1}{-x_2}$. Die Abbildung ist linear nach (i) und beschreibt die Spiegelung an der x_1-Achse.

(iii) Sei $V = \{f : (0,1) \to \mathbb{R} |\ f$ ist differenzierbar$\}$. V ist ein $\mathbb{R}$-VR. Dann ist

$$' : V \to \{g : (0,1) \to \mathbb{R}\},$$
$$f \mapsto f'$$

lineare Abbildung, denn für $f, g \in V$ gilt $(f+g)' = f' + g'$ und $(\lambda \cdot f)' = \lambda \cdot f'$ $(\lambda \in \mathbb{R})$.

Lemma 4.3. *Sei $f : V \to W$ eine lineare Abbildung. Dann gilt:*

(i) $f(0) = 0$

(ii) $f\big(\sum_{i=1}^n \lambda_i v_i\big) = \sum_{i=1}^n \lambda_i f(v_i)$ *für alle* $v_i \in V$, $\lambda_i \in K$ $(i = 1, \ldots, n)$

(iii) $V' \subset V$ *UVR* $\Rightarrow f(V')$ *ist UVR*

(iv) $W' \subset W$ *UVR* $\Rightarrow f^{-1}(W) \subset V$ *ist UVR* (f^{-1} *Urbild)*

(v) $(v_i)_{i \in I}$ *linear abhängige Familie in* $V \Rightarrow (f(v_i))_{i \in I}$ *linear abhängige Famile in* W

(vi) $V' = \mathrm{Lin}\left((v_i)_{i\in I}\right) \Rightarrow f(V') = \mathrm{Lin}\left((f(v_i))_{i\in I}\right)$

(vii) *W endlichdim. $\Rightarrow$ $f(V)$ endlichdim. UVR von W mit* $\dim f(V) \leq \dim W$.

Beweis. (i) Es gilt $f(0) = f(0+0) \overset{(L1)}{=} f(0) + f(0) \overset{\text{Kürzungsregel}}{\Rightarrow} f(0) = 0$.

(ii) folgt aus iterativer Anwendung von (L1) und (L2).

(iii) Sei $V' \subset V$ UVR. Zu zeigen: $f(V')$ it UVR von W. Dazu weisen wir die Bedingungen aus Lemma 3.6 nach.

- Wegen $0 \in V'$ ist $f(0) \overset{(i)}{=} 0 \in f(V')$. Insbesondere ist $f(V') \neq \emptyset$.
- Seien $w_1, w_2 \in f(V')$, d.g. es existieren $v_1, v_2 \in V'$ mit $w_1 = f(v_1)$, $w_2 = F(v_2)$.
  $\Rightarrow w_1 + w_2 = f(v_1) + f(v_2) \overset{(L1)}{=} f(\underbrace{v_1 + v_2}_{\in V'}) \in f(V')$.
- Sei $\lambda \in K$, $w \in f(V')$, d.h. $w = f(v)$ für ein $v \in V'$.
  $\Rightarrow \lambda w = \lambda f(v) \overset{(L2)}{=} f(\underbrace{\lambda v}_{\in V'}) \in f(V')$.

(iv) Sei $W' \subset W$ UVR. Zu zeigen: $f^{-1}(W') \subset V$ ist UVR. Wieder weisen wir dazu die Bedingungen aus Lemma 3.6 nach.

- Wegen $f(0) \overset{(i)}{=} 0 \in W'$ ist $0 \in f^{-1}(\{0\})$, womit $f^{-1}(W') \neq \emptyset$.
- Seien $v_1, v_2 \in f^{-1}(W') \Rightarrow f(v_1), f(v_2) \in W'$
  $\Rightarrow f(v_1 + v_2) \overset{(L1)}{=} f(v_1) + f(v_2) \in W' \Rightarrow v_1 + v_2 \in f^{-1}(W')$.
- Seien $\lambda \in K$, $v \in f^{-1}(W')$. $\Rightarrow f(v) \in W'$
  $\Rightarrow f(\lambda v) \overset{(L2)}{=} \lambda \cdot f(v) \in W' \Rightarrow \lambda v \in f^{-1}(W')$.

(v) Sei $(v_i)_{i\in I}$ linear abhängige Familie. $\Rightarrow \exists\, J \subset I$, J endlich und $\lambda_i \in K$ für $i \in J$ nicht alle gleich Null mit $\sum_{i\in J} \lambda_i v_i = 0$.

$$\Rightarrow \quad 0 \overset{(i)}{=} f(0) = f\left(\sum_{i\in J} \lambda_i v_i\right) \overset{(ii)}{=} \sum_{i\in J} \lambda_i f(v_i).$$

$\Rightarrow \left((f(v_i))_{i\in I}\right)$ ist linear abhängig.

(vi) ‘

“$\subset$”: Sei $w \in f(V')$, d.h. $w = f(v)$ für ein $v \in V'$.
$\Rightarrow \exists\, J \subset I$ endlich und $\lambda_i \in K$ für $i \in J$ mit $v = \sum_{i\in J} \lambda_i v_i$.
$\Rightarrow w = f(v) \overset{(ii)}{=} \sum_{i\in J} \lambda_i f(v_i)$, also $w \in \mathrm{Lin}\left((f(v_i))_{i\in I}\right)$.

"$\supset$" Sei $w \in \mathrm{Lin}\big((f(v_i))_{i\in I}\big)$.
$\Rightarrow \exists\, J \subset I$ endlich und $\lambda_i \in K$ für $i \in J$ mit

$$w = \sum_{i\in J} \lambda_i f(v_i) \overset{(ii)}{=} f\Big(\sum_{i\in J} \lambda_i v_i\Big) \in f(V').$$

(vii) Nach (iii) ist $f(V)$ UVR von W. Die Behauptung ist dann gerade Aussage (ii) aus Korollar 3.34. □

Lemma 4.4. *Seien $f : V \to W$, $g : U \to V$ lineare Abbildungen. Dann ist auch $f \circ g : U \to W$ eine lineare Abbildung.*

Beweis. Es sind (L1) und (L2) zu verifizieren. Seien $u_1, u_2 \in U$. Dann folgt

$$(f \circ g)(u_1 + u_2) = f\big(g(u_1 + u_2)\big) = f\big(g(u_1) + g(u_2)\big) = (f \circ g)(u_1) + (f \circ g)(u_2),$$

also (L1). Analog zeigt man (L2), d.h. $(f \circ g)(\lambda u) = \lambda(f \circ g)(u)$ für $\lambda \in K$. □

Definition 4.5. *Man bezeichnet*

- *eine lineare Abbildung $f : V \to W$ als <u>Homomorphismus</u> und setzt*

$$\mathrm{Hom}_K(V, W) := \big\{f : V \to W \,\big|\, f \text{ ist } K\text{-linear}\big\},$$

- *eine lineare Abbildung $f : V \to V$ als <u>Endomorphismus</u> und setzt*

$$\mathrm{End}_K(V) := \big\{f : V \to V \,\big|\, f \text{ ist } K\text{-linear}\big\}.$$

Lemma 4.6. *(i) $\mathrm{Hom}_k(V, W)$ ist bzgl.*
der Addition $(f, g) \mapsto f + g$ mit $(f + g)(v) = f(v) + g(v)\ \forall\, v \in V$ und
der skalaren Multiplikation $(\lambda, f) \mapsto \lambda \cdot f$ mit $(\lambda \cdot f)(v) = \lambda\big(f(v)\big)\ \forall\, v \in V$
ein Vektorraum.

(i) $\mathrm{End}_K(V)$ ist bzgl. $+ : (f, g) \mapsto f+g$ und $\circ : (f, g) \mapsto f\circ g$ ein Ring mit Einselement id_V.

Beweis. Nachrechnen! □

Definition 4.7. *Man bezeichnet*

- *eine bijektive lineare Abbildung $f : V \to W$ als <u>Isomorphismus</u> und setzt*

$$\mathrm{Iso}_K(V, W) := \big\{f : V \to W \,\big|\, f \text{ ist Isomorphismus}\big\},$$

- *eine bijektive lineare Abbildung $f : V \to V$ als Automorphismus und setzt*

$$\mathrm{End}_K(V) := \{f : V \to V \mid f \text{ ist Automorphismus}\}.$$

Existiert zwischen Vektorräumen V und W ein Isomorphismus, so heißen V und W isomorph (Notation $V \cong W$).

Lemma 4.8. *Sei $f : V \to W$ eine lineare Abbildung. Dann gilt*

$$f \text{ Isomorphismus} \quad \Rightarrow \quad f^{-1} \text{ Isomorphismus.}$$

Beweis. Analog zum Beweis bei Gruppen (Lemma 2.16 (iii)). □

4.1 Bild, Kern und Dimensionsformel

Definition 4.9. *Sei $f : V \to W$ lineare Abbildung. Dann heißen*

- $\mathrm{Bild}\, f := f(V) = \{w \in W \mid \exists\, v \in V \text{ mit } f(v) = w\}$ *das Bild von f,*
- $\mathrm{Kern}\, f := f^{-1}(\{0\}) = \{v \in V \mid f(v) = 0\}$ *der Kern von f.*

Satz 4.10. *Seien $f : V \to W$ lineare Abbildungen. Dann gelten folgende Aussagen.*

(i) $\mathrm{Bild}\, f \subset W$ *und* $\mathrm{Kern}\, f \subset V$ *sind UVRs.*

(ii) f *surjektiv* $\Leftrightarrow \mathrm{Bild}\, f = W$.

(iii) f *injektiv* $\Leftrightarrow \mathrm{Kern}\, f = \{0\}$.

(iv) f *injektiv und* $(v_i)_{i\in I}$ *linear unabhängige Familie in* $V \Rightarrow \big(f(v_i)\big)_{i\in I}$ *ist linear unabhängig.*

Beweis. (i) folgt aus Lemma 4.3 (iii) und (iv).

(ii) ist gerade die Definition von Surjektivität.

(iii)

"$\Rightarrow$": Sei f injektiv. Zu zeigen: $\mathrm{Kern}\, f = \{0\}$.

"$\supset$": $f(0) = 0 \Rightarrow 0 \in \mathrm{Kern}\, f$.

"$\subset$": Sei $u \in \mathrm{Kern}\, f \Rightarrow f(u) = 0 = f(0) \overset{f \text{ injektiv}}{\Rightarrow} u = 0$.

"$\Leftarrow$": Gelte nun $\mathrm{Kern}\, f = 0$. Seien $u, v \in V$ mit $f(u) = f(v)$. $\overset{f \text{ linear}}{\Rightarrow} f(u - v) = 0 \overset{\mathrm{Kern}\, f = \{0\}}{\Rightarrow} u - v = 0$, d.h. f ist injektiv.

(iv) Seien $J \subset I$, J endlich und $\lambda_j \in K$ $(j \in J)$ mit

$$\sum_{j \in J} \lambda_j f(v_j) = 0. \tag{4.1}$$

Zu zeigen: $\lambda_j = 0 \; \forall \, j \in J$. Wegen

$$0 = \sum_{j \in J} \lambda_j f(v_j) \overset{\text{Lemma 4.3}(ii)}{=} f\Big(\sum_{j \in J} \lambda_j v_j \Big)$$

folgt aus (iii) aber $\sum_{j \in J} \lambda_j v_j = 0 \overset{(v_i)_{i \in I} \text{ lin. unabh}}{\Rightarrow} \lambda_j = 0 \; \forall \, j \in J.$ □

Definition 4.11. *Sei $f : V \to W$ eine lineare Abbildung. Dann heißt*

$$\operatorname{Rang} f := \dim \big(\operatorname{Bild}(f) \big)$$

der Rang von f.

Beispiel und Definition 4.12 (Matrizen)**.** *Wir betrachten wie in Beispiel 4.2 (i) die zu $A \in M(m \times n, K)$ gehörende Abbildung $\tilde{A} : K^n \to K^m$, $x \mapsto Ax$. Wegen $K^n = \operatorname{Lin}(e_1, \ldots, e_n)$ folgt aus Lemma 4.3 (vi)*

$$\begin{array}{ccccc} \operatorname{Bild} \tilde{A} & = & \operatorname{Lin} \big(\tilde{A}(e_1), \ldots, \tilde{A}(e_n) \big). \\ & & \| & & \| \\ & & Ae_1 & & Ae_n \end{array}$$

$Ae_1, \ldots, Ae_n$ sind aber genau die Spalten von A, d.h.

$$\operatorname{Rang} \tilde{A} = \dim \big(\operatorname{Bild} \tilde{A} \big) = \dim \big(SR(A) \big) = \; \textit{Spaltenrang}\,(A).$$

Wir definieren den Rang der Matrix A durch

$$\operatorname{Rang}(A) := \operatorname{Rang} \tilde{A} = \; \textit{Spaltenrang}\,(A).$$

Satz 4.13 (Dimensionsformel für lineare Abbildungen)**.** *Seien V endlichdimensionaler K-VR und $f : V \to W$ eine lineare Abbildung. Sei ferner $(v_1, \ldots, v_k)$ eine Basis von* Kern f*, $(w_1, \ldots, w_l)$ eine Basis von* Bild f*. Für $i = 1, \ldots, l$ seien $u_i \in V$ mit $f(u_i) = w_i$. Dann gilt: $B = (v_1, \ldots, v_k, u_1, \ldots, u_l)$ ist eine Basis von V und*

$$\dim V = \dim \big(\operatorname{Kern} f \big) + \dim \big(\operatorname{Bild} f \big).$$

Beweis. Wir zeigen (i) B ist Erzeugendensystem von V und (ii) B ist linear unabhängig.

(i) Sei $v \in V$. $\Rightarrow f(v) \in \operatorname{Bild} f$. $\Rightarrow \exists\, \mu_1, \ldots, \mu_l \in K$ mit

$$f(v) = \sum_{j=1}^{l} \mu_j w_j.$$

Sei nun $u = \sum_{j=1}^{l} \mu_j u_j$.

$$\Rightarrow \quad f(u) = \sum_{j=1}^{l} \mu_j f(u_j) = \sum_{j=1}^{l} \mu_j w_j = f(v).$$

$\Rightarrow f(u - v) = 0 \Rightarrow v - u \in \operatorname{Kern} f$.
$\Rightarrow \exists\, \lambda_1, \ldots, \lambda_k \in K$ mit $v - u = \sum_{j=1}^{k} \lambda_j v_j$.

$$\Rightarrow \quad v = \sum_{j=1}^{k} \lambda_j v_j + \sum_{j=1}^{l} \mu_j u_j.$$

(ii) Seien $\mu_1, \ldots, \mu_l, \lambda_1, \ldots, \lambda_k \in K$ mit

$$\sum_{j=1}^{k} \lambda_j v_j + \sum_{j=1}^{l} \mu_j u_j = 0.$$

Anwendung von f auf beiden Seiten der Identität ergibt nach Lemma 4.3 (i) – (ii)

$$\sum_{j=1}^{k} \lambda_j \underbrace{f(v_j)}_{=0} + \sum_{j=1}^{l} \mu_j \underbrace{f(u_j)}_{=w_j} = 0.$$

$\overset{(w_1,\ldots,w_l) \text{ Basis}}{\Rightarrow} \mu_1 = \cdots = \mu_l = 0.$
$\Rightarrow \sum_{j=1}^{k} \lambda_j v_j = 0.$
$\overset{(v_1,\ldots,v_k) \text{ Basis}}{\Rightarrow} \lambda_1 = \cdots = \lambda_k = 0.$

Damit ist B Basis von $V \Rightarrow \dim V = k + l = \dim(\operatorname{Kern} f) + \dim(\operatorname{Bild} f)$. □

Korollar 4.14. *Seien V und W endlichdimensionale K-Vektorräume. Dann sind äquivalent:*

(i) $V \cong W$

(ii) $\dim V = \dim W$.

Beweis. (i) ⇒ (ii): Sei $V \cong W$, d.h. es existiert ein Isomorphismus $f : V \to W$. Sei $(v_1, \ldots, v_r)$ eine Basis von V. Da f injektiv ist, folgt aus Satz 4.10 (iv), dass $\big(f(v_1), \ldots, f(v_r)\big)$

linear unabhängig ist. Die Surjektivität von f ergibt damit

$$W = \operatorname{Bild} f = \operatorname{Lin}\big(f(v_1), \ldots, f(v_r)\big),$$

d.h. $\big(f(v_1), \ldots, f(v_r)\big)$ ist ein Erzeugendensystem und damit insgesamt eine Basis.
$\Rightarrow \dim W = r = \dim V$.

(ii) $\Rightarrow$ (i): Sei $\dim V = \dim W = r \in \mathbb{N}$. Seien $(v_1, \ldots, v_r)$ Basis von V und $(w_1, \ldots, w_r)$ Basis von W. Wir definieren

$$\begin{aligned} f : V &\to W \\ v = \sum_{j=1}^{r} \lambda_j v_j &\mapsto \sum_{j=1}^{r} \lambda_j w_j. \end{aligned}$$

- f ist wohldefiniert, da $(v_1, \ldots, v_r)$ eine Basis von V ist und damit jedes $v \in V$ eine eindeutige Darstellung als Linearkombination aus $v_1, \ldots, v_r$ besitzt.
- f ist linear (Nachrechnen!).
- Es gilt: $\operatorname{Bild} f = \operatorname{Lin}(w_1, \ldots, w_r) = W$, d.h. f ist surjektiv.
- f ist injektiv, denn aus

$$\underbrace{\dim V}_{=r} = \dim\big(\operatorname{Kern} f\big) + \underbrace{\dim\big(\underbrace{\operatorname{Bild} f}_{W}\big)}_{=r}$$

folgt $\dim\big(\operatorname{Kern} f\big) = 0$, d.h. $\operatorname{Kern} f = \{0\}$.

□

Korollar 4.15. *(i) Seien $n, m \in N_0$. Dann gilt: $K^n \cong K^m \Leftrightarrow n = m$.*

(ii) Ist V ein endlichdimensionaler K-Vektorraum, so gilt $V \cong K^n$ mit $n := \dim V$.

Korollar 4.16. *Seien V und W endlichdimensionale K-Vektorräume mit $\dim V = \dim W$ und $f : V \to W$ linear. Dann sind äquivalent:*

(i) f ist injektiv,

(ii) f ist surjektiv.

(iii) f ist bijektiv.

Beweis. (i) $\Rightarrow$ (ii): f injektiv $\Rightarrow \operatorname{Kern} f = \{0\}$, d.h. $\dim\big(\operatorname{Kern} f\big) = 0$.

$$\Rightarrow \dim\big(\operatorname{Bild} f\big) \overset{\text{Satz } 4.13}{=} \dim V = \dim W \Rightarrow \operatorname{Bild} f = W \Rightarrow f \text{ surjektiv.}$$

(ii) $\Rightarrow$ (iii): Sei f surjektiv. $\Rightarrow \dim\big(\operatorname{Kern} f\big) = \dim(V) - \dim\big(\underbrace{\operatorname{Bild} f}_{=W}\big) = 0.$

$$\Rightarrow \operatorname{Kern} f = \{0\} \overset{\text{Satz } 4.10(iii)}{\Rightarrow} f \text{ injektiv.}$$

Insgesamt ist f also bijektiv.

(iii) $\Rightarrow$ (i): Klar. □

4.2 Affine Unterräume

Um die Urbilder $f^{-1}(\{w\})$ genauer untersuchen zu können, brauchen wir den Begriff des affinen Unterraums.

Definition 4.17. *Sei V ein K-VR. $Z \subset V$ heißt affiner Unterraum von V, wenn es ein $z \in V$ und einen UVR $U \subset V$ gibt mit*

$$Z = z + U := \{z + u \,|\, u \in U\},$$

d.h. affine Unterräume entstehen durch "Parallelverschiebung" von UVRs.

Beachte: Ist $z \notin U$, dann ist $0 \notin z + U$, d.h. in diesem Falle ist Z kein UVR von V.

Lemma 4.18. *Seien $z \in V$ und $U \subset V$ UVR, ferner $Z = z + U$. Dann gilt:*

(i) Für jedes $z' \in Z$ ist $Z = z' + U$.

(ii) Sind $\tilde{z} \in V$ und $\tilde{U} \subset V$ UVR mit $\tilde{z} + \tilde{U} = z + U$, dann ist $U = \tilde{U}$ und $z - \tilde{z} \in U$.

Beweis. (i) Sei $z' \in Z$, d.h. $z' = z + u'$ mit $u' \in U$.

$$\Rightarrow \quad z' + U = z + \underbrace{\big(u' + U\big)}_{=U} = z + U = Z.$$

(ii) Es gilt $U = \{y_1 - y_2 \,|\, y_1, y_2 \in z + U\}$, womit

$$U = \big\{y_1 - y_2 \,\big|\, y_1, y_2 \in z + U\big\} = \big\{y_1 - y_2 \,\big|\, y_1, y_2 \in \tilde{z} + \tilde{U}\big\} = \tilde{U}.$$

$\Rightarrow z + U = \tilde{z} + U \Rightarrow z \in z + U = \tilde{z} + U \Rightarrow z - \tilde{z} \in U.$ □

Konsequenz und Definition. Bei einem affinen Unterraum $Z = z + U$ ist der UVR eindeutig bestimmt, der "Verschiebungspunkt" z kann beliebig aus Z gewählt werden. Da U eindeutig ist, können wir die Dimension definieren durch

$$\dim Z := \dim U.$$

Beispiel 4.19. *Wir vergleichen UVRs und affine Unterräume in* $\mathbb{R}^2$.

UVRs:

$\dim U = 0:\ \{0\}$
$\dim U = 1:\ \mathrm{Lin}(v), 0 \neq v \in \mathbb{R}^2$ *(Geraden durch den Ursprung)*
$\dim U = 2:\ \mathbb{R}^2$.

Affine Unterräume:

$\dim Z = 0:\ \{z\}, z \in \mathbb{R}^2$ *(Punkte)*
$\dim Z = 1:\ z + \mathrm{Lin}(v), 0 \neq v \in \mathbb{R}^2$ *(verschobene Geraden)*
$\dim Z = 2:\ \mathbb{R}^2$.

Lemma 4.20. *Sei* $f : V \to W$ *eine lineare Abbildung,* $w \in \mathrm{Bild}\, f$ *und* $v \in f^{-1}(\{w\})$. *Dann gilt:*

$$f^{-1}(\{w\}) = v + \mathrm{Kern}\, f \quad \textit{und} \quad \dim f^{-1}(\{w\}) = \dim V - \dim\big(\mathrm{Bild}\, f\big).$$

Beweis. "$\subset$": Sei $u \in f^{-1}(\{w\})$. $\Rightarrow f(u) = w = f(v) \Rightarrow f(u) - f(v) = f(u - v) = 0$
$\Rightarrow u - v \in \mathrm{Kern}\, f \Rightarrow u \in v + \mathrm{Kern}\, f$.

"$\supset$": Sei $u \in v + \mathrm{Kern}\, f \Rightarrow \exists\, x \in \mathrm{Kern}\, f$: $u = v + x$

$$\Rightarrow \quad f(u) = f(v + x) = f(v) + \underbrace{f(x)}_{=0} = f(v) = w,$$

da $v \in f^{-1}(\{w\})$. Aber damit ist $u \in f^{-1}(\{w\})$.
Schließlich gilt $\dim f^{-1}(\{w\}) = \dim\big(\mathrm{Kern}\, f\big) \overset{\text{Satz } 4.13}{=} \dim V - \dim\big(\mathrm{Bild}\, f\big)$. □

4.3 Lineare Gleichungssysteme

In diesem Abschnitt seien $A = (a_{ij}) \in M(m \times n, K)$,

$$b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in K^m.$$

Wir untersuchen das lineare Gleichungssystem (LGS)

$$\begin{array}{ccccccc} a_{11}x_1 & + & \dots & + & a_{1n}x_n & = & b_1 \\ & & \vdots & & & & \\ a_{m1}x_1 & + & \dots & + & a_{mn}x_n & = & b_m, \end{array}$$

in Matrix-Schreibweise $Ax = b$. Wir gehabt induziert die Matrix die lineare Abbildung

$$\tilde{A} : K^n \to K^m, \quad x \mapsto A \cdot x.$$

Wir betrachten das Problem der Lösung zunächst theoretisch und dann algorithmisch.

Definition 4.21. *Das LGS $Ax = b$ heißt*

homogen, wenn $b = 0$,

inhomogen, wenn $b \neq 0$.

Das LGS $Ax = 0$ heißt das zu $Ax = b$ gehörende homogene LGS. A heißt Koeffizientenmatrix.

$$\text{Lös}(A, b) := \{x \in K^n | \, Ax = b\} = \tilde{A}^{-1}(\{b\})$$

heißt Lösungsraum des LGS $Ax = b$.

Es gilt

$$\text{Lös}(A, 0) = \{x \in K^n | \, Ax = 0\} = \text{Kern}\, \tilde{A}.$$

Satz 4.22. *Es gilt:*

(i) $\text{Lös}(A, 0) \subset K^n$ *ist ein UVR der Dimension* $n - \text{Rang}(A)$.

(ii) $\text{Lös}(A, b) \subset K^n$ *ist ein affiner Unterraum von* K^n. *Ist* $\text{Lös}(A, b) \neq \emptyset$, *dann hat dieser die Dimension* $n - \text{Rang}(A)$.

(iii) Sind $\text{Lös}(A, b) \neq \emptyset$ *und* $v \in \text{Lös}(A, b)$, *dann ist*

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

Bemerkung. *(iii) bedeutet: Falls eine Lösung v von $Ax = b$ existiert, dann erhält man alle Lösungen, indem man zu der speziellen Lösung v alle Lösungen des zugehörigen homogenen Gleichungssystems addiert.*

Beweis. (i) Es ist $\text{Lös}(A, 0) = \text{Kern}\, \tilde{A}$. $\text{Kern}\, \tilde{A}$ ist ein $UVR \subset K^n$ mit

$$\dim\left(\text{Kern}\, \tilde{A}\right) \overset{\text{Dimensionsformel}}{=} \dim K^n - \dim\left(\text{Bild}\, \tilde{A}\right) = n - \text{Rang}\, A.$$

(ii) Es ist $\text{Lös}(A,b) = \tilde{A}^{-1}(\{b\})$ nach Lemma 4.20 ein affiner Unterraum von K^n. Falls $\text{Lös}(A,b) \neq \emptyset$, dann gilt $b \in \text{Bild}\,\tilde{A}$ und

$$\dim\big(\text{Lös}(A,b)\big) = \dim \tilde{A}^{-1}(\{b\}) = \dim\big(\text{Kern}\,\tilde{A}\big) = n - \text{Rang}\,A.$$

(iii) Mit $v \in \text{Lös}(A,b)$ gilt nach Lemma 4.20

$$\text{Lös}(A,b) = \tilde{A}^{-1}(\{b\}) = v + \text{Kern}\,\tilde{A} = v + \text{Lös}(A,0).$$

□

Bemerkung. $\text{Lös}(A,0)$ *enthält immer die triviale Lösung* 0*; nicht-triviale Lösungen von* $Ax = 0$ *existieren wegen (i) genau dann, wenn* $\text{Rang}\,A < n$.

Definition 4.23.

$$A|b := \begin{pmatrix} a_{11} & \dots & a_{1n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m1} & \dots & a_{mn} & b_m \end{pmatrix} \in M(m \times (n+1), K)$$

heißt erweiterte Koeffizientenmatrix des LGS $Ax = b$.

Satz 4.24. *Es sind äquivalent:*

(i) $\text{Lös}(A,b) \neq \emptyset$*, d.h. das LGS* $Ax = b$ *besitzt eine Lösung.*

(ii) $\text{Rang}\,A = \text{Rang}(A|b)$.

Beweis. Es gilt $\text{Bild}\,\tilde{A} = SR(A) \subset SR(A|b) = \text{Bild}\,\widetilde{A|b}$. Damit erhalten wir

$$\begin{aligned} \text{Lös}(A,b) \neq \emptyset &\Leftrightarrow b \in \text{Bild}\,\tilde{A} \\ &\Leftrightarrow \dim \text{Bild}\,\tilde{A} = \dim \text{Bild}\,\widetilde{A|b} \\ &\Leftrightarrow \text{Rang}\,\tilde{A} = \text{Rang}\,\widetilde{A|b} \\ &\Leftrightarrow \text{Rang}\,A = \text{Rang}\,A|b. \end{aligned}$$

□

Korollar 4.25. *Es sind äquivalent:*

(i) Das LGS $Ax = b$ *hat genaue eine Lösung.*

(ii) $\text{Rang}\,A = \text{Rang}(A|b) = n$.

Beweis. "(i)⇒(ii)": Nach Satz 4.24 folgt aus der Existenz der Lösung Rang $A = \text{Rang}(A|b)$. Aus der Eindeutigkeit der Lösung folgt $\dim\big(\text{Lös}(A,b)\big) = 0$, also

$$0 = \dim\big(\text{Lös}(A,b)\big) = n - \text{Rang}\, A,$$

d.h. Rang $A = n$.

"(ii)⇒(i)": Sei Rang $A = \text{Rang}(A|b) = n$. Nach Satz 4.24 ist dann $\text{Lös}(A,b) \neq \emptyset$. Nach Satz 4.22 (ii) gilt $\dim\big(\text{Lös}(A,b)\big) = n - \text{Rang}\, A = 0$, d.h. die Lösung ist eindeutig. □

Wir möchten schließlich noch einen Algorithmus zur Bestimmung der Lösungen $\text{Lös}(A,b)$ angeben.

Definition 4.26. *Sei $A \in M(m \times n, K)$. Man sagt, A sei in strenger Zeilenstufenform (SZSF), wenn A in ZSF mit Pivotspalten an $j_1, \ldots, j_r$ ist und wenn gilt:*

(i) $a_{1j_1} = \cdots = a_{rj_r} = 1$ *und*

(ii) $a_{ij_k} = 0$ *für alle* $i \in \{1, \ldots, k-1\}$ *und* $k \in \{1, \ldots, r\}$.

Satz 4.27. *A lässt sich durch elementare Zeilenumformungen auf SZSF bringen.*

Beweis. A lässt sich mit dem Gaußschen Eliminationsverfahren aus Abschnitt 3.4.1 durch elementare Zeilenumformungen auf ZSF

$$B = \left(\begin{array}{ccccccccccc}
0 & \ldots & 0 & b_{1j_1} & * & & \ldots & & & * \\
0 & & \ldots & & 0 & b_{2j_2} & * & & \ldots & * \\
 & & & & \ddots & & & & & \\
0 & & & \ldots & & & & 0 & b_{rj_r} & * \\
\hline
0 & & & 0 & \ldots & 0 & & & & 0
\end{array}\right)$$

bringen, d.h. man erhält aus A damit B. Multipliziere nun die i-te Zeile mit $1/b_{ij_i}$ und annuliere dann die Einträge der j_k-ten Spalte oberhalb des Pivot-Elements durch Subtraktion geeigneter Vielfache der k-ten Zeile. □

Lemma 4.28. *Sei $C \in M(m \times n, K)$, $d \in K^n$. Ist $C|d$ durch eine Folge von elementaren Zeilenumformungen aus $A|b$ entstanden, so ist* $\text{Lös}(C,d) = \text{Lös}(A,b)$.

Beweis. Wegen Bemerkung 3.53 reicht es, Umformungen vom Typ (I) und (II) zu betrachten.

Typ I: Sei $C|d$ durch $A|b$ dadurch entstanden, dass die j-te Zeile mit $\lambda \in K \setminus \{0\}$

multipliziert wurde, d.h.

$$A|b := \begin{pmatrix} a_{11} & \dots & a_{1n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m1} & \dots & a_{mn} & b_m \end{pmatrix} \quad \text{und} \quad C|d := \begin{pmatrix} a_{11} & \dots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ \lambda a_{j1} & \dots & \lambda a_{jn} & \lambda b_j \\ \vdots & & \vdots & \vdots \\ a_{m1} & \dots & a_{mn} & b_m \end{pmatrix}.$$

so gilt: $x \in \text{Lös}(A|b) \;\Leftrightarrow\; Ax = b \;\Leftrightarrow Cx = d \;\Leftrightarrow\; x \in \text{Lös}(C, d)$.

Typ II: Analog. □

Beispiel 4.29. *Gegeben sei das LGS $Ax = b$ mit*

$$A = \begin{pmatrix} 1 & 2 & -1 & 1 & 3 \\ 3 & 6 & -3 & 3 & 9 \\ 4 & 8 & -4 & 5 & 9 \end{pmatrix} \quad \textit{und einem Vektor } b \in \mathbb{R}^3.$$

Betrachte zunächst das zugehörige homogene LGS. Mit elementaren Zeilenumformungen erhält man

$$A \to \begin{pmatrix} 1 & 2 & -1 & 1 & 3 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -3 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & -1 & 1 & 3 \\ 0 & 0 & 0 & 1 & -3 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & -1 & 0 & 6 \\ 0 & 0 & 0 & 1 & -3 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} := S.$$

Setze $B = \left(\begin{smallmatrix} 2 & -1 & 6 \\ 0 & 0 & -3 \end{smallmatrix}\right)$. Es gilt $Sx = 0$ genau dann, wenn $\binom{x_1}{x_4} = -B \begin{pmatrix} x_2 \\ x_3 \\ x_5 \end{pmatrix}$.

x_2, x_3, x_5 können beliebig dann gewählt werden. Der Lösungsraum $\text{Lös}(A, 0)$ des homogenen Systems ist ein UVR (Satz 4.22 (i)), der am besten durch die Angabe einer Basis beschrieben werden kann. Hierzu gibt es natürlich viele Möglickeiten; eine einfache ist, für $(x_2\ x_3\ x_5)'$ die Einheitsvektoren e_1, e_2, e_3 des $\mathbb{R}^3$ zu wählen. Für e_i gilt dann

$$\binom{x_1}{x_4} = -Be_i = -\ i\text{-te Spalte von } B,$$

d.h. wir erhalten durch Einsetzen von e_1, e_2, e_3 folgende Basisvektoren von $\text{Lös}(A, 0)$:

$$w_1 = \begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad w_2 = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad w_3 = \begin{pmatrix} -6 \\ 0 \\ 0 \\ 3 \\ 1 \end{pmatrix}.$$

Algorithmus (Gaußalgorithmus zur Lösung für ein homogenes LGS)

Eingabe: $A \in M(m \times n, K)$

Ausgabe: Basis von $\text{Lös}(A, 0)$.

1. Schritt: Bringe die Matrix durch elementare Zeilenumformungen in SZSF

$$S = \left(\begin{array}{ccccccccccc} 0 & \dots & 0 & 1 & * & 0 & \dots & & 0 & * \\ 0 & & \dots & & 0 & 1 & * & \dots & 0 & * \\ & & & & \ddots & & & & & \\ 0 & & & \dots & & & & 0 & 1 & * \\ \hline 0 & & & 0 & \dots & 0 & & & & 0 \\ & & & j_1 & & j_2 & \cdots & & j_r & \end{array}\right)$$

$r = \text{Zeilenrang}(A)$

2. Schritt: Sei $B \in M(r \times (n-r), K)$ die Matrix, die durch Streichen der Spalten mit den Indizes $j_1, \dots, j_r$ und den Zeilen mit den Indizes $r+1, \dots, n$ entsteht (diese beinhalten nur Nullen als Einträge). Seien $k_1 < k_2 < \cdots < k_{n-r}$ mit $\{1, \dots, n\} = \{j_1, \dots, j_r, k_1, \dots, k_{n-r}\}$ (d.h. die k_i sind die Indizes von Nicht-Pivot-Spalten).

3. Schritt: Eine Basis von $\text{Lös}(A, 0)$ ist gegeben durch $w_1, \dots, w_{n-r} \in K^n$, wobei

$$w_i = \begin{pmatrix} w_{i1} \\ \vdots \\ w_{in} \end{pmatrix}$$

gegeben ist durch

$$\begin{pmatrix} w_{ij_1} \\ \vdots \\ w_{ij_r} \end{pmatrix} = i\text{-te Spalte von } -B, \quad \begin{pmatrix} w_{ik_1} \\ \vdots \\ w_{ik_{n-r}} \end{pmatrix} = e_i \in K^{n-r}.$$

Beweis. Nach Lemma 4.28 gilt $\text{Lös}(A, 0) = \text{Lös}(S, 0)$ und ferner $x \in \text{Lös}(S, 0)$

$$\Leftrightarrow \quad Sx = 0 \quad \Leftrightarrow \quad 0 = \begin{pmatrix} x_{j_1} \\ \vdots \\ x_{j_r} \end{pmatrix} + B \begin{pmatrix} x_{k_1} \\ \vdots \\ x_{k_{n-r}} \end{pmatrix} \quad \Leftrightarrow \quad \begin{pmatrix} x_{j_1} \\ \vdots \\ x_{j_r} \end{pmatrix} = -B \begin{pmatrix} x_{k_1} \\ \vdots \\ x_{k_{n-r}} \end{pmatrix}.$$

Nach beliebiger Vorgabe von $x_{k_1}, \dots, x_{k_{n-r}}$ ergeben sich $x_{j_1}, \dots, x_{j_r}$ eindeutig, wenn $x \in K^n$ eine Lösung ist. Um eine Basis des Lösungsraums $\text{Lös}(A, 0) \subset K^n$ zu erhalten,

kann man mit $(x_{k_1}, \ldots, x_{k_{n-r}})'$ eine Basis des K^{n-r} durchlaufen, also bspw.

$$\begin{pmatrix} x_{k_1} \\ \vdots \\ x_{k_{n-r}} \end{pmatrix} = e_i \in K^{n-r} \quad \text{für } i = 1, \ldots, n-r.$$

Dann ist

$$\begin{pmatrix} x_{j_1} \\ \vdots \\ x_{j_r} \end{pmatrix} = i\text{-te Spalte von } -B,$$

d.h. wir erhalten obige Vektoren $w_1, \ldots, w_{n-r}$. Nach Konstruktion ist $(w_1, \ldots, w_{n-r})$ ein Erzeugendensystem von $\text{Lös}(S, 0) = \text{Lös}(A, 0)$. Die Familie $(w_1, \ldots, w_{n-r})$ ist aber auch linear unabhängig: Denn sind $\lambda_1, \ldots, \lambda_{n-r} \in K$ mit

$$\lambda_1 w_1 + \cdots + \lambda_{n-r} w_{n-r} = 0,$$

so lautet der Eintrag der k_i-ten Zeile ($i \in \{1, \ldots, n-r\}$)

$$\underbrace{\lambda_1 \underbrace{w_{1k_i}}_{=0} + \ldots + \lambda_i \underbrace{w_{ik_i}}_{=1}}_{=0} + \cdots + \underbrace{\lambda_{n-r} \underbrace{w_{n-r,k_i}}_{=0}}_{=0} = 0$$

$\Rightarrow \lambda_i = 0$ für $i = 1, \ldots, n-r$. □

Satz 4.30 (Korollar aus dem Gaußalgorithmus zur Lösung homogener LGS)**.** *Sei $A \in M(m \times n, K)$. Dann gilt*

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

Beweis. Im obigen Algorithmus haben wir gezeigt

$$\dim\big(\text{Lös}(A, 0)\big) = n - \text{Zeilenrang}(A) = n - r.$$

Nach Satz 4.22 (i) ist

$$\dim\big(\text{Lös}(A, 0)\big) = n - \text{Spaltenrang}(A) = \text{Rang } A,$$

also folgt die Behauptung. □

Beispiel 4.31 (Fortsetzung von Beispiel 4.29)**.** *Zur Suche einer speziellen Lösung des inhomogenen Systems $Ax = b$ bringen wir die Matrix $A|b$ in SZSF und erhalten für*

$b = (3, 9, 13)'$ *bzw.* $b = (3, 10, 13)'$ *mit den Umformungen aus Beispiel 4.29*

$$\left(\begin{array}{ccccc|c} 1 & 2 & -1 & 0 & 6 & 0 \\ 0 & 0 & 0 & 1 & -3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right) := S|z \quad \textit{bzw.} \quad \left(\begin{array}{ccccc|c} 1 & 2 & -1 & 0 & 6 & 2 \\ 0 & 0 & 0 & 1 & -3 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right) := \tilde{z}.$$

Für z *mit* $z_3 = 1$ *ist klar, dass es keine Lösung von* $Sx = z$ *gibt, d.h.* $\text{Lös}(A, b) = \text{Lös}(S, z) = 0$. *Im Falle* $\tilde{z}$ *ist*

$$\begin{array}{ll} j_1 = 1 \ \rightarrow & \\ & \\ & \\ j_2 = 4 \ \rightarrow & \end{array} \quad \begin{pmatrix} \tilde{z}_1 \\ 0 \\ 0 \\ \tilde{z}_2 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

eine Lösung. Man beachte, dass mit $\tilde{z}$ *gilt* $r = 2$ *und* $j_2 = 4$ *und mit* z *ist* $r = 3$ *und* $j_r = j_3 = 6 = n + 1$.

Algorithmus (Gaußalgorithmus zur Lösung für ein inhomogenes LGS)

Eingabe: $A \in M(m \times n, K)$, $b \in K^m$.

Ausgabe: Affiner Unterraum $\text{Lös}(A, b)$.

1. Schritt: Bringe die Matrix $A|b$ durch elementare Zeilenumformungen auf SZSF $S|z$. Seien $r = \text{Rang}(A|b) = \text{Rang}(S|z)$ und $j_1, \ldots, j_r$ die Positionen der Pivot-Spalten.

2. Schritt: Falls $j_r = n + 1$, dann gilt $\text{Lös}(A, b) = \emptyset$.

3. Schritt: Ist $j_r < n + 1$, dann gilt $\text{Lös}(A, b) = v + \text{Lös}(A, 0)$ mit einem $v \in \text{Lös}(A, b)$. Eine Basis von $\text{Lös}(A, 0)$ wird ermittelt wie im zugehörigen Algorithmus für ein homogenes LGS. Eine spezielle Lösung ist gegeben durch $v = (v_1, \ldots, v_n)' \in K^n$, wobei

$$\begin{pmatrix} v_{j_1} \\ \vdots \\ v_{j_r} \end{pmatrix} = \begin{pmatrix} z_1 \\ \vdots \\ z_r \end{pmatrix} \quad \text{und} \quad v_i = 0 \text{ für } i \in \{1, \ldots, n\} \setminus \{j_1, \ldots, j_r\}.$$

Beweis. Gilt $j_r = n + 1$ ist klar, dass $\text{Lös}(A, b) = \text{Lös}(S, z) = \emptyset$ ist, denn die j_r-te Gleichung des Gleichungssystems lautet $0 = 1$. Im Falle $j_r < n + 1$ ist v aus Schritt 3 eine spezielle Lösung von $Sx = z$, d.h. auch von $Ax = b$. □

4.4 Darstellende Matrizen

In Beispiel 4.2 war $\tilde{A} : K^n \to K^m$, $x \mapsto Ax$ mit $A \in M(m \times n, K)$, ein Beispiel für eine lineare Abbildung. In diesem Abschnitt wird gezeigt, dass man jede lineare Abbildung praktisch so schreiben kann. Nachfolgend seien V und W endlichdimensionale K-VRs.

Lemma 4.32. *Seien $v_1, \ldots, v_r \in V$ und $w_1, \ldots, w_r \in W$. Dann gelten:*

(i) Ist $(v_1, \ldots, v_r)$ eine linear unabhängige Familie, dann gibt es eine lineare Abbildung $f : V \to W$ mit $f(v_i) = w_i$ für $i = 1, \ldots, r$.

(ii) Ist $(v_1, \ldots, v_r)$ Basis von V, dann gibt es genau eine lineare Abbildung $f : V \to W$ mit $f(v_i) = w_i$ für $i = 1, \ldots, r$. Diese hat folgende Eigenschaften:

(a) $\operatorname{Bild} f = \operatorname{Lin}(w_1, \ldots, w_r)$. Insbesondere gilt
f ist surjektiv $\Leftrightarrow$ $(w_1, \ldots, w_r)$ ist ein Erzeugendensystem von W.

(b) f ist injektiv $\Leftrightarrow$ $(w_1, \ldots, w_r)$ ist linear unabhängig.

Beweis. (i) folgt aus (ii) mit dem Basisergänzungssatz.

(ii) Da $(v_1, \ldots, v_r)$ Basis ist, ist die Darstellung eines jeden Vektors $v \in V$ als Linearkombination aus $v_1, \ldots, v_r$ eindeutig. Somit ist folgende Abbildung $f : V \to W$ wohldefiniert:

$$v = \sum_{i=1}^{r} \lambda_i v_i \mapsto \sum_{i=1}^{r} \lambda_i w_i.$$

Es gilt $f(v_i) = w_i$ für $i = 1, \ldots, r$. Außerdem ist f linear, denn mit $u = \sum_{i=1}^{r} \mu_i v_i$ ist

$$f(u + v) = f\Big(\sum_{i=1}^{r} (\lambda_i + \mu_i) v_i \Big) = \sum_{i=1}^{r} (\lambda_i + \mu_i) w_i = f(u) + f(v),$$

analog gilt $f(\lambda v) = \lambda \cdot f(v)$ für $\lambda \in K$. [Bemerkung: Diese Konstruktion wurde auch schon einmal im Beweis von Korollar 4.14 verwendet.]

Eindeutigkeit von f: Sei $g : V \to W$ eine weitere lineare Abbildung mit $g(v_i) = w_i$. Für $v = \sum_{i=1}^{r} \lambda_i w_i$ gilt dann $g(v) = \sum_{i=1}^{r} \lambda_i g(v_i) = \sum_{i=1}^{r} \lambda_i w_i = f(v)$, d.h. $f = g$.

(a) $\operatorname{Bild} f = \operatorname{Lin}(w_1, \ldots, w_r)$ folgt aus Aussage (vi) aus Lemma 4.3.

(b) Es gilt: f injektiv $\overset{\text{Satz } 4.10(iii)}{\Leftrightarrow}$ $\operatorname{Kern} f = \{0\}$ $\overset{\text{Satz } 4.10(iv)}{\Rightarrow}$ $(\underbrace{f(v_1)}_{=w_1}, \ldots, \underbrace{f(v_r)}_{=w_r})$ linear unabh.

Umgekehrt gilt: $(w_1, \ldots, w_r)$ linear unabhängig

$\Rightarrow \dim\big(\operatorname{Bild} f\big) = r$
$\Rightarrow \dim\big(\operatorname{Kern} f\big) = \dim V - \dim\big(\operatorname{Bild} f\big) = 0$
$\Rightarrow \operatorname{Kern} f = \{0\}$, d.h. f ist injektiv.

□

Bemerkung. *Man braucht in Lemma 4.32 die lineare Unabhängigkeit der v_i, damit die Abbildung f wohldefiniert ist. Ist bspw. (v_1, v_2) mit $v_1 = v_2$, kann man nicht einfach $f(v_1) = w_1$ und $f(v_2) = w_2$ für beliebige w_1, w_2 setzen.*

Korollar und Definition 4.33. *Sei $B = (v_1, \dots, v_n)$ eine Basis von V (entspricht hier dem W aus Lemma 4.32). Dann gibt es genau einen Isomorphismus*

$$\Phi_B : K^n \to V \quad \text{mit} \quad \Phi_B(e_i) = v_i \quad \text{für } i = 1, \dots, n.$$

Die Abbildung Φ_B heißt das durch B bestimmte Koordinatensystem von V. Für $v = \sum_{i=1}^n \lambda_i v_i$ gilt

$$\Phi_B \left(\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \right) = \sum_{i=1}^n \lambda_i v_i, \quad \text{womit} \quad \Phi_B^{-1}(v) = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}.$$

D.h. Φ_B^{-1} ordnet dem Vektor $v \in V$ seine Koordinaten bzgl. B zu.

Bemerkung. *Es mag auf den ersten Blick merkwürdig erscheinen, den Begriff "Koordinatensystem" für eine Abbildung zu verwenden. Allerdings ist klar, dass zu einem Koordinatensystem neben den Basisvektoren, welche die Achsen beschreiben, auch eine Methode gehören muss, wie man einen einzelnen Vektor dann darstellt. Das beschreibt gerade die Abbildung Φ_B^{-1}.*

Beispiel 4.34 (Gedrehtes Koordinatensystem)**.** *Wir möchten den Vektor $\binom{1}{3}$ in zwei verschiedenen Koordinatensystemen darstellen.*

- *Einerseits gilt $\binom{1}{3} = 1 \cdot \binom{1}{0} + 3 \cdot \binom{0}{1}$, d.h. die Koordinaten bzgl. $B = \left(\binom{1}{0}, \binom{0}{1}\right)$ sind $\binom{1}{3}$ und $\Phi_B^{-1}\left(\binom{1}{3}\right) = \binom{1}{3}$.*
  Vektor ↑ *Koordinaten* ↑
- *Wir betrachten nun das gedrehte Koordinatensystem mit den Achsen $\binom{1}{1}$ und $\binom{-1}{1}$. Es gilt $\binom{1}{3} = 2 \cdot \binom{1}{1} + 1 \cdot \binom{-1}{1}$, d.h. die Koordinaten bzgl. $B = \left(\binom{1}{1}, \binom{-1}{1}\right)$ sind $\binom{2}{1}$ und $\Phi_B^{-1}\left(\binom{1}{3}\right) = \binom{2}{1}$.*
  Vektor ↑ *Koordinaten* ↑

Im zweiten Fall sind der dargestellte Vektor und die Koordinaten verschieden. Im ersten Fall sind der Vektor und seine Koordinaten gleich. Das liegt daran, dass als Basis die Einheitsvektoren benutzt worden sind, d.h. $B = (e_1, e_2)$ sowie daran, dass wir ein Beispiel aus dem $\mathbb{R}^2$ (allgemeiner K^n) gewählt haben.

Beispiel 4.35 (Polynomraum)**.** *Wir betrachten den $\mathbb{R}$-Vektorraum*

$$\mathbb{R}[t]_n = \{P \in \mathbb{R}[t] | \, deg(P) \leq n\} \cup \{0\}$$

der Polynome mit reellen Koeffizienten vom Grad $\leq n$ inklusive Nullpolynom von Übungsblatt 8, Aufgabe 4. $B = (P_0, P_1, \ldots, P_n)$ mit $P_0(t) = 1$ und $P_k(t) = t^k$, $1 \leq k \leq n$, bildet eine Basis von $\mathbb{R}[t]_n$. Die Abbildung Φ_B ist nun

$$\Phi_B : \mathbb{R}^{n+1} \to \mathbb{R}[t]_n, \quad \begin{pmatrix} \lambda_0 \\ \vdots \\ \lambda_n \end{pmatrix} \mapsto \sum_{i=0}^{n} \lambda_i P_i.$$

$\begin{pmatrix} \lambda_0 \\ \vdots \\ \lambda_n \end{pmatrix} = \Phi_B^{-1}\left(\sum_{i=0}^{n} \lambda_i P_i\right)$ *sind die Koordinaten des Polynoms* $\sum_{i=0}^{n} \lambda_i P_i$.

Man könnte aber auch die Basis $B' = (P_0, P_0 + P_1, \ldots, \sum_{k=0}^{n} P_k)$ verwenden mit zugehörigem Koordinatensystem $\Phi_{B'}$ und entsprechenden Koordinaten $\Phi_{B'}^{-1}(P)$ für ein Polynom $P \in \mathbb{R}[t]_n$. Z. Bsp. für $n = 2$ gilt dann

$$\Phi_B^{-1}(P_0 + P_1 + P_2) = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \quad \text{und} \quad \Phi_{B'}^{-1}(P_0 + P_1 + P_2) = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

Setzt man für die Unbekannte t Elemente des Körpers $\mathbb{R}$ ein, ist die einem Polynom $P = \sum_{i=0}^{n} \lambda_i P_i \in \mathbb{R}[t]_n$ zugeordnete Abbildung

$$\tilde{P} : \mathbb{R} \to \mathbb{R}, \quad x \mapsto P(x),$$

differenzierbar und $\tilde{P}'(x) = \sum_{i=1}^{n} i\lambda_i x^{i-1}$. Sei entsprechend

$$d: \ \mathbb{R}[t]_n \to \mathbb{R}[t]_n, \quad d(P_i) = \begin{cases} i \cdot P_{i-1} & \text{falls } i = 1, \ldots, n \\ 0 & \text{falls } i = 0. \end{cases} \qquad (d \text{ für “derivative”})$$

Damit ist die lineare Abbildung d nach Lemma 4.32 eindeutig bestimmt. Ist nun $\sum_{i=0}^{n} \lambda_i P_i$ mit Koordinaten

$$\begin{pmatrix} \lambda_0 \\ \vdots \\ \lambda_n \end{pmatrix} = \Phi_B^{-1}\left(\sum_{i=0}^{n} \lambda_i P_i\right)$$

gegeben, so gilt

$$d\Big(\sum_{i=0}^{n}\lambda_i P_i\Big)=\sum_{i=1}^{n} i\lambda_i P_{i-1}=\sum_{i=0}^{n-1}(i+1)\lambda_{i+1}P_i,$$

d.h. die Koordinaten der Abbildung sind

$$\begin{pmatrix} 1\cdot\lambda_1 \\ \vdots \\ n\cdot\lambda_n \\ 0 \end{pmatrix}.$$

Auf "Koordinatenebene" kann man das schreiben als

$$\begin{pmatrix} 1\cdot\lambda_1 \\ \vdots \\ n\cdot\lambda_n \\ 0 \end{pmatrix} = \underbrace{\begin{pmatrix} 0 & 1 & & 0 \\ & & \ddots & \\ & & \ddots & n \\ 0 & & & 0 \end{pmatrix}}_{=:A} \cdot \begin{pmatrix} \lambda_0 \\ \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$$

(Koeffizientenmatrix)

oder als Abbildung $d=\Phi_B\circ\tilde{A}\circ\Phi_B^{-1}$ von $\mathbb{R}[t]_n$ nach $\mathbb{R}[t]_n$ mit der zu A gehörenden linearen Abbildung $\tilde{A}$.

Satz und Definition 4.36. *Seien $B=(v_1,\dots,v_n)$ eine Basis von V und $C=(w_1,\dots,w_m)$ eine Basis von W. Dann gelten folgende Aussagen:*

(i) Für jede lineare Abbildung $f: V\to W$ gibt es genau eine Matrix $A=(a_{ij})$ aus $M(m\times n,K)$ mit

$$f(v_j)=\sum_{i=1}^{m} a_{ij}w_i \quad \text{für alle } j=1,\dots,n.$$

$M_C^B(f):=A$ heißt die Darstellungsmatrix von f bzgl. der Basen B und C (von V bzw. W). In der j-ten Spalte von $M_C^B(f)$ stehen die Koordinaten von $f(v_j)$ bzgl. der Basis C von W (für $j=1,\dots,n$).

(ii) Es gilt dann $f=\Phi_C\circ\widetilde{M_C^B(f)}\circ\Phi_B^{-1}$.

(iii) Die in (i) enthaltene Abbildung

$$M_C^B:\operatorname{Hom}_K(V,W)\to M(m\times n,K),\quad f\mapsto M_C^B(f)$$

ist ein Isomorphismus von K-Vektorräumen.

Insbesondere gilt

$$\dim \mathrm{Hom}_K(V,W) = m \cdot n.$$

Im Falle $V = W$ und $B = C$ ist die Abbildung

$$M_B : \mathrm{End}_K(V) \to M(n \times n, K), \quad f \mapsto M_B^B(f) =: M_B(f)$$

ein Isomorphismus von K-Vektorräumen.

Beweis. (i) folgt aus Lemma 4.32 (ii), da $B = (v_1, \ldots, v_n)$ eine Basis ist. Da $(w_1, \ldots, w_m)$ eine Basis von W ist, kann man die Bilder $f(v_j)$ als Linearkombination daraus darstellen:

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

(ii) Es gilt mit $e_j \in K^n$

$$\begin{aligned}\Big(\Phi_C \circ \widetilde{M_C^B(f)} \circ \Phi_B^{-1}\Big)(v_j) &= \Big(\Phi_C \circ \widetilde{M_C^B(f)}\Big)(e_j) \\ &= \Phi_C\big(Ae_j\big) = \Phi_C \left(\begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} \right) = \sum_{i=1}^{m} a_{ij} w_i = f(v_j).\end{aligned}$$

Da f eindeutig bestimmt ist, folgt Gleichheit.

(iii) Nachweis der Linearität: Seien $f, g \in \mathrm{Hom}_K(V,W)$ mit $M_C^B(f) = (a_{ij})$, $M_C^B(g) = (b_{ij})$. $\Rightarrow$ $(f+g)(v_j) = f(v_j) + g(v_j) = \sum_{i=1}^m a_{ij} w_i + \sum_{i=1}^m b_{ij} w_i = \sum_{i=1}^m \big(a_{ij} + b_{ij}\big) w_i$, womit

$$M_C^B(f+g) = \big(a_{ij} + b_{ij}\big) = M_C^B(f) + M_C^B(g)$$

ist. Analog zeigt man $M_C^B(\lambda f) = \lambda M_C^B(f)$.

Nachweis der Bijektivität: Ist $A = (a_{ij}) \in M(n \times n, K)$, so gibt es nach Lemma 4.32 (ii) genau ein $f \in \mathrm{Hom}_K(V,W)$ mit $f(v_j) = \sum_{i=1}^m a_{ij} w_i$ für $i = 1, \ldots, n$, d.h. M_C^B ist surjektiv und injektiv. □

Bemerkung 4.37. *Für $f \in Hom_K(V,W)$ und $v \in V$ mit $v = \sum_{j=1}^n \lambda_j v_j$ gilt damit*

$$f(v) = \sum_{j=1}^{n} \lambda_j f(v_j) = \sum_{j=1}^{n} \lambda_j \left(\sum_{i=1}^{m} a_{ij} w_i \right) = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} a_{ij} \lambda_j \right) w_i = \sum_{i=1}^{m} \left(A \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \right)_i w_i.$$

Dies ist eine andere Schreibweise für Aussage (ii) in Satz 4.36 und verdeutlicht nochmal, dass mit $A = M_C^B(f)$ die Koordinaten bezüglich der Basen B und C transformiert werden.

Was besagt Satz 4.36 für $V = K^n$, $W = K^m$ mit den Einheitsbasen $B = (e_1, \ldots, e_n)$ von K^n und $C = (e_1, \ldots, e_m)$ von K^m? Zu gegebenem $f \in \mathrm{Hom}_K(K^n, K^m)$ ist A definiert durch

$$f(e_j) = \sum_{i=1}^{m} a_{ij} e_i = \underbrace{\begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}}_{j\text{-te Spalte von } A} = Ae_j.$$

Das ist dieselbe Beziehung wie zwischen $\tilde{A}$ und A in Beispiel 4.2, d.h. $f = \tilde{A}$. Wir halten dies als Korollar fest.

Korollar 4.38. *Die Abbildung* $M_{(e_1,\ldots,e_m)}^{(e_1,\ldots,e_n)} : \mathrm{Hom}_K(K^n, K^m) \to M(m \times n, K)$ *ist ein Isomorphismus mit Umkehrabbildung*

$$\sim \; : M(m \times n, K) \to \mathrm{Hom}_K(K^n, K^m), \quad A \mapsto \tilde{A}.$$

Man kann dieses Korollar nun verwenden, um eine nicht-triviale Aussage für Matrizen herzuleiten.

Satz 4.39. *Sei $A \in M(n \times n, K)$. Dann sind äquivalent:*

(i) A besitzt eine Rechtsinverse, d.h. es existiert $B \in M(n \times n, K)$ mit $A \cdot B = E_n$.

(ii) $\tilde{A} : K^n \to K^n$ ist ein Isomorphismus.

(iii) A ist invertierbar, d.h. es existiert $B \in M(n \times n, K)$ mit $A \cdot B = B \cdot A = E_n$.

Die Aussage gilt auch, wenn man in (i) die Existenz der Linksinversen verlangt. Die Beweisidee besteht darin, die Frage nach der Inversen anstelle von $M(n \times n, K)$ in $\mathrm{Hom}_K(K^n, K^n)$ zu diskutieren, wo unmittelbar klar ist, dass aus der Existenz der Rechtsinversen auch die Existenz der Inversen folgt.

Beweis. (iii)⇒(i) ist trivial. $\tilde{A} \circ \tilde{B} = \widetilde{AB} = \tilde{E}_n = id_{K^n}$

(i)⇒(ii): Sei $B \in M(n \times n, K)$ mit $AB = E_n$.

$\Rightarrow \; K^n = (\tilde{A} \circ \tilde{B})(K^n) \subset \tilde{A}(K^n) \subset K^n$

$\Rightarrow \; \tilde{A}$ surjektiv

$\overset{\text{Korollar 4.16}}{\Rightarrow}$ $\tilde{A}$ ist bijektiv, d.h. $\tilde{A}$ ist Isomorphismus.

(ii)⇒(iii): Sei $\tilde{A}$ Isomorphismus, d.h. es existiert die inverse Abbildung g mit $\tilde{A} \circ g = g \circ \tilde{A} = id_{K^n}$. Nach Korollar 4.38 gibt es ein $B \in M(n \times n, K)$ mit $g = \tilde{B}$. ⇒ Behauptung. □

Satz 4.40 (Ringisomorphismus). *(i) Die Abbildung*

$$M_{(e_1,\dots,e_n)}^{(e_1,\dots,e_n)} : \mathrm{End}_K(K^n) \to M(n \times n, K)$$

ist auch ein Ringisomorphismus (also bijektiv und die Ringstruktur erhaltend), d.h.

$$M_{(e_1,\dots,e_n)}^{(e_1,\dots,e_n)}(f+g) = M_{(e_1,\dots,e_n)}^{(e_1,\dots,e_n)}(f) + M_{(e_1,\dots,e_n)}^{(e_1,\dots,e_n)}(g) \quad \textit{und}$$
$$M_{(e_1,\dots,e_n)}^{(e_1,\dots,e_n)}(f \circ g) = M_{(e_1,\dots,e_n)}^{(e_1,\dots,e_n)}(f) \cdot M_{(e_1,\dots,e_n)}^{(e_1,\dots,e_n)}(g) \quad \textit{für alle } f,g \in \mathrm{End}_K(K^n).$$

(ii) Sei "$*$" eine beliebige Multiplikation auf $M(n \times n, K)$, so dass $M(n \times n, K)$ mit den Verknüpfungen $+$ und $*$ einen Ring bildet. Ist $M_{(e_1,\dots,e_n)}^{(e_1,\dots,e_n)}$ dann ein Ringisomorphismus, so folgt "$* = \cdot$", d.h. die Matrixmultiplikation ist gerade so definiert, dass das Matrixprodukt die Matrix der hintereinander ausgeführten Abbildungen ist.

Bemerkung. *Eine analoge Aussage gilt auch für das Matrixprodukt $A \cdot B$ mit Matrizen $A \in M(m \times n, K)$ und $B \in M(n \times r, K)$.*

Beweis. Wir setzen $M := M_{(e_1,\dots,e_n)}^{(e_1,\dots,e_n)}$.

(i) Wir verwenden wie oben die Bezeichnung $\tilde{A}$ für die durch $A \in M(n \times n, K)$ definierte lineare Abbildung von K^n nach K^n. Es gilt für alle $x \in K^n$

$$\widetilde{AB}(x) = (AB)x = A(Bx) = A \cdot \tilde{B}(x) = \tilde{A}\big(\tilde{B}(x)\big) = \big(\tilde{A} \circ \tilde{B}\big)(x),$$

womit $M\big(\tilde{A} \circ \tilde{B}\big) = M\big(\widetilde{AB}\big) = A \cdot B = M\big(\tilde{A}\big) \cdot M\big(\tilde{B}\big)$. Da M nach Satz 4.36 bereits VR-Isomorphismus ist, gilt auch $M\big(\tilde{A} + \tilde{B}\big) = M\big(\tilde{A}\big) + M\big(\tilde{B}\big)$ und M ist bijektiv, also ist M damit Ringisomorphismus.

(ii) Sei $\sim$ die Umkehrabbildung von M aus Korollar 4.38. Nach Satz 4.36 (i) besteht die j-te Spalte von $A = M\big(\tilde{A}\big)$ aus $\tilde{A}(e_j)$, d.h. für $C = A * B$ mit $A, B \in M(n \times n, K)$ gilt

$$c_{ij} = \Big(\widetilde{A * B}(e_j)\Big)_i = \Big(\underbrace{\widetilde{M\big(\tilde{A}\big) * M\big(\tilde{B}\big)}}_{\substack{= M(\tilde{A} \circ \tilde{B}) \\ \text{da } M \text{ Ringiso-} \\ \text{morphismus}}}(e_j)\Big)_i = \Big(\big(\tilde{A} \circ \tilde{B}\big)(e_j)\Big)_i$$
$$= \big(\tilde{A}\big(\tilde{B}(e_j)\big)\big)_i = \left(\tilde{A}\left(\begin{pmatrix} b_{1j} \\ \vdots \\ b_{nj} \end{pmatrix}\right)\right)_i$$
$$= \left(\sum_{k=1}^{n} b_{kj}\tilde{A}(e_k)\right)_i = \left(\sum_{k=1}^{n} b_{kj}\begin{pmatrix} a_{1k} \\ \vdots \\ a_{nk} \end{pmatrix}\right)_i = \sum_{k=1}^{n} a_{ik}b_{kj}.$$

□

Im restlichen Teil dieses Abschnittes formulieren wir noch Konsequenzen aus Satz 4.36 und Korollar 4.38.

Satz 4.41. *Sei $U \subset K^n$. Dann sind äquivalent:*

(i) U ist UVR von K^n.

(ii) Es gibt ein $m \in \mathbb{N}$ und ein $A \in M(m \times n, K)$ mit $U = \text{Lös}(A, 0)$.

Beweis. (ii)⇒(i): Aussage (i) aus Satz 4.22.

(i)⇒(ii): Sei $(u_1, \ldots, u_r)$ eine Basis von U. Diese kann nach dem Basisergänzungssatz zu einer Basis $(u_1, \ldots, u_r, u_{r+1}, \ldots, u_n)$ von K^n ergänzt werden. Sei $m = n - r$. Definiere nun $f : K^n \to K^n$ durch

$$f(u_i) = \begin{cases} 0 & \text{falls } i \in \{1, \ldots, r\} \\ e_{i-r} & \text{falls } i \in \{r+1, \ldots, n\}. \end{cases}$$

Wegen $U \subset \text{Kern } f$ und $\dim\big(\text{Kern } f\big) = n - \dim\big(\text{Bild } f\big) = n - (n-r) = r$ (Dimensionsformel) folgt $\text{Kern } f = U$ nach Korollar 3.34 (iii). Nach Satz 4.36 und Korollar 4.38 gibt es genau ein $A \in M(m \times n, K)$ mit $f(x) = Ax$. Es gilt $\text{Lös}(A, 0) = \text{Kern } f = U$. □

Satz 4.42. *Sei $Z \subset K^n$. Dann sind äquivalent:*

(i) Z ist affiner Unterraum von K^n.

(ii) Es gibt $m \in \mathbb{N}$, $A \in M(m \times n, K)$ und $b \in K^m$ mit $Z = \text{Lös}(A, b)$.

Beweis. (ii)⇒(i): Aussage (ii) aus Satz 4.22.

(i)⇒(ii): Sei $Z = z + U$ mit $z \in Z$ und einem UVR $U \subset K^n$. Nach Satz 4.41 existieren $m \in \mathbb{N}$ und $A \in M(m \times n, K)$ mit $U = \text{Lös}(A, 0)$. Mit $b := Az$ ist $z \in \text{Lös}(A, b)$ und nach Satz 4.22 (iii) folgt $\text{Lös}(A, b) = z + U = Z$. □

Bemerkung. *Zusammenfassend ergeben Satz 4.41 und Satz 4.42:*

- *UVRs von K^n sind Lösungsräume homogener linearer Gleichungssysteme und*
- *affine Unterräume von K^n sind Lösungsräume inhomogener linearer Gleichungssysteme.*

Wir geben zu $f \in \text{Hom}_K(V, W)$ schließlich noch eine einfache Darstellungsmatrix an.

Lemma 4.43. *Sei $f : V \to W$ eine lineare Abbildung. Dann gibt es Basen B von V und C von W mit*

$$M_C^B(f) = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}, \quad r = \text{Rang } f.$$

Beweis. Sei $\bar{C} = (w_1, \ldots, w_r)$ Basis von Bild f. Sind $u_1 \in f^{-1}(\{w_1\}), \ldots, u_r \in f^{-1}(\{w_r\})$ und ist $(v_1, \ldots, v_k)$ eine Basis von Kern f, dann ist nach Satz 4.13 (Dimensionsformel) $B = (u_1, \ldots, u_r, v_1, \ldots, v_k)$ eine Basis von V mit $r + k = \dim V$. Nach Konstruktion ist $f(u_1) = w_1, \ldots, f(u_r) = w_r,\ f(v_1) = 0, \ldots, f(v_k) = 0$, d.h. $M_C^B(f) = \left(\begin{smallmatrix} E_r & 0 \\ 0 & 0 \end{smallmatrix}\right)$, wobei C eine von $\bar{C}$ ergänzte Basis von W ist. □

Bemerkung. *Sehr viel schwieriger ist es, für $f \in \mathrm{End}_K(V)$ eine Basis B zu finden, so dass $M_B(f)$ möglichst einfach ist ($\rightarrow$ Jordansche Normalform, Lineare Algebra II).*

4.5 Kommutative Diagramme und Basiswechsel

In diesem Abschnitt soll untersucht werden, wie sich die Darstellungsmatrix $M_C^B(f)$ einer linearen Abbildung f bei einem Basiswechsel verhält. Nach Satz 4.36 (ii) gilt

$$f = \Phi_C \circ \widetilde{M_C^B(f)} \circ \Phi_B^{-1}. \tag{4.2}$$

Bemerkung 4.44 (Kommutative Diagramme)**.** *In der linearen Algebra werden häufig sogenannte kommutative Diagramme verwendet, um die Gleichheit von Abbildungsverknüpfungen zu visualisieren. Schreibt man obige Identität in der Form*

$$f \circ \Phi_B = \Phi_C \circ \widetilde{M_C^B(f)},$$

so erhält man folgendes "kommutatives Diagramm":

$$\begin{array}{ccc} K^n & \xrightarrow{\Phi_B} & V \\ {\scriptstyle \widetilde{M_C^B(f)}}\downarrow & & \downarrow{\scriptstyle f} \\ K^m & \xrightarrow{\Phi_C} & W \end{array}$$

Man sagt "das Diagramm ist kommutativ", wenn man jeden Weg entlang der Pfeile "laufen" kann und immer dasselbe Ergebnis erhält ("laufen" bedeutet, die jeweilige Abbildung anzuwenden, d.h. die Abbildungen entlang des Pfads werden verknüpft). Die einzelnen Abbildungen müssen nicht bijektiv und im Allgemeinen kein Homomorphismus sein. Ist eine Abbildung bijektiv, kann man ihre Inverse hinschreiben und den Pfeil umdrehen:

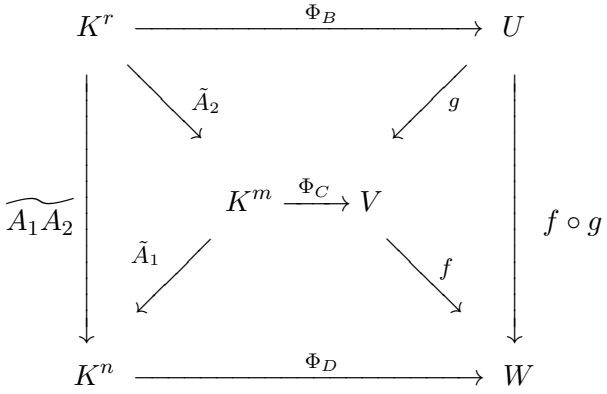
$$\begin{array}{ccc} K^n & \xleftarrow{\Phi_B^{-1}} & V \\ {\scriptstyle \widetilde{M_C^B(f)}}\downarrow & & \downarrow{\scriptstyle f} \\ K^m & \xrightarrow{\Phi_C} & W \end{array}$$

Die Kommutativität des Diagramms liefert dann direkt (4.2).

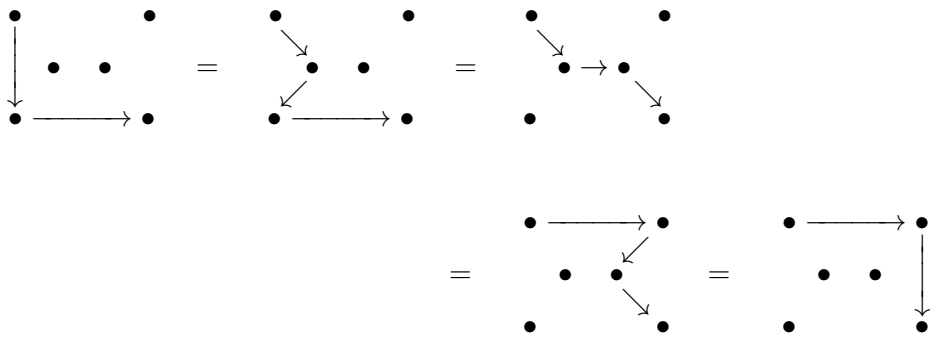
Satz 4.45. *Seien U, V, W endlichdimensionale K-VRs mit Basen B, C, D; $g : U \to V$, $f : V \to W$ lineare Abbildungen. Dann gilt*

$$M_D^B(f \circ g) = M_D^C(f) \cdot M_C^B(g).$$

Beweis. Wir setzen $r := \dim U$, $m := \dim V$, $n := \dim W$ sowie $A_1 := M_D^C(f)$, $A_2 := M_C^B(g)$. Damit ergibt sich folgendes Diagramm:



Die beiden Trapeze sind kommutativ wegen (4.2), das linke Dreieck wegen $\widetilde{A_1 A_2} = \tilde{A}_1 \circ \tilde{A}_2$, das rechte Dreieck nach Definition der Hintereinanderschaltung von Abbildungen auch. Es bleibt noch zu zeigen, dass auch das äußere Reckteck kommutiert (das gilt nicht automatisch!). Mithilfe der bereits als kommutativ verifizierten Teildiagramme folgt aber



Die Kommutativität des äußeren Rechtecks ergibt nun

$$\Phi_D \circ \widetilde{A_1 A_2} = (f \circ g) \circ \Phi_B.$$

$$\Rightarrow \widetilde{A_1 A_2} = \Phi_D^{-1} \circ (f \circ g) \circ \Phi_B = \widetilde{M_D^B(f \circ g)} \Rightarrow M_D^C(f) \cdot M_C^B(g) = A_1 A_2 = M_D^B(f \circ g). \quad \square$$

Bemerkung. *Der Beweis muss nicht mithilfe des kommutativen Diagramms geführt werden. Alternativ kann man in jedem Schritt die Gleichheit der Formeln einsetzen.*

Bemerkung 4.46. *Insbesondere ergibt Satz 4.45 für* $f, g \in \mathrm{End}_K(V)$

$$M_B(f \circ g) = M_B(f) M_B(g)$$

und damit analog zu Satz 4.40 (i), dass

$$M_B : \mathrm{End}_K(V) \to M(n \times n, K), \;\; f \mapsto M_B(f)$$

ein Ringisomorphismus ist.

Definition 4.47. *Seien* B *und* B' *Basen von* V *sowie* $n = \dim V$.

$$T^B_{B'} := M^B_{B'}(id_V) \in M(n \times n, K)$$

heißt Transformationsmatrix des Basiswechsels von B *nach* B'.

Lemma 4.48. *Seien* B, B', B'' *Basen von* V. *Dann gelten folgende Aussagen:*

(i) $T^B_{B'} \in GL(n, K)$

(ii) $\widetilde{T^B_{B'}} = \Phi^{-1}_{B'} \circ \Phi_B$

(iii) $T^B_{B'} = \left(T^{B'}_B\right)^{-1}$

(iv) $T^B_{B''} = T^{B'}_{B''} \cdot T^B_{B'}$

(v) Ist $(v_1, \ldots, v_n)$ *eine Basis von* $V = K^n$, *so folgt* $T^{(v_1,\ldots,v_n)}_{(e_1,\ldots,e_n)} = \underbrace{(v_1 \ldots v_n)}_{\substack{\text{Matrix mit} \\ \text{Spalten } v_j}}$.

Bemerkung. *(ii) zeigt, dass* $\widetilde{T^B_{B'}}$ *die Koordinaten eines beliebigen Vektors* $v \in V$ *bzgl.* B *in die Koordinaten von* v *bzgl.* B' *überführt.*

Beweis. (ii) Wir wenden (4.2) auf $f = id$ an und erhalten

$$id_V = \Phi_{B'} \circ \widetilde{T^B_{B'}} \circ \Phi^{-1}_B.$$

Da Φ_B und $\Phi_{B'}$ Isomorphismen sind, folgt

$$\Phi^{-1}_{B'} = \widetilde{T^B_{B'}} \circ \Phi^{-1}_B \text{ und daraus } \Phi^{-1}_{B'} \circ \Phi_B = \widetilde{T^B_{B'}}.$$

(i) Da Φ_B und $\Phi_{B'}$ Isomorphismen sind, ist auch $\widetilde{T^B_{B'}} = \Phi^{-1}_{B'} \circ \Phi_B$ ein Isomorphismus. Nach Satz 4.39 ist $T^B_{B'}$ damit invertierbar, d.h. $T^B_{B'} \in GL(n, K)$.

(iii) Die Aussage ist heuristisch klar. Formal: Es gilt $\widetilde{A_1 A_2} = \tilde{A}_1 \circ \tilde{A}_2$, d.h.

$$\widetilde{T^B_{B'} \cdot T^{B'}_B} = \widetilde{T^B_{B'}} \circ \widetilde{T^{B'}_B} = \Phi^{-1}_{B'} \circ \underbrace{\Phi_B \circ \Phi^{-1}_B}_{id_V} \circ \Phi_{B'} = id_{K^n} = \tilde{E}_n.$$

$\overset{\text{Satz } 4.40(i)}{\Rightarrow} T^B_{B'} \cdot T^{B'}_B = E_n \Rightarrow T^B_{B'} = \left(T^{B'}_B\right)^{-1}$.

(iv) folgt aus Satz 4.45 für $f = g = id_V$.

(v) folgt aus der Definition 4.36 der Darstellungsmatrix. □

Beispiele 4.49. *Zur Erinnerung: Sind $B = (v_1, \ldots, v_n)$ und $B' = (v'_1, \ldots, v'_n)$ Basen eines K-VRs V ($\dim_K V = n$) und $(t_{ij}) = T^B_{B'} = M^B_{B'}(id_V)$, so gilt gemäß Definition 4.36*

$$v_j = id_V(v_j) = \sum_{i=1}^{n} t_{ij} v'_i.$$

Wir betrachten nun die Beispiele 4.34 und 4.35.

Beispiel 4.34: (gedrehtes Koordinatensystem)

Mit

$$B = \left(\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right), \quad B' = \left(\begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}-1\\1\end{pmatrix}\right)$$

gelten

$$\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{2}\begin{pmatrix}1\\1\end{pmatrix} - \frac{1}{2}\begin{pmatrix}-1\\1\end{pmatrix} \quad \textit{und} \quad \begin{pmatrix}0\\1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}1\\1\end{pmatrix} + \frac{1}{2}\begin{pmatrix}-1\\1\end{pmatrix}.$$

$\Rightarrow$

$$T^B_{B'} = \begin{pmatrix} 1/2 & 1/2 \\ -1/2 & 1/2 \end{pmatrix}.$$

Beispiel 4.35: (Polynomraum)

Seien $B = (P_0, P_1, \ldots, P_n)$ und $B' = (P_0, P_0 + P_1, \ldots, \sum_{k=0}^{n} P_k)$ mit dem Nullpolynom P_0 und $P_j(t) = t^j$ für $j = 1, \ldots, n$. Dann ist $P_j = \sum_{k=0}^{j} P_k - \sum_{k=0}^{j-1} P_k$, womit

$$T^B_{B'} = \begin{pmatrix} 1 & -1 & & 0 \\ & & \ddots & \\ & & \ddots & -1 \\ 0 & & & 1 \end{pmatrix}.$$

Das Polynom $P_1 - P_0$ hat bezüglich B die Koordinaten $(-1, 1, 0, \ldots, 0)'$ und als Koordinaten in B'

$$T^B_{B'} \begin{pmatrix} -1 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} -2 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \quad \textit{(Es gilt: } P_1 - P_0 = -2P_0 + 1 \cdot (P_0 + P_1)\textit{.)}.$$

Satz 4.50 (Transformationsformel)**.** *Seien $f : V \to W$ eine lineare Abbildung, B, B' Basen von V sowie C, C' Basen von W. Dann gilt*

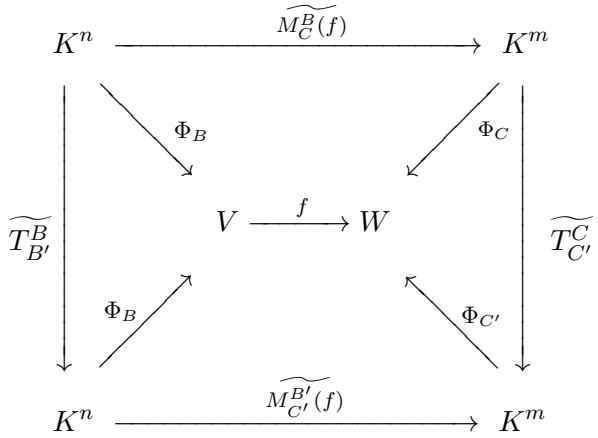
$$M_{C'}^{B'}(f) = T_{C'}^{C} M_C^B(f) T_B^{B'}.$$

Beweis. Nach (4.2) gilt

$$\widetilde{M_{C'}^{B'}(f)} = \Phi_{C'}^{-1} \circ f \circ \Phi_{B'} = \underbrace{\Phi_{C'}^{-1} \circ \Phi_C}_{=\widetilde{T_{C'}^{C}}} \circ \underbrace{\Phi_C^{-1} \circ f \circ \Phi_B}_{=\widetilde{M_C^B(f)}} \circ \underbrace{\Phi_B^{-1} \circ \Phi_{B'}}_{=\widetilde{T_B^{B'}}} = \widetilde{T_{C'}^{C} M_C^B(f) T_B^{B'}}.$$

$\Rightarrow$ Behauptung. □

Bemerkung. *Man kann den Beweis auch mit kommutativen Diagrammen zeigen (was letztlich dasselbe ist).*



Das Diagramm sieht ähnlich aus wie das im Beweis von Satz 4.45, allerdings zweimal mit anderen Richtungen im unteren Trapez ($\nearrow$ statt $\swarrow$ und $\nwarrow$ statt $\searrow$). Da $\Phi_{B'}$ und $\Phi_{C'}$ Isomorphismen sind, kann man diese Richtungen aber umdrehen und erhält wie im Beweis von Satz 4.45:

$$\underbrace{\widetilde{M_{C'}^{B'}(f)} \circ \widetilde{T_{B'}^{B}}}_{\| \; \widetilde{M_{C'}^{B'}(f) T_{B'}^{B}}} = \underbrace{\widetilde{T_{C'}^{C}} \circ \widetilde{M_C^B(f)}}_{\| \; \widetilde{T_{C'}^{C} M_C^B(f)}}$$

$\Rightarrow M_{C'}^{B'}(f) T_{B'}^{B} = T_{C'}^{C} M_C^B(f)$
$\Rightarrow M_{C'}^{B'}(f) = T_{C'}^{C} M_C^B(f) (T_{B'}^{B})^{-1} = T_{C'}^{C} M_C^B(f) T_B^{B'}$ *nach Lemma 4.48 (iii).*

Setzen wir $A_1 := M_C^B(f)$, $A_2 = M_{C'}^{B'}(f)$, $S := T_{C'}^{C}$ und $T := T_{B'}^{B}$, so gilt:

$$S \in GL(m, K), \; T \in GL(n, k) \text{ und } A_2 = S A_1 T^{-1}.$$

Im Spezialfall $W = V$ ist insbesondere der Fall $C = B$ und $C' = B'$ interessant. Hier folgt

$$M_{B'}^{B'}(f) = T_{B'}^{B} M_B^B(f) T_B^{B'},$$

d.h. mit $S := T_{B'}^B \in GL(n, K)$ ist

$$A_2 = S A_1 S^{-1}.$$

Definition 4.51.

(i) Zwei Matrizen $A_1, A_2 \in M(m \times n, K)$ heißen äquivalent ($A_1 \sim A_2$), falls es Matrizen $S \in GL(m, K)$ und $T \in GL(n, K)$ gibt mit $A_2 = S A_1 T^{-1}$.

(i) Matrizen $A_1, A_2 \in M(n \times n, K)$ heißen ähnlich, falls es eine Matrix $S \in GL(n, K)$ gibt mit $A_2 = S A_1 S^{-1}$.

Die Relation $\sim$ ist reflexiv ($A \sim A$), symmetrisch ($A_1 \sim A_2 \Rightarrow A_2 \sim A_1$) und transitiv ($A_1 \sim A_2,\ A_2 \sim A_3 \Rightarrow A_1 \sim A_3$) und definiert somit eine Äquivalenzrelation auf $M(m \times n, K)$. Analog definiert Ähnlichkeit eine Äquivalenzrelation auf $M(n \times n, K)$.

Satz 4.52. *Seien $A_1, A_2 \in M(m \times n, K)$, B Basis von K^n, C Basis von K^m, desweiteren $f : K^n \to K^m$ eine lineare Abbildung und $M_C^B(f) = A_1$. Dann sind äquivalent:*

(i) $A_1 \sim A_2$.

(ii) Es gibt Basen B' von K^n und C' von K^m mit $M_{C'}^{B'}(f) = A_2$.

(iii) $\operatorname{Rang} A_1 = \operatorname{Rang} A_2$.

Insbesondere ist jede Matrix $A \in M(m \times n, K)$ vom Rang r äquivalent zu $\left(\begin{smallmatrix} E_r & 0 \\ 0 & 0 \end{smallmatrix}\right)$.

Beweis. [Wir hatten oben (ii)⇒(i) gezeigt.]

(i)⇒(ii): Sei $A_1 \sim A_2$, d.h. es existieren $S \in GL(m, K)$, $T \in GL(n, K)$ mit $A_2 = S A_1 T^{-1}$. Sei $B = (v_1, \ldots, v_n)$, $T^{-1} = (t_{ij})$. Setze

$$v_j' := t_{1j} v_1 + \cdots + t_{nj} v_n \text{ für } j = 1, \ldots, n, \quad B' := (v_1', \ldots, v_n').$$

Es gilt: $T^{-1} \in GL(n, k) \overset{\text{Satz 4.39}}{\Rightarrow} \widetilde{T^{-1}}$ ist Isomorphismus $\overset{\text{Lemma 4.32}}{\Rightarrow} B'$ Basis. Nach Konstruktion ist

$$T^{-1} = M_B^{B'}(id_{K^n}) = T_B^{B'}.$$

Analog erhalten wir eine Basis C' mit $S^{-1} = T_C^{C'} \Leftrightarrow S = T_{C'}^C$. Es folgt

$$A_2 = S A_1 T^{-1} = T_{C'}^C M_C^B(f) T_B^{B'} = M_{C'}^{B'}(f).$$

(ii)⇒(iii): Es gilt:

$$\begin{aligned}\operatorname{Rang} A_1 = \operatorname{Rang} \tilde{A}_1 = \operatorname{Rang} \widetilde{M_C^B(f)} &= \operatorname{Rang}\left(\Phi_C^{-1} \circ f \circ \Phi_B\right) \\ &\overset{\Phi_B \text{ Isom.}}{=} \dim\left((\Phi_C^{-1} \circ f)(K^n)\right) \\ &\overset{\Phi_C^{-1} \text{ Isom.}}{=} \dim f(K^n) = \dim \operatorname{Bild}(f) = \operatorname{Rang} f.\end{aligned}$$

Analog zeigt man $\operatorname{Rang} A_2 = \operatorname{Rang} f \Rightarrow \operatorname{Rang} A_1 = \operatorname{Rang} A_2$.

(iii)⇒(i): Gelte $\operatorname{Rang} A_1 = \operatorname{Rang} A_2$ $(= r)$. Nach Lemma 4.43 gibt es Basen B von K^n und C von K^m mit

$$\begin{aligned}\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} &= M_C^B(\tilde{A}_1) \\ &= T_C^{(e_1,\ldots,e_n)} M_{(e_1,\ldots,e_n)}^{(e_1,\ldots,e_n)}(\tilde{A}_1) T_{(e_1,\ldots,e_n)}^B =: S A_1 T^{-1}.\end{aligned}$$

$\Rightarrow A_1 \sim \left(\begin{smallmatrix} E_r & 0 \\ 0 & 0 \end{smallmatrix}\right)$. Analog zeigt man $\left(\begin{smallmatrix} E_r & 0 \\ 0 & 0 \end{smallmatrix}\right) \sim A_2 \Rightarrow A_1 \sim A_2$. □

Literatur

wird noch ergänzt.