Zusammenfassung*Lineare Algebra I

gehalten von Prof. Dr. Stefan Schwede, Universität Bonn
im Wintersemester 2012/2013

Robert Hemstedt
r@twopi.eu

4. Februar 2013

Hinweise zur Verwendung

Die stets aktuelle Version dieser Zusammenfassung lässt sich finden unter
`http://github.com/euklid/Zusf-LinAI` .
Dort sind auch die `.tex`-Dateien zu finden, wenn man selbst Veränderungen vornehmen möchte.
Bitte beachtet die **Lizenzhinweise**.

Werter Kommilitone, diese Zusammenfassung basiert zum größten Teil auf meinen Mitschriften unserer LA-Vorlesungen bei Prof. Dr. Schwede sowie teilweise auf dem Fischer[1].

Was die Nummerierung der Sätze und Kapitelabschnitte angeht, so ist sie nicht mit der aus dem Fischer identisch.

Gedacht ist diese Zusammenfassung explizit als Prüfungsvorbereitung und wird daher auch noch bis zur letzten Vorlesung weiterhin ergänzt. Wenn du Anmerkungen, Ergänzungen, Lob oder Kritik haben solltest, dann sprich mich einfach an, schick mir eine E-Mail oder, was das beste wohl ist, benutze `github.com`, um mir eine *pull*-Request zu schicken.

Ich hafte weder für „fehlende“ Inhalte noch für inhaltliche oder sprachliche Fehler.

Ich hoffe, dass diese Zusammenfassung und der damit verbundene Aufwand sich nicht nur für mich als Verfasser, sondern auch noch für dich als Kommilitone lohnen wird und der Aufwand auch in Form einer möglichst guten Klausurnote entlohnt wird.
Viel Spaß beim Lernen!

Lizenz

*nach meinen persönlichen Aufzeichnungen
[1] Gerd Fischer, Lineare Algebra, Vieweg

Weitere Hinweise lassen sich finden unter: `http://de.wikipedia.org/wiki/Beerware`

1 Erste Anfänge

$\mathbb{R}$ = Körper der reellen Zahlen; $\mathbb{R}^n = \{(x_1, \ldots, x_n) : x_{i\in\{1,\ldots,n\}} \in \mathbb{R}\}$, entspricht der Menge der n-Tupel reller Zahlen; $n \in \mathbb{N} = \{1, 2, 3, \ldots\}$
$x = (x_1, \ldots, x_n)$ hat x_i als i-te Koordinate/Komponente
Addition in $\mathbb{R}^n : (x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$
Skalarmultiplikation: $\lambda \in \mathbb{R}, \lambda \cdot (x_1, x_2, \ldots, x_n) = (\lambda \cdot x_1, \lambda \cdot x_2, \ldots, \lambda \cdot x_n)$
Nullvektor: $0 = (\underbrace{(0, 0, \ldots, 0)}_{n \text{ Nullen}}; 0 + x = x = x + 0$
Negative: $-x = (-x_1, -x_2, \ldots, -x_n)$

1.1 Gerade in der Ebene

$v, v' \in R, v \neq v', w = v' - v$, $L = \{x \in \mathbb{R}^2 :$es gibt $\lambda \in R$ mit $x = v + \lambda w\} = v + \mathbb{R} \cdot w$
Parametrisierung: $\Phi : \mathbb{R} \to L \subseteq \mathbb{R}^2$, $\lambda \mapsto v + \lambda w = \Phi(\lambda)$
Alternativ: Beschreibung durch Gleichungssystem: Seien $a_1, a_2, b \in \mathbb{R}$. Betrachte die Menge $L = \{(x_1, x_2) \in \mathbb{R}^2 : a_1x_1 + a_2x_2 = b\}$, Koeffizienten: a_1, a_2, b; Unbestimmte: x_1, x_2
Spezialfall: $a_1 = a_2 = 0$, also $L = \{(x_1, x_2) \in \mathbb{R}^2 : 0 = b\} = \begin{cases} \mathbb{R}^2, & \text{falls } b = 0 \\ \emptyset, & \text{sonst} \end{cases}$
Spezialfall: $a_2 = 0, a_1 \neq 0 : L = \{(x_1, x_2) \in \mathbb{R}^2 : a_1x_1 = b\}, x_1 = \frac{b}{a_1} \to$ Parametrisierung $\Phi : \mathbb{R} \to L, \Phi(\lambda) = \left(\frac{b}{a_1}, \lambda\right)$
Spezialfall: $a_1 = 0, a_2 \neq 0$ analog
„Allgemeiner Fall“: $a_1 \neq 0, a_2 \neq 0$
Schnittpunkte von L mit den Achsen sind: $x_1 = 0 : x_2 = \frac{b}{a_2} \Rightarrow \left(0; \frac{b}{a_2}\right) \in L, x_2 = 0 : x_1 = \frac{b}{a_1} \Rightarrow \left(\frac{b}{a_1}; 0\right) \in L \Rightarrow$ Parametrisierung für $b \neq 0 : \Phi : \mathbb{R} \to L \subset \mathbb{R}^2, \Phi(\lambda) = \left(0, \frac{b}{a_2}\right) + \lambda\left(\frac{b}{a_1}, -\frac{b}{a_2}\right) = \left(\lambda\frac{b}{a_1}, \frac{b}{a_2} - \lambda\frac{b}{a_2}\right)$
Zwei Geraden in einer Ebene schneiden sich „typischerweise“ in einem Punkt.

Definition 1.1: *Eine Teilmenge $L \subseteq \mathbb{R}^2$ heißt Gerade, falls es $a_1, a_2 \in \mathbb{R}$ gibt mit $(a_1, a_2) \neq (0, 0)$, so dass $L = \{(x_1, x_2) \in \mathbb{R}^2 : a_1x_1 + a_2x_2 = b\}$.*

Satz 1.2: *Eine Teilmenge $L \subseteq \mathbb{R}^2$ ist genau dann Gerade, wenn es $v, w \in \mathbb{R}^2$ gibt, mit $w \neq 0$, sodass $L = v + \mathbb{R}w$*

1.2 Ebenen und Geraden im Raum ($\mathbb{R}^3$)

Durch zwei gegebene verschiedene Punkte $v, v' \in \mathbb{R}^3$ geht genau eine Gerade $L = \{v + \lambda w : \lambda \in \mathbb{R}\}$, wobei $w = v' - v$.
Betrachte lineare Gleichung $a_1x_1 + a_2x_2 + a_3x_3 = b$ mit $(E = \{(x_1, x_2, x_3) \in \mathbb{R}^3 : a_1x_1 + a_2x_2 + a_3x_3 = b\})$, Parameter $a_1, a_2, a_3, b \in \mathbb{R}$
1. Fall: $a_1 = a_2 = a_3 = 0 \Rightarrow \begin{cases} E = \emptyset, & \text{falls } b \neq 0 \\ E = \mathbb{R}^3, & \text{falls } b = 0 \end{cases}$
2. Fall: $a_1 = a_2 = 0, a_3 \neq 0$ $E = \left\{(x_1, x_2, x_3) : x_3 = \frac{b}{a_3}\right\}$
3. Fall: $a_3 = 0, (a_1, a_2) \neq 0$ $E = \{(x_1, x_2, x_3) : a_1x_1 + a_2x_2 = b\}$

Definition 1.3: *Eine Teilmenge $E \subseteq \mathbb{R}^3$ heißt Ebene, wenn es $a_1, a_2, a_3, b \in \mathbb{R}$ mit $(a_1, a_2, a_3) \neq (0,0,0)$ gibt, sodass $E = \{(x_1, x_2, x_3) \in \mathbb{R}^3 : a_1x_1 + a_2x_2 + a_3x_3 = b\}$.*
Parametrisierung? $\Phi : \mathbb{R}^2 \to \mathbb{R}^3$ mit Bild die Menge E. Sei z.B. $a_3 \neq 0 :\Rightarrow x_3 = \frac{b-a_1x_1-a_2x_2}{a_3}$, x_1 und x_2 frei wählbar, x_3 festgelegt.
Wir können nun bezeichnen $\Phi(\lambda_1, \lambda_2) = \left(\lambda_1, \lambda 2, \frac{b-a_1\lambda_1-a_2\lambda_2}{a_3}\right) \in E$. Φ ist eine Bijektion auf E.
Andere Schreibweise: $E = u + \mathbb{R}v + \mathbb{R}w = \{(x_1, x_2, x_3) = x \in \mathbb{R}^3 :$ es gibt $\lambda_1, \lambda_2 \in \mathbb{R}$ mit $x = u + \lambda_1 v + \lambda_2 w\}$. Man nehme z.B. $u = Phi(0;0), v = \Phi(1;0), w = \Phi(0;1)$.

1.3 Kompakte Schreibweisen für lineare Gleichungssysteme

Gleichungssystem mit n Unbestimmten und m Gleichungen: $a_{ij}, b_i \in \mathbb{R}$ (i-te Zeile und j-te Spalte)

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

Man kodiert die Koeffizienten in einer sogenannten Koeffizientenmatrix

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i1} & a_{i2} & \ldots & a_{in} \\ \vdots & \vdots & \ddots & \vdots \\ a_{11} & a_{12} & \ldots & a_{1n} \end{pmatrix}$$

$m \times n$-Matrix
m - Anzahl Zeilen
n - Anzahl der Spalten

Wir schreiben die Unbestimmten in einen Spaltenvektor: $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, $b = \begin{pmatrix} x_1 \\ \vdots \\ b_m \end{pmatrix}$. Wir definieren ein Produkt aus einer $m \times n$- Matrix und einem n-Spaltenvektor:

$$A \cdot x = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{11} & a_{12} & \ldots & a_{1n} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \left.\begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n \\ \vdots \qquad\qquad \vdots \qquad\quad \ddots \qquad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n \end{pmatrix}\right\} m\text{-Spaltenvektor}$$

die i-te Gleichung des Systems lautet dann $\sum_{j=1}^{n} a_{ij}x_j = b_i$. Das gesamte Gleichungssystem ist also äquivalent zu $\sum_{j=1}^{n} a_{ij}x_j = b_i$ für alle $i = 1, \ldots, m$.
Lösungsmenge des Gleichungssystems: $\text{Lös}(A, b) = \{x \in \mathbb{R}^n : Ax = b\}$.

1.4 Gauß'sches Eliminierungsverfahren

1. Umformung der Matrix auf Zeilenstufenform
2. explizites Lösen „von unten nach oben“

1.4.1 Explizites Lösen

Definition 1.4: *Eine $m \times n$-Matrix hat Zeilenstufenform, wenn sie von folgender Form ist:*

Definition 1.5 (formaler):

- *Es gibt eine Zahl r mit $0 \leq r \leq m$, sodass die ersten r Zeilen nicht 0 sind und die Zeilen $r+1, \ldots, m$ 0 sind.*
- *Für alle $1 \leq i \leq r$ sei j_i der Index derjenigen Spalte, die zuerst $\neq 0$ ist. $j_i = \min\{j : a_{ij} \neq 0\}$. Dann gilt $j_1 < j_2 < \ldots < j_r$.*

Spezialfall: $j_1 = 1, j_2 = 2, \ldots, j_r = r$ Die erweiterte Koeffizientenmatrix hat folgende Form: $a_{ii} \neq 0$ für $i = 1, \ldots, r$.

1. Fall: es gibt ein $i = r+1, \ldots, m$ mit $b_i \neq 0$. Dann ist eine der Gleichungen $0 = b_i \neq 0$. Dann ist $\text{Lös}(A, b) = \emptyset$.
2. Fall: $b_{r+1} = b_{r+2} = \ldots = b_m = 0$ (Beachte: $r = m$ zugelassen, dann sind wir immer im zweiten Fall.) Dann sind $x_{r+1}, \ldots, x_m$ freie Variablen, deren Werte frei gewählt werden können und man erhält $x_r, x_{r-1}, \ldots, x_2, x_1$ durch sukzessives Auflösen nach der Variable und einsetzen. Wir wählen Parameter $\lambda_1, \ldots, \lambda_k \in \mathbb{R}$ ($k = n - r$, Anzahl der freien Variablen) und setzen $x_{r+1} := \lambda_1, \ldots, x_m := \lambda_k$. x_r erhält man durch Auflösen von $a_{rr}x_r + a_{r,r+1}\lambda_1 + \ldots + a_{rn}\lambda_k = b_r$. Auflösen gibt dann: $x_r := \frac{1}{a_{rr}}(b_r - a_{r,r+1}\lambda_1 - \ldots - a_{rn}\lambda_k)$. Am Ende erhalten wir (alle) Lösungen des Gleichungssystems als $x_n = \lambda_k, \ldots, x_{r+1} = \lambda_1$ frei wählbar, $x_r = \frac{1}{a_{rr}}(b_r - a_{r,r+1}\lambda_1 - \ldots - a_{rn}\lambda_k)$, usw. $x_{r-1} = \ldots, \ldots, x_1 = \ldots$ als explizite Ausdrücke in den $\lambda_1, \ldots, \lambda_k$.
Man erhält auf diese Weise eine Parametrisierung des Lösungsraumes $\Phi : \mathbb{R}^k \to \text{Lös}(A, b) \subseteq \mathbb{R}^n$, $(\lambda_1, \ldots, \lambda_k) \mapsto (x_1, \ldots, x_r, \lambda_1, \ldots, \lambda_k)$. Φ ist injektiv, später zeigen wir, dass Φ auch surjektiv ist.

1.4.2 Umformung zur Zeilenstufenform

Definition 1.6: *Eine elementare Zeilenumformung eines Gleichungssystems ist eine von folgenden Operationen:*

1. *Vertauschen von zwei Zeilen*
2. *Addieren des λ-fachen der i-ten Zeile zu k-ten Zeile, wobie $\lambda \in \mathbb{R}, \lambda \neq 0, i \neq k$.*

Satz 1.7: *Sei (A, b) die erweiterte Koeffizientenmatrix eines linearen Gleichungssystems und $(\tilde{A}, \tilde{b})$ entstehe aus (A, b) durch endliche viele Umformungen von Typ 1 und 2. Dann haben die Gleichungssysteme $A \cdot x = b$ und $\tilde{A} \cdot x = b$ dieselben Lösungen, d.h.* $\text{Lös}(A, b) = \text{Lös}(\tilde{A}, \tilde{b})$.
Vorsicht: Der Lösungsraum ändert sich bei elementaren Spaltenumformungen.

Satz 1.8: *Jede Matrix A kann durch endlich viele elementare Zeilenumformungen auf Zeilenstufenform gebracht werden. (Einfach Gauß-Algorithmus mit Umformungen des Typs 1 und 2 anwenden...)*

1.4.3 Zusammenfassung des Gauß-Verfahrens

1. Man stelle die erweiterte Koeffizientenmatrix auf.
2. Man bringt die Matrix A auf Zeilenstufenform und führt gleichartig die Umformungen mit b durch.
3. Man liest an b und r ab, ob es überhaupt Lösungen gibt. Falls es Lösungen gibt, wählt man die freien Variablen als Parameter und löst von unten nach oben auf.

2 Gruppen

Eine binäre Verknüpfung (Komposition) ist eine Abbildung $* : G \times G \to G, (a, b) \mapsto *(a, b) = a * b$.
Sei X eine Menge. Dann ist $\mathrm{Abb}(X, X)$ die Menge aller Abbildungen von X zu sich. Auf $\mathrm{Abb}(X, X)$ gibt es die Komposition $\circ : \mathrm{Abb}(X, X) \times \mathrm{Abb}(X, X) \to \mathrm{Abb}(X, X)$, $(f, g) \mapsto f \circ g$, wobei $f \circ g : X \to X$ definiert ist durch $(f \circ g)(x) = f(g(x))$ für $x \in X$. Diese Verknüpfung ist assoziativ.

Definition 2.1: *Eine Gruppe ist eine Menge G zusammen mit einer Verknüpfung $* : G \times G \to G$, die folgende Eigenschaften hat:*

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

(G2) *(a) Es existiert ein $e \in G$ mit linksneutraler Eigenschaft: $e * a = a$ für alle $a \in G$.*

(b) Existenz von Linksinverse: zu jedem $a \in G$ gibt es ein $a' \in G$, sodass $a' * a = e$.

Eine Gruppe heißt kommutativ, falls zusätzlich gilt $a * b = b * a \ \forall a, b \in G$. Typische Symbole für Verknüpfungen von Gruppen: $*, +, \cdot, \circ, \ldots$. Konvention: das Symbol „+“ wird nur für kommutative Verknüpfungen verwendet.
Wenn eine Verknüpfung assoziativ ist, kann man Klammern weglassen: $(a * b) * c = a * (b * c) = a * b * c$. Man lässt unter Umständen das Verknüpfungssymbol weg und schreibt abc für $a * b * c$.

$\mathrm{Abb}(X, X)$ ist wegen fehlender Inverse keine Gruppe. Betrachtet man jedoch nur die bijektiven Abbildungen, so ist $(S(X), \circ)$ eine Gruppe (die **symmetrische Gruppe von X**) mit der Komposition $\circ$ von Funktionen als Verknüpfung, wobei $S(X)$ die Menge aller bijektiven Abbildungen von X nach X ist, für X nichtleere Menge. Beispiele für kommutative Gruppen sind $(\mathbb{Z}, \cdot), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R} \setminus \{0\}, \cdot)$.

Satz 2.2: *Sei $(G, \cdot)$ eine Gruppe, dann gilt:*

(a) *Das neutrale Element e ist eindeutig. Außerdem ist es auch rechtsneutral: $a \cdot e = a$ für alle $a \in G$.*

(b) *Das linksinverse Element a' zu a bzgl. e ist eindeutig und auch rechtsinverse, d.h. $a \cdot a' = e$. Notation: Wir bezeichnen in einer Gruppe mit a^{-1} das zu a inverse Element.*

(c) *Für alle $a, b \in G$ gilt: $(a^{-1})^{-1}$ und $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$*

(d) *Kürzungsregel: Seien $a, \tilde{x}, x, \tilde{y}, y \in G$. Wenn gilt $a \cdot \tilde{x} = a \cdot x$, dann auch $\tilde{x} = x$. Wenn $y \cdot a = \tilde{y} \cdot a$, dann auch $y = \tilde{y}$.*

Sei $(G, \cdot)$ ein Paar aus einer Menge $G \neq \emptyset$ und einer Verknüpfung $\cdot$. Für $a \in G$ definieren wir die **Translationabbildung** $\tau_a : G \to G, x \mapsto \tau_a(x) = x \cdot a$, ${}_a\tau : G \to G, x \mapsto {}_a\tau(x) = a \cdot x$.

Lemma 2.3: *Ist $(G, \cdot)$ eine Gruppe, so sind für jedes $a \in G$ die Abbildungen τ_a und ${}_a\tau$ bijektiv. Sei $(G, \cdot)$ mit $\cdot$ assoziativ. Falls für alle $a \in G$ die Abbildungen τ_a und ${}_a\tau$ surjektiv sind, so ist $(G, \cdot)$ eine Gruppe.*

Verknüpfungstafeln: Für eine n-elementige Menge $G = \{a_1, \ldots, a_n\}$ kann man im Prinzip die Verknüpfung durch Angabe aller Werte in einer quadratischen Tafel angeben. In der i-ten Zeile (Spalte) der Tafel stehen die Bilder der Translationsabbildungen ${}_{a_i}\tau$ (bzw. τ_{a_i}). Da ${}_{a_i}\tau$ und τ_{a_i} in einer Gruppe bijektiv sind, muss in jeder Zeile und Spalte jedes Element genau einmal vorkommen.

Definition 2.4: *Sei $(G, \cdot)$ eine Gruppe. Eine nichtleere Teilmenge $G' \subseteq G$ heißt Untergruppe, falls gilt:*

- *für alle $a, b \in G'$ liegt auch $a \cdot b$ in G',*
- *für alle $a \in G'$ liegt auch a^{-1} in G'.*

Bemerkung 2.5: G' ist selbst eine Gruppe bezüglich der eingeschränkten Verknüpfung $\cdot : G' \times G' \to G'$.

- Assoziativität: gilt in G, daher auch in G'
- neutrales Element: wegen $a \in G' \Rightarrow a^{-1} \in G' \Rightarrow e = a^{-1} \cdot a \in G'$. e linksneutral in G, also auch in G'. Weiterhin ist a^{-1} das linksinverse von a, sodass G' alle Gruppeneigenschaften erfüllt.

Sei X eine Menge, $Y \subseteq X$ eine Teilmenge. Dann ist $\{f : X \to X : f \text{ ist bijektiv, } f(y) = y \; \forall y \in Y\}$ eine Untergruppe von $(S(X), \circ)$.

Definition 2.6: *Seien $(G, \cdot)$ und $(H, *)$ zwei Gruppen. Eine Abbildung $\varphi : G \to H$ heißt* **Gruppenhomomorphismus**, *falls $\varphi(a \cdot b) = \varphi(a) * \varphi(b)$ für alle $a, b \in G$.*

Bemerkung 2.7: Sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Dann gilt:

(a) Es gilt $\varphi(e) = \bar{e}$, wenn $e \in G$ bzw. $\bar{e} \in H$ die neutralen Elemente bezeichnen.

(b) Es gilt $\varphi(a)^{-1} = \varphi(a^{-1})$ für alle $a \in G$.

(c) Falls φ bijektiv ist, so ist die Umkehrabbildung $\varphi^{-1} : H \to G$ auch ein Gruppenhomomorphismus.

Bemerkung 2.8:

(i) Sei $\varphi : G \to H$ ein Gruppenhomomorphismus. Dann ist das Bild $\mathrm{Im}(\varphi) = \{h \in H : \text{es gibt ein } g \in G \text{ mit } \varphi(g) = h\}$ eine Untergruppe von $(H, *)$.

(ii) Sein $\psi : H \to K$ ein weiterer Gruppenhomomorphismus. Dann ist auch $\psi \circ \varphi : G \to K$ ein Gruppenhomomorphismus.

Definition 2.9: *Für alle $m \in \mathbb{Z}$ ist die Abbildung $m \cdot - : \mathbb{Z} \to \mathbb{Z}$ ein Endomorphismus von $(\mathbb{Z}, +)$. Also ist $m\mathbb{Z} = \mathrm{Im}(m \cdot -) = \{m \cdot a : a \in \mathbb{Z}\}$ die durch m teilbaren Zahlen eine Untergruppe von $(\mathbb{Z}, +)$. Zu $r, m \in \mathbb{Z}$ definieren wir die Menge $r + m\mathbb{Z} := \{r + m \cdot a : a \in \mathbb{Z}\}$ als um r verschobene Untergruppe $m\mathbb{Z}$ in $\mathbb{Z}$.*

Weiter ist $0 + m\mathbb{Z} = m\mathbb{Z}, m + m\mathbb{Z} = m\mathbb{Z}$.
Sei nun $m \geq 1$ und $0 \leq r \leq m - 1$ „die möglichen Reste bei Teilen durch m“. $\mathbb{Z} = \bigcup_{r=0}^{m-1} (r + m\mathbb{Z})$. Der Rest beim Teilen durch m entscheidet, in welcher der Mengen in der Vereinigung eine ganze Zahl liegt. Die Mengen $0 + m\mathbb{Z}, 1 + m\mathbb{Z}, 2 + m\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z}$ sind disjunkt.

Bemerkung 2.10: a und $a' \in \mathbb{Z}$ liegen genau dann in derselben Restklasse modulo m, wenn gilt, dass $a - a'$ durch m teilbar ist.

Wenn ein $m \geq 1$ fixiert ist, schreiben wir kürzer $\bar{a} = a + m\mathbb{Z}$ für die Restklasse von a modulo m. Dann gilt also $\bar{a} = \bar{a}' \Leftrightarrow a - a'$ ist durch m teilbar.

Definition 2.11: *Für $m \geq 1$ ganze Zahl ist $\mathbb{Z}/m\mathbb{Z}$ die Menge aller Restklassen modulo m.* $\mathbb{Z}/m\mathbb{Z} = \{r+m\mathbb{Z} : r \in \mathbb{Z}\} = \{0+m\mathbb{Z}, 1+m\mathbb{Z}, \ldots, (m-1)+m\mathbb{Z}\}$. $+ : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ *ist definiert durch* $(\bar{a}, \bar{b}) \mapsto \bar{a} + \bar{b} := \overline{a+b}$.

Satz 2.12: *Sei $m \geq 1$ eine ganze Zahl. Dann bildet die Menge* $\mathbb{Z}/m\mathbb{Z} = \{r + m\mathbb{Z} : r \in \mathbb{Z}\} = \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$ *eine kommutative Gruppe bezüglich* $+ : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, $(\bar{a}, \bar{b}) \mapsto \bar{a} + \bar{b} := \overline{a+b}$. *Außerdem ist die Restklassenabbildung* $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, $a \mapsto a + m\mathbb{Z} = \bar{a}$ *ein surjektiver Gruppenhomomorphismus.*

$m = 0 : 0\mathbb{Z} = \{0\}, r + 0\mathbb{Z} = \{r\}, Z/0\mathbb{Z} = \{\{r\} : r \in \mathbb{Z}\}$"="$\mathbb{Z}$ unendliche zyklische Gruppe.
zyklisch: Die Translationsabbildung $\tau_{\bar{1}} : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ „rotiert“ die Elemente zyklisch.

3 Ringe, Körper

Definition 3.1: *Ein Ring ist eine Menge R mit zwei binären Verknüpfungen* $+ : R \times R \to R, (a, b) \mapsto a + b$ *und* $\cdot : R \times R \to R, (a, b) \mapsto a \cdot b$ *mit folgenden Eigenschaften:*

(R1) $(R, +)$ *ist eine kommutative Gruppe. Notation:* 0 *bezeichnet das bezüglich* $+$ *neutrale Element,* $-a$ *das bezüglich* a *inverse Element.*

(R2) $\cdot$ *ist assoziativ.*

(R3) *Distributivgesetze: für alle* $a, b, c \in R$ *gilt:*

- $a \cdot (b + c) = a \cdot b + a \cdot c$ *und*
- $(a + b) \cdot c = a \cdot b + b \cdot c$

„Punkt- vor Strichrechnung“.
Ein Ring heißt **kommutativ**, *wenn die Verknüpfung $\cdot$ kommutativ ist. Ein Element $1 \in R$ heißt* **Einselement**, *wenn gilt $1 \cdot a = a = a \cdot 1$ $\forall a \in R$ (d.h., 1 ist beidseitig neutral bezüglich $\cdot$).*
Vorsicht: Viele Quellen verlangen, dass ein Ring ein Einselement enthalten muss.

Bemerkung 3.2: Wenn 0 das neutrale Element bezüglich + bezeichnet, so gilt $0 \cdot a = 0 = a \cdot 0$ für alle $a \in R$

Definition 3.3: *Ein Ring heißt* **nullteilerfrei**, *falls für alle $a, b \in R$ mit $a \cdot b = 0$ schon folgt $a = 0$ oder $b = 0$. $\Leftrightarrow$ die Menge $R \setminus \{0\}$ ist abgeschlossen unter $\cdot$.*

Lemma 3.4: *Sei $m \geq 2$ eine ganze Zahl. Der Ring $\mathbb{Z}/m\mathbb{Z}$ ist genau dann nullteilerfrei, wenn m eine Primzahl ist.*

Definition 3.5: *Sei $(R, +, \cdot)$ ein Ring. Eine Teilmenge $R' \subseteq R$ heißt* **Unterring**, *wenn R' bezüglich $+$ eine Untergruppe ist und R' ist bezüglich $\cdot$ abgeschlossen, d.h. für alle $a, b \in R'$ ist $a \cdot b \in R'$.*

Wenn R' ein Unterring von $(R,+,\cdot)$ ist, dann ist $(R',+,\cdot)$ ein Ring.

Definition 3.6: *Seien $(R,+,\cdot)$ und $(S,+,\cdot)$ Ringe. Eine Abbildung $\varphi: R \to S$ ist ein* **Ringhomomorphismus***, falls für alle $a,b \in R$ gilt, dass $\varphi(a+b) = \varphi(a)+\varphi(b)$ und $\varphi(a\cdot b) = \varphi(a)\cdot\varphi(b)$.*

Definition 3.7: *Ein Körper ist ein kommutativer Ring mit 1 mit der Eigenschaft, dass $(R \setminus \{0\},\cdot)$ eine Gruppe bildet.*

Da $R \setminus \{0\}$ unter $\cdot$ abgeschlossen sein muss, muss ein Körper insbesondere nullteilerfrei sein.

Definition 3.8 (äquivalent zu oben): *Ein Körper ist eine Menge K zusammen mit zwei binären Verknüpfungen $+$ und $\cdot$, sodass gilt:*

(K1) *$(K,+)$ ist eine abelsche (=kommutativ) Gruppe.*

(K2) *Für alle $a,b \in K \setminus \{0\}$ ist $a \cdot b \neq 0$ und $(K \setminus \{0\},\cdot)$ bildet eine kommutative Gruppe.*

(K3) *Für alle $a,b,c \in K$ gilt $a(b+c) = ab + bc$*

Schreibweise: für $a \neq 0$ ist $a^{-1} = \frac{1}{a}$ das multiplikativ Inverse zu a. $a^{-1} \cdot b = b \cdot a^{-1} = \frac{b}{a}$.

Bemerkung 3.9: Sei K ein Körper und $a,b,x,\tilde{x} \in K$. Dann gilt:

(a) $0 \neq 1$, ein Körper hat mindestens zwei Elemente.

(b) $0 \cdot a = a \cdot 0 = 0$

(c) $a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$

(d) $a \cdot (-b) = -(a \cdot b) = (-a) \cdot b$

(e) Wenn $a \neq 0$ und $x \cdot a = \tilde{x} \cdot a$, dann gilt $x = \tilde{x}$

Satz 3.10: *$(\mathbb{C},+,\cdot)$ (mit komplexer Multiplikation) bildet einen Körper.*

Wir fassen $\mathbb{R}$ als Untergruppe von $\mathbb{C}$ auf. Vermöge der injektiven Abbildung $\mathbb{R} \to \mathbb{C}, a \mapsto (a,0)$, $(a,0)+(a',0) = (a+a',0) \Rightarrow$ Abbildung ist Ringhomomorphismus.

Definition 3.11: *$i = (0,1)$, $i^2 = -1$.*

Mit dieser Notation gilt folgendes: $(a,b) = a + b \cdot i$.

Definition 3.12 Komplexe Konjugation: *$^- : \mathbb{C} \to \mathbb{C}$ ist definiert durch $\overline{(a,b)} = (a,-b)$. Äquivalent: $\overline{a+bi} = a - bi; a,b \in \mathbb{R}$*

$\lambda \mapsto \bar{\lambda}$ für $\lambda \in \mathbb{C}$ ist Ringhomomorphismus.

Definition 3.13 Betrag Komplexer Zahlen: *$|\cdot| : \mathbb{C} \to \mathbb{R}_{\geq 0}$ ist definiert durch $|(a,b)| = \sqrt{a^2+b^2}$, $|\lambda| = \sqrt{\lambda\bar{\lambda}}$. Eigenschaften: $|\lambda\mu| = |\lambda| \cdot |\mu|$, $|\lambda+\mu| \leq |\lambda| + |\mu|$*

Lemma 3.14: *Sei R endlicher nullteilerfreier, kommutativer Ring mit 1 und $1 \neq 0$. Dann ist R ein Körper. Insbesondere ist $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ für jede Primzahl p ein Körper.*

Für einen Ring R mit 1 und $n \in \mathbb{N}$ definieren wir $n \cdot a := \underbrace{a + a + \ldots + a}_{n-mal}, a \in R$.

Definition 3.15: *Sei R ein Ring mit 1. Die Charakteristik von R ist*

$$\mathrm{char}(R) = \begin{cases} 0, & \text{falls } n \cdot 1 \neq 0 \text{ in } R \text{ für alle } n \in \mathbb{N} \\ \min\{n \in \mathbb{N} : n \cdot 1 = 0\} & \text{sonst} \end{cases}$$

Lemma 3.16: *Für jeden Körper K ist die Charakteristik 0 oder eine Primzahl.*

4 Polynome

Definition 4.1: *Sei R ein Ring mit 1. Der **Polynomring** $R[t]$ ist die Menge aller Funktionen $R[t] := \{f : \mathbb{N} \to \mathbb{R} : \text{ fast alle } f(i) = 0\} = \{f : \mathbb{N} \to \mathbb{R} : \text{ die Menge } \{j : f(j) \neq 0\} \text{ ist endlich}\}$. „fast alle“=„alle bis auf endlich viele“.*

Definition 4.2: *Wir definieren eine Addition auf $R[t]$ elementweise: $f, g \in \mathbb{R}[t]$, dann $(f + g)(i) := f(i) + g(i)$ für alle $i \in \mathbb{N}$.*

Sei $s(f) = \{j \in \mathbb{N} | f(j) \neq 0\}$, $s(g) = \{j \in \mathbb{N} | g(j) \neq 0\}$ (endlich für $f, g \in R[t]$). Dann $s(f + g) \subseteq s(f) \cup s(g)$ ist wieder eine endliche Menge.
$(R[t], +)$ ist abelsche Gruppe, sogar eine Untergruppe von $(\{f : \mathbb{N} \to \mathbb{R}\}, +)$. Neutrales Element bezüglich + ist die Nullfunktion 0, mit $0(j) = 0$ für alle $j \in \mathbb{N}$.

Definition 4.3: *Wir definieren eine Multiplikation auf $R[t]$ wie folgt: $f, g \in R[t] : (f \cdot g)(j) = \sum_{i=0}^{j} f(i) \cdot g(j - i)$ für ein $j \in \mathbb{N}$.*

Wenn f und g fast überall 0 sind, dann auch $f \cdot g$. Weiterhin ist $R[t]$ bezüglich $\cdot$ assoziativ.
Wenn R ein Ring mit 1 ist, dann ist auch $(R[t], +, \cdot)$ ein Ring mit 1; falls R kommutativ ist, dann auch $R[t]$.
Einselement: Sei $1 \in R[t]$ die Funktion mit $1(j) = \begin{cases} 1, & \text{falls } j = 0 \\ 0, & \text{sonst.} \end{cases}$ Es gilt $(1 \cdot g)(j) = g(j)$.

Definition 4.4: *Die „Unbestimmte“ ist wie folgt definiert: wir setzen $t \in R[t]$: also $t(j) = \begin{cases} 1, & \text{falls } j = 1 \\ 0, & \text{sonst.} \end{cases}$*

Für alle $f \in R[t]$ gilt $f = \sum_{n \geq 0} f(n) t^n$ in $R[t]$. $t^n := \underbrace{t \cdot t \cdot \ldots \cdot t}_{n-mal}, t^0 = 1$. Für $a \in R, f \in R[t]$ ist $(a \cdot f)(j) = a \cdot f(j); a \cdot f \in R[t]$. Weiterhin ist $(t^n)(j) = \begin{cases} 1, & \text{für } j = n \\ 0, & \text{sonst} \end{cases}$
Sei R ein Ring mit 1, dann Polynomring $R[t] = \{f_0 + f_1 t + f_2 t^2 + \ldots + f_n t^n | n \geq 0, f_0, f_1, \ldots, f_n \in R\}$. $f + g = \sum_{i=0}^{n} f_i t^i + \sum_{i=0}^{n} g_i t^i = \sum_{i=0}^{n} (f_i + g_i) t^i$. $(\sum_{i=0}^{n} f_i t^i) \cdot (\sum_{i=0}^{n} g_i t^i) = f_0 g_0 + (f_1 g_0 + f_0 g_1) t + \ldots + \left(\sum_{i=0}^{j} f_i g_{j-i} t^i\right) + \ldots$.

Definition 4.5: *Sei $f \in R[t]$ ein Polynom mit Koeffizienten in einem Ring R mit 1. Dann definiert f eine Polynomfunktion $\tilde{f} : R \to R$ definiert durch: $f = f_0 + f_1 t^1 + \ldots + f_n t^n$, dann ist $\tilde{f}(\lambda) := f_0 + f_1 \lambda + \ldots + f_n \lambda^n = \sum_{j \geq 0}^{n} f(j) \lambda^j$ für $\lambda \in R$.*

Man kann dies auffassen als eine Abbildung. $R[t] \to \text{Abb}(R, R), f \mapsto \tilde{f}$. Typischerweise ist nicht jede Funktion von R nach R von der Form $\tilde{f}$ für ein Polynom f.

Definition 4.6: *Sei $f \in R[t]$ ein Polynom. Der* **Grad** *von f ist*
$\deg(f) = \begin{cases} -\infty, & \text{falls } f = 0 \\ \max\{j : f(j) \neq 0\}, & \text{sonst.} \end{cases}$ $\deg(f_0 + f_1 t + \ldots + f_n t^n) = n$ *falls* $f_n \neq 0$.

Falls R nullteilerfrei ist (z.B. ein Körper), dann gilt: $\deg(f \cdot g) = deg(f) + deg(g)$.

Satz 4.7: *Sei K ein Körper und $f, g \in K[t]$ mit $g \neq 0$. Dann gibt es eindeutig bestimmte Polynome $q, r \in K[t]$ mit $f = q \cdot g + r$ und $\deg(r) < \deg(q)$.*

Sei K ein endlicher Körper $K = \{a_0, \ldots, a_n\}$ und $f = (t - a_0)(t - a_1) \cdot \ldots \cdot (t - a_n) + 1$ hat Grad $n + 1$ und keine Nullstelle, es gilt $f(\lambda) = 1$ für alle $\lambda \in K$.

Lemma 4.8: *Sei $\lambda \in K$ eine Nullstelle des Polynoms $f \in K[t]$. Dann gibt es ein eindeutig bestimmtes Polynom $g \in K[t]$ mit $f = (t - \lambda) \cdot g$ und* $\deg(g) = \deg(f) - 1$.

Korollar 4.9: *Sei $f \in K[t]$ ein Polynom mit $f \neq 0$ vom Grad n. Dann hat f höchstens n verschiedene Nullstellen.*

Korollar 4.10: *Für jeden unendlichen Körper K ist die Abbildung $K[t] \to \mathrm{Abb}(K, K), f \mapsto \tilde{f}$ injektiv.*

Definition 4.11: *Sei K ein Körper, $0 \neq f \in K[t]$ und $\lambda \in K$. Die* **Vielfachheit (Multiplizität)** *von λ in f ist $\mu(f; \lambda) = \max\{r \in \mathbb{N} : f = (t - \lambda)^r \cdot g$ für ein $g \in K[t]\}$.*

Bemerkung 4.12: Also $f(\lambda) = 0 \Leftrightarrow \mu(f, \lambda) \geq 1$. Wenn $f = (t - \lambda)^r \cdot g$ und $r = \mu(f; \lambda)$, dann ist $g(\lambda) \neq 0$. $\mu(f; \lambda)$ gibt an „wie oft“ $(t - \lambda)$ in f enthalten ist. Für $K = \mathbb{R}, \mathbb{C}$ (also für $\mathrm{char}(K) = 0$) ist $\mu(f; \lambda) = \max\{r \in \mathbb{N} : f(\lambda) = f'(\lambda) = \ldots = f^{(r-1)}(\lambda) = 0\}$. Für $f = a_0 + a_1 t + \ldots + a_n t^n$ definiere $f' = a_1 + 2a_2 t + 3a_3 t^2 + \ldots + n a_n t^{n-1}$.

Bemerkung 4.13: Sind $\lambda_1, \ldots, \lambda_k \in K$ die paarweise verschiedene Nullstellen eines Polynoms $f \in K[t]$ mit Vielfachheiten $r_i = \mu(f; \lambda_i)$, dann gilt $f = (t - \lambda_1)^{r_1}(t - \lambda_2)^{r_2} \cdot \ldots \cdot (t - \lambda_k)^{r_k} \cdot g$ für ein Polynom g ohne Nullstelle.

Ein Körper, über den jedes Polynom vom Grad mindestens 1 eine Nullstelle hat, heißt **algebraisch abgeschlossen**. Endliche Körper sind nicht algebraisch abgeschlossen. $\mathbb{R}$ ist nicht algebraisch abgeschlossen ($f = t^2 - 1$ hat keine Nullstellen in $\mathbb{R}$)

Satz 4.14 Fundamentalsatz der Algebra: *$\mathbb{C}$ ist algebraisch abgeschlossen, d.h. sei $f \in \mathbb{C}[t]$ mit* $\deg(f) \geq 1$, *dann hat f mindestens eine Nullstelle.*

Korollar 4.15: *Sei K ein algebraisch abgeschlossener Körper (z.B. $K = \mathbb{C}$) und $f \in K[t]$ ein Polynom mit* $\deg(f) \geq 1$. *Dann zerfällt f vollständig in Linearfaktoren, d.h. es gibt $a, \lambda_1, \lambda_2, \ldots, \lambda_n \in K$ mit $f = a(t - \lambda_1)(t - \lambda_2) \cdot \ldots \cdot (t - \lambda_n), n = \deg(f)$.*

Lemma 4.16: *Sei $f \in \mathbb{R}[t]$ und sei $\lambda \in \mathbb{C}$ eine komplexe Nullstelle von f. Dann ist auch die komplexe konjugierte Zahl $\bar{\lambda}$ eine Nullstelle von f und es gilt sogar $\mu(f; \lambda) = \mu(f; \bar{\lambda})$. Mit anderen Worten: die komplexen Nullstellen eines reellen Polynoms liegen symmetrisch zur reellen Achse.*

Satz 4.17: *Jedes Polynom $f \in \mathbb{R}[t]$ hat eine Darstellung $f = a \cdot (t - \lambda_1) \cdot \ldots \cdot (t - \lambda_k) \cdot g_{k+1} \cdot g_{k+3} \cdot \ldots \cdot g_{n-1}$, wobei $\lambda_1, \ldots, \lambda_k \in \mathbb{R}$ und $g_{k+1}, \ldots, g_{n-1} \in \mathbb{R}[t]$ quadratisch und haben keine reellen Nullstellen.*

Korollar 4.18: *Jedes Polynom $f \in \mathbb{R}[t]$ von ungeradem Grad hat eine reelle Nullstelle.*

Für Polynome ersten bis vierten Grades lassen sich Formeln ihrer Nullstellen angeben, für Polynome höheren Grades ist das im Allgemeinen nicht mehr möglich.
Wenn der Koeffizient höchstens Grades eines Polynoms 1 ist, so lässt es sich aus seinen Nullstellen eindeutig konstruieren.

Satz 4.19 Vieta: *Für* $f = t^n + a_{n-1}t^{n-1} + \ldots + a_0 = (t-\lambda_1)(t-\lambda_2)\cdot\ldots\cdot(t-\lambda_n)$ *gilt* $a_k = (-1)^{n-k}S_{n-k}(\lambda_1,\ldots,\lambda_2)$, *wobei* $S_k(\lambda_1,\ldots,\lambda_n) = \sum_{1\le i_1\le i_2\le\ldots\le i_k\le n}\lambda_{i_1}\lambda_{i_2}\ldots\lambda_{i_k}$.

Satz 4.20: *Angenommen* $f = t^n + a_{n-1}t^{n-1} + \ldots + a_0$, *erfülle* $a_0 \neq 0$ *und habe* n *reelle Nullstellen. Dann*

(a) $\lambda_1,\ldots,\lambda_n < 0 \Leftrightarrow a_0,\ldots,a_{n-1} > 0$,

(b) $\lambda_1,\ldots,\lambda_n > 0 \Leftrightarrow (-1)^{n-j}a_j > 0$ *für* $j = 0,\ldots,n-1$.

$f_- = t^n - a_{n-1}t^{n-1} + a_{n-2}t^{n-2} + \ldots + (-1)^n a_0$.
Notation: Sei $f = t^n + a_{n-1}t^{n-1} + \ldots + a_0 \in \mathbb{R}[t]$. Dann sei $N_+(f)$ = Anzahl der positiven Nullstellen, $N_-(f)$ = Anzahl der negativen Nullstellen und $Z(f)$ = Anzahl der Vorzeichenwechsel der Koeffizienten in f.

Satz 4.21 Vorzeichenregel von Descartes: *Sei* $f = t^n + a_{n-1}t^{n-1} + \ldots + a_0 \in \mathbb{R}[t]$ *mit* $a_o \neq 0$. *Dann* $N_+ \le Z(f)$ *und* $N_-(f) \le Z(f_-)$

5 Vektorräume

Definition 5.1: *Sei* K *ein Körper. Ein* **K-Vektorraum** *ist ein Tripel* $(V,+,\cdot)$ *bestehend aus einer Menge* V, *einer Verknüpfung* $+ : V\times V \to V$ *und einer Verknüpfung* $\cdot : K\times V \to V$, *sodass gilt:*

(V1) $(V,+)$ *bildet eine abelsche Gruppe.*

(V2) *Für alle* $\lambda,\mu \in K$, $v,w \in V$ *gelten*
$(\lambda+\mu)\cdot v = \lambda\cdot v + \mu\cdot v$, $\lambda\cdot(v+w) = \lambda\cdot v + \lambda\cdot w$, $\lambda\cdot(\mu\cdot v) = (\lambda\cdot\mu)\cdot v$, $1\cdot v = v$.

Beispiel 5.2: a) „Standardvektorraum“ K^n für $n = 1,2,3,\ldots$ mit komponentenweiser Addition sowie gewohnter Multiplikation mit einem Skalar.

b) Die Menge $M(m\times n, K)$ aller $m\times n$-Matrizen $A = (a_{ij})_{i=1,\ldots,m,\ j=1,\ldots,n}$ mit $a_{ij} \in K$ bildet Vektorraum mit Matrixaddition und Multiplikation mit einem Skalar.

c) $\mathbb{C}$ ist ein $\mathbb{R}$-Vektorraum vermöge $\lambda \in \mathbb{R}, (a,b) = a+bi \in \mathbb{C}$, $\lambda(a+bi) = \lambda a + (\lambda b)i$
Allgemeiner: Sei L ein Ring mit 1 und $K \subseteq$ ein Teilring (mit 1), der ein Körper ist. Dann wird L ein K-Vektorraum vermöge der eingeschränkten Addition und Multiplikation in L.

d) Der Polynomring $K[t]$ ist ein K-Vektorraum vermöge der Addition in $K[t]$ und der Skalarmultiplikation definiert als $\lambda(a_0+a_1t^1+\ldots+a_nt^n) = (\lambda a_0)t_0+(\lambda a_1)t^1+\ldots+(\lambda a_n)t^n; \lambda_i a_i \in K$

e) Sei M eine Menge. Die Menge Abb$((M,K)$ aller Abbildungen $f : M \to K$ bildet einen K-Vektorraum vermöge: $f,g \in$Abb$(M,K), \lambda \in K$ $(f+g)(m) = f(m)+g(m)$ für alle $m \in M$ und $(\lambda\cdot f)(m) = \lambda\cdot f(m)$.

Bemerkung 5.3: In jedem K-Vektorraum V gelten folgende Regeln für alle $\lambda \in K, v \in V$:

a) $0\cdot v = 0$

b) $\lambda\cdot 0 = 0$

c) $\lambda \cdot v = 0$, dann gilt $v = 0$ oder $\lambda = 0$

d) $(-1) \cdot v = -v$

Definition 5.4: *Sei V ein K-Vektorraum und $W \subseteq V$ eine Teilmenge. W heißt* **Untervektorraum***, falls gilt:*

UV1 *W ist nicht leer.*

UV2 *abgeschlossen bezüglich Addition: für alle $v, w \in W$ ist $v + w \in W$.*

UV3 *abgeschlossen bezüglich Skalarmultiplikation: für alle $\lambda \in K, w \in W$ ist $\lambda \cdot W \in W$.*

Satz 5.5: *Sei $W \subseteq V$ ein Untervektorraum. Dann ist W selbst ein Vektorraum (mit den eingeschränkten Verknüpfungen $+$ und $\cdot$)*

Lemma 5.6: *Sei V ein Vektorraum, I eine Menge und $(W_i)_{i \in I}$ eine Familie von Untervektorräumen von V. Dann ist der Durchschnitt $W = \bigcap_{i \in I} W_i = \{w \in V : \text{für alle } i \in I \text{ gilt } w \in W_i\}$ wieder ein Untervektorraum von V.*

Lemma 5.7: *Seien W, W' Untervektorräume eines K-Vektorraums V. Falls $W \cup W'$ auch ein Untervektorraum ist, dann gilt $W \subseteq W'$ oder $W' \subseteq W$.*

6 Erzeugendensystem, Lineare Unabhängigkeit, Basis und Dimension

Definition 6.1: *Sei V ein K-Vektorraum und $(v_i)_{i \in I}$ eine Familie von Vektoren aus V. Ein $v \in V$ heißt Linearkombination von $(v_i)i \in I$, falls es endlich viele $i_1, \ldots, i_r \in I$ und Skalare $\lambda_1, \ldots, \lambda_r \in K$ gibt, mit $v = \lambda_1 v_{i_1} + \lambda_2 v_{i_2} + \ldots + \lambda_r v_{i_r}$. Der* **Span** *der Familie $(v_i)_{i \in I}$ ist die Menge aller Linearkombinationen, die man so erhält.*
$\text{span}(v_i)_{i \in I} = \text{span}_K(v_i)_{i \in I} = \{v \in V : v \text{ ist Linearkombination von } (v_i)_{i \in I}\}$.

Für den Spezialfall $I = \{1, \ldots, n\}$ ist $\text{span}(v_i)_{i \in \{1,\ldots,n\}} = \text{span}(v_1, \ldots, v_n) = \{\lambda_1 v_1 + \ldots + \lambda_n v_n : \lambda_1, \ldots, \lambda_n \in K\} = Kv_1 + Kv_2 + \ldots + Kv_n$

Lemma 6.2: *Sei V ein K-Vektorraum und $(v_i)_{i \in I}$ eine Familie von Elementen aus V. Dann gilt:*

a) $\text{span}(v_i)_{i \in I}$ *ist ein Untervektorraum von V*

b) *Sei W ein Untervektorraum von V mit $v_i \in W$ für alle $i \in I$. Dann gilt* $\text{span}(v_i)_{i \in I} \subseteq W$.

Sei $M \subseteq V$ eine Teilmenge. Wir fassen M als eine M-indizierte Familie auf. Und setzen $\text{span}(M) = \text{span}(m)_{m \in M} = \{v \in V : \text{es gibt } m_1, \ldots, m_r \in M, \lambda_1, \ldots, \lambda_r \in K \text{ mit } v = \lambda_1 m_1 + \ldots + \lambda_r m_r\}$. $M \subseteq \text{span}(M) \subseteq V$ und $\text{span}(M)$ ist der kleinste Untervektorraum von V, der die Menge M enthält.

Definition 6.3: *Sei $V = K^n$ K-Vektorraum. Für $1 \leq i \leq n$ definieren wir $e_i \in K^n$ als $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ (1 an der i-ten Stelle, sonst Null).*

Für $\lambda_1, \lambda_2, \ldots, \lambda_n \in K$ gilt $(\lambda_1, \ldots, \lambda_n) = (\lambda_1, 0, \ldots, 0) + (0, \lambda_2, 0, \ldots, 0) + \ldots + (0, \ldots, 0, \lambda_n) = \lambda_1 e_1 + \lambda_2 e_2 + \ldots + \lambda_n e_n$. Also gilt $\text{span}(e_i)_{i=1,\ldots,n} = K^n$. $K[t] = \text{span}(t^n)_{n \in \mathbb{N} \cup 0}$
Sei $\bar{V} = \text{Abb}(\mathbb{N}, K)$ mit elementweiser K-Vektorraumstruktur. Dann ist $K[t]$ ein Untervektorraum von $\text{Abb}(\mathbb{N}, K)$.
Es ist immer $0 \in \text{span}(v_i)_{i \in I}$. Für jede endliche Teilmenge $i_1, \ldots, i_r$ gibt es immer die **triviale Linearkombination** $0 = 0 \cdot v_{i_1} + 0 \cdot v_{i_2} + \ldots + 0 \cdot v_{i_r}$.

Definition 6.4: *Sei V ein K-Vektorraum und $(v_1, \ldots, v_r)$ eine Familie aus Vektoren aus V. $(v_1, \ldots, v_r)$ heißt* **linear unabhängig**, *wenn für alle $\lambda_1, \ldots, \lambda_r \in K$ mit $0 = \lambda_1 v_1 + \ldots + \lambda_r v_r$ gilt $\lambda_1 = \lambda_2 = \ldots = \lambda_r = 0$. Eine beliebige Familie $(v_i)_{i \in I}$ von Vektoren aus V heißt linear unabhängig, wenn jede endliche Teilfamilie linear unabhängig ist, d.h. für jede endliche Teilmenge $J = \{i_1, \ldots, i_r : i_j \neq i_{j'} \text{ für } j \neq j'\} \subseteq I$.*

Lemma 6.5: *Sei $(v_i)_{i \in I}$ eine Familie von Vektoren eines K-Vektorraums V. Dann sind äquivalent:*

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

(ii) *Jeder Vektor $v \in \text{span}(v_i)_{i_I}$ lässt sich auf genau eine Weise als Linearkombination der v_i schreiben.*

Bemerkung 6.6:

- Ein einzelner Vektor $v \in V$ ist genau dann linear unabhängig, wenn $v \neq 0$.
- Ist $v_i = 0$ für ein $i \in I$, dann ist $(v_i)_{i \in I}$ linear abhängig.
- Ist $v_i = v_j$ für ein $i \neq j \in I$, so ist $(v_i)_{i \in I}$ linear abhängig.
- Sei $r \geq 2, (v_1, \ldots, v_r)$ ist genau dann linear abhängig, wenn einer der Vektoren eine Linearkombination der anderen ist.

Definition 6.7: *Eine Familie $\mathcal{B} = (v_i)_{i \in I}$ von Vektoren aus einem K-Vektorraum V heißt* **Basis von V**, *falls $\mathcal{B}$* **Erzeugendensystem** *von V ist, d.h. $V = \text{span}(v_i)$ und $\mathcal{B}$ linear unabhängig ist. V heißt* **endlich erzeugt**, *falls V ein endliches Erzeugendensystem hat.*

Satz 6.8: *Sei $\mathcal{B} = (v_1, \ldots, v_r)$ eine Familie von Vektoren aus V. $V \neq \{0\}$. Dann sind äquivalent:*

- *$\mathcal{B} = (v_1, \ldots, v_r)$ ist eine Basis, d.h. linear unabhängiges Erzeugendensystem.*
- *$\mathcal{B}$ ist ein* **unverkürzbares Erzeugendensystem**, *d.h. für alle $j \in \{1, \ldots, r\}$ ist $(v_1, \ldots, v_{j-1}, v_{j+1}, .$ kein Erzeugendensystem.*
- *Zu jedem $v \in V$ gibt es eindeutig bestimmte $\lambda_1, \ldots, \lambda_r \in K$ mit $v = \lambda_1 v_1 + \ldots + \lambda_r v_r$.*
- *$\mathcal{B}$ ist* **unverlängerbar linear unabhängig**, *d.h. für alle $v \in V$ ist $(v_1, \ldots, v_r, v)$ linear abhängig.*

Bemerkung 6.9: Sie V ein K-Vektorraum, der nicht endlich erzeugt ist. Dann gibt es in V eine unendlich linear unabhängige Familie.

Korollar 6.10: *Jeder endlich erzeugte Vektorraum besitzt eine Basis.*

Satz 6.11: *Jeder Vektorraum hat eine Basis.*

Lemma 6.12 Austauschlemma: *Sei V ein K-Vektorraum mit Basis $\mathcal{B} = (v_1, \ldots, v_r)$ und $w = \lambda_1 v_1 + \ldots + \lambda_r v_r$ mit $\lambda_1, \ldots, \lambda_r \in K$. Wenn für ein $j \in \{1, \ldots, r\}$ gilt, dass $\lambda_j \neq 0$, dann ist $\mathcal{B}' = (v_1, \ldots, v_{j-1}, w, v_{j+1}, \ldots, v_r)$ auch eine Basis.*

Satz 6.13 Austauschsatz: *Sei $\mathcal{B} = (v_1, \ldots, v_r)$ eine Basis des K-Vektorraums V und $(w_1, \ldots, w_n)$ eine linear unabhängige Familie. Dann gilt $n \leq r$ und es gibt paarweise verschiedene Indizes $i_1, \ldots, i_n \in \{1, \ldots, r\}$, sodass nach Ersetzen von v_{i_j} durch w_j eine neue Basis von V entsteht. Nach Umordnung können wir also annehmen, dass $i_1 = 1, i_2 = 2, \ldots, i_n = n$ und die neues Basis damit $(w_1, \ldots, w_n, v_{n-1}, \ldots, v_r)$ ist.*

Korollar 6.14: *Hat ein K-Vektorraum eine endliche Basis, dann ist jede Basis endlich.*

Korollar 6.15: *Je zwei endliche Basen eines Vektorraums haben gleich viele Elemente.*

Definition 6.16: *Sei V ein K-Vektorraum. Die* **Dimension** *von V ist definiert als* $\dim_K(V) = \dim(V) = \begin{cases} r, & \text{falls } V \text{ eine endliche Basis mit } r \text{ Elementen hat,} \\ \infty, & \text{falls } V \text{ nicht endlich erzeugt ist.} \end{cases}$

Sei M eine Menge. Dann gilt $\dim_K(\mathrm{Abb}(M, K)) = \begin{cases} |M|, & \text{falls } M \text{ endlich ist,} \\ \infty, & \text{falls } M \text{ unendlich ist.} \end{cases}$

Korollar 6.17: *Ist $W \subseteq V$ ein Untervektorraum eines endlich erzeugten K-Vektorraums V, dann ist auch W endlich erzeugt. Außerdem gilt* $\dim(W) \leq \dim(V)$. *Falls* $\dim(W) = \dim(V)$, *dann gilt schon $W = V$.*

Satz 6.18 Basisergänzungssatz: *Sei $(w_1, \ldots, w_n)$ eine linear unabhängige Familie in einem endlich erzeugten K-Vektorraum V. Dann gibt es Vektoren $w_{n+1}, \ldots, w_r$, sodass $\mathcal{B} = (w_1, \ldots, w_n, w_{n+1}, \ldots, w_r)$ eine Basis von V ist.*

Bemerkung 6.19: Da $\mathrm{span}(a_1, \ldots, a_n)$ ein Untervektorraum von K^n ist, ist dieser span endlichdimensional und $\dim(\mathrm{span}(a_1, \ldots, a_n)) \leq \dim(K^n) = n$.

Betrachte die Vektoren $a_1, \ldots, a_m$ und die $m \times n$-Matrix

$$A = (a_{ij}) = (a_i)_j = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i1} & a_{i2} & \ldots & a_{in} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix} \begin{matrix} \leftarrow a_1 \\ \vdots \\ \leftarrow a_i \\ \vdots \\ \leftarrow a_m \end{matrix}$$

Elementare Zeilenumformungen für $m \times n$-Matrizen über

I Multiplikation der i-ten Zeile mit $\lambda \in K \backslash \{0\}$

$$A = \begin{pmatrix} \vdots \\ a_i \\ \vdots \end{pmatrix} \mapsto \begin{pmatrix} \vdots \\ \lambda a_i \\ \vdots \end{pmatrix}$$

II Addition der j-ten Zeile zur i-ten Zeile ($i \neq j$)

$$A = \begin{pmatrix} \vdots \\ a_i \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \mapsto \begin{pmatrix} \vdots \\ a_i + a_j \\ \vdots \\ a_j \\ \vdots \end{pmatrix}$$

III Addition des λ-fachen der j-ten Zeile zur i-ten Zeile ($\lambda \in K \setminus \{0\}, i \neq j$)

$$A = \begin{pmatrix} \vdots \\ a_i \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \mapsto \begin{pmatrix} \vdots \\ a_i + \lambda a_j \\ \vdots \\ a_j \\ \vdots \end{pmatrix}$$ Kombination von I und II

IV Vertauschen der i-ten und j-ten Ziele ($i \neq j$)

$$A = \begin{pmatrix} \vdots \\ a_i \\ \vdots \\ a_j \\ \vdots \end{pmatrix} \mapsto \begin{pmatrix} \vdots \\ a_j \\ \vdots \\ a_i \\ \vdots \end{pmatrix}$$ Kombination von I und II

Definition 6.20: *Der Zeilenraum* $\mathrm{ZR}(A)$ *von* $A \in M(m \times n, K)$ *ist der Untervektorraum* $\mathrm{span}(a_1 \ldots, a_m) \subseteq K^n$*, der von den Zeilen* $a_1, \ldots, a_m$ *der Matrix erzeugt wird.*

Lemma 6.21: *Die Matrix* B *entstehe aus* A *durch endlich viele elementare Zeilenumformungen. Dann gilt* $\mathrm{ZR}(B) = \mathrm{ZR}(A)$.

Satz 6.22: *Jede Matrix in* $M(m \times n, K)$ *kann durch endlich viele elementare Zeilenumformungen auf Zeilenstufenform gebracht werden.*

Sei B eine Matrix in Zeilenstufenform. Dann sind $b_1, \ldots, b_r$ linear unabhängig. $\mathrm{ZR}(B) = \mathrm{span}(b_1, \ldots, b_m) = \mathrm{span}(b_1, \ldots, b_r)$. $(b_1, \ldots, b_r)$ ist eine Basis von $\mathrm{ZR}(B)$.

Transposition

Sei $A \in M(m \times n, K)$. Die **transponierte Matrix** ${}^tA \in M(n \times m, K)$ erhält man durch Spiegeln an der Diagonalen / Vertauschen von Zeilen und Spalten. Formal: Wenn $A = (a_{ij})_{i=1,\ldots,m;j=1,\ldots,n}$, dann ist ${}^tA = (a'_{ij})_i = 1, \ldots, n; j = 1, \ldots, m$ mit $a'_{ij} = a_{ji}$.
Eigenschaften: $A, B \in M(m \times n, K), \lambda \in K$ ${}^t(A + B) = {}^tA + {}^tB$, ${}^t(\lambda A) = \lambda\, {}^tA$, ${}^t({}^t(A)) = A$.
Also ist Transposition ${}^t : M(m \times n, K) \to M(n \times m, K)$ bijektiv.
Der **Spaltenraum** einer Matrix $A \in M(m \times n, K)$ ist der Raum $\mathrm{SR}(A) = \mathrm{span}(n$ Spalten von $A) = \mathrm{span}(a^1, \ldots, a^n) \subseteq K^m$. $A = (a^1, \ldots, a^m)$.
$\mathrm{ZR}(A) \subseteq K^n$, $\mathrm{SR}(A) \subseteq K^m$, $\mathrm{SR}(A) = \mathrm{ZR}({}^tA)$, $\mathrm{ZR}(A) = \mathrm{SR}({}^tA)$.

Satz 6.23: *Für alle* $A \in M(m \times n, K)$ *gilt* **Zeilenrang** $= \dim(\mathrm{ZR}(A)) = \dim(\mathrm{SR}(A)) =$ **Spaltenrang**.

7 Summen von Untervektorräumen

Definition 7.1: *Sei* V *ein* K*-Vektorraum mit Untervektorräumen* $W_1, \ldots, W_r$ $(r \geq 2)$*. Die Summe ist definiert als:* $W_1 + \ldots + W_r = \{v \in V :$ *es gibt* $w_1 \in W_1, \ldots, w_r \in W_r$ *mit* $v = w_1 + \ldots + w_r\}$

Bemerkung 7.2: Es gilt:

a) $W_1 + \ldots + W_r$ ist ein Untervektorraum von V.

b) $W_1 + \ldots + W_r = \mathrm{span}(W_1 \cup W_2 \cup \ldots \cup W_r)$.

c) $\dim(W_1 + \ldots + W_r) \leq \dim(W_1) + \ldots + \dim(W_r)$.

Satz 7.3 Dimensionsformel für Summen: *Seien W_1 und W_2 Untervektorräume eines Vektorraums V, W_1 und W_2 endlichdimensional. Dann gilt* $\dim(W_1+W_2) = \dim(W_1)+\dim(W_2)-\dim(W_1 \cap W_2)$.

Lemma 7.4: *Sei $V = W_1 + W_2$ endlich erzeugter K-Vektorraum. Dann sind äquivalent:*

(i) $W_1 \cap W_2 = \{0\}$

(ii) *Für jedes $v \in V$ gibt es eindeutig bestimmte $w_1 \in W_1$ und $w_2 \in W_2$ mit $v = w_1 + w_2$.*

(iii) *Sei $w_1 \in W_1 \setminus \{0\}$ und $w_2 \in W \setminus \{0\}$, dann ist (w_1, w_2) linear unabhängig.*

(iv) $\dim(V) = \dim(W_1) + \dim(W_2)$.

Definition 7.5: *Seien W_1, W_2 Untervektorräume des K-Vektorraums V. V heißte* **direkte Summe** *von W_1 und W_2, falls gilt $V = W_1 + W_2$ und $W_1 \cap W_2 = \{0\}$. Notation $V = W_1 + \oplus W_2$.*

Satz 7.6: *Seien W_1, W_2 Untervektorräume von V (V endlichdimensional). Dann sind äquivalent:*

(i) $V = W_1 \oplus W_2$

(ii) *Es gibt Basen $(w_1, \ldots, w_k)$ von W_1 und $(w'_1, \ldots, w'_l)$ von W_2, sodass $(w_1, \ldots, w_k, w'_1, \ldots, w'_l)$ eine Basis von V ist.*

(iii) $V = W_1 + W_2$ *und* $\dim(V) = \dim(W_1) + \dim(W_2)$

Korollar 7.7: *Sei V endlichdimensionaler Vektorraum und $W \subseteq V$ ein Untervektorraum. Dann gibt es einen Untervektorraum W' von V mit $V = W \oplus W'$.*

Definition 7.8: *Seien $W_1, \ldots, W_r$ Untervektorräume von V. V heißt die* **direkte Summe** *der W_i; $V = W_1 \oplus W_2 \oplus \ldots \oplus W_r = \bigoplus_{i=1}^{r} W_i$, falls*

DS1 $V = W_1 + \ldots + W_r$

DS2 *$w_1 \in W_1, w_2 \in W_2, \ldots, w_r \in W_r$ von 0 verschiedene Vektoren. Dann ist $(w_1, \ldots, w_r)$ linear unabhängig.*

Satz 7.9: *Seien $W_1, \ldots, W_k$ Untervektorräume eines endlichdimensionalen Vektorraums V. Dann sind äquivalent:*

(i) $V = W_1 \oplus \ldots \oplus W_k$

(ii) *Sei für jedes $i = 1, \ldots, k$ eine Basis $\mathcal{B}^{(i)} = (v_1^{(i)}, \ldots, v_{r_i}^{(i)})$ von W_i gegeben, so ist $\mathcal{B} := (v_1^{(1)}, \ldots, v_{r_1}^{(1)}, \ldots, v_1^{(k)}, \ldots, v_{r_k}^{(k)})$ eine Basis von V.*

(iii) $V = W_1 + \ldots + W_k$ *und* $\dim(V) = \dim(W_1) + \ldots + \dim(W_k)$.

8 Lineare Abbildungen

Definition 8.1: *Eine Abbildung $F : V \to W$ zwischen K-Vektorräumen heißt* **linear** *(oder* **Vektorraumhomomorphismus***), wenn gilt:*

(i) *für alle $v, v' \in V$ gilt $F(v + v') = F(v) + F(v')$*

(ii) *für alle $\lambda \in K$ und $v \in V$ gilt $F(\lambda v) = \lambda F(v)$*

Äquivalent: für alle $v, v' in V$ und $\mu, \lambda \in K$ gilt $F(\lambda v + \mu v') = \lambda F(v) + \mu(F(v')$.
i) *alleine besagt, dass $F : (V, +) \to (W, +)$ ein Gruppenhomomorphismus ist.*

Bemerkung 8.2: Für jede lineare Abbildung $F : V \to W$ gilt:

- $F(0) = 0$
- $F(v - w) = F(v) - F(w)$
- $F(\lambda_1 v_1 + \ldots + \lambda_r v_r) = \lambda_1 F(v_1) + \ldots + \lambda_r F(v_r)$ für alle $\lambda_1, \ldots, \lambda_r \in K$ und $v_1, \ldots, v_r \in V$

Drehmatrix A für Drehung (im mathematisch positiven Sinne) eines Vektors $x \in \mathbb{R}^2$ um Winkel ϑ im $\mathbb{R}^2$ um den Ursprung: $x \mapsto A \cdot x$, $A = \begin{pmatrix} \cos(\vartheta) & -\sin\vartheta \\ \sin\vartheta & \cos\vartheta \end{pmatrix}$
Sei K ein beliebiger Körper und $A \in M(m \times n, K)$. Multiplikation von Matrix mit Vektor ist eine lineare Abbildung $A \cdot - : K^n \to K^m$ definiert durch $A = (a_{ij})_{i=1,\ldots,m;j=1,\ldots,n}, x = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}$,
dann ist $A \cdot x = \begin{pmatrix} a_{11}x_1 + \ldots + a_{1n}x_n \\ \vdots \\ a_{i1}x_1 + \ldots + a_{in}x_n \\ \vdots \\ a_{m1}x_1 + \ldots + a_{mn}x_n \end{pmatrix}$. Es gilt $A \cdot (x + y) = Ax + Ay$, $A(\lambda x) = \lambda(Ax)$ für $x, y \in K^n, \lambda \in K$.
Umgekehrt ist jede Abbildung, die linear ist, $F : K^n \to K^m$ gegeben durch Multiplikation mit einer eindeutig bestimmten Matrix A. $A \cdot e_j = j$-te Spalte von A. Die Spalten von A sind die Bilder der Vektoren $e_1, \ldots, e_n$ unter der linearen Abbildung $A \cdot - : K^n \to K^m$. Zu jeder linearen Abbildung $F : K^n \to K^m$ kann es also höchstens eine Matrix A geben mit $F(x) = A \cdot x$ für alle $x \in K^n$. Zu F bilden wir also die Matrix $A := (F(e_1), F(e_2), \ldots, F(e_n)) \in M(m \times n, K)$.
Abbildung $M(m \times n, K) \to \mathrm{Hom}_K(K^n, K^m)$, $A \mapsto A \cdot -$ ist bijektiv.
Transposition ist lineare Abbildung.
Ist $(v_i)_{i \in I}$ eine linear abhängige Familie von V, so ist $(F(v_i))_{i \in I}$ linear abhängig in W.
Sind $V' \subseteq V$ und $W' \subseteq W$ Untervektorräume, dann sind auch $F(V') = \{F(v) : v \in V'\}$ und $F^{-1}(W') = \{v \in V : F(v) \in W'\}$ wieder Untervektorräume.
$\dim F(v) \leq \dim V$
Falls F bijektiv ist, dann ist auch $F^{-1} : W \to V$ linear.

Bemerkung 8.3: Seien U, V und W K-Vektorräume und $G : U \to V$ und $F : V \to W$ linear, dann ist auch $F \circ G : U \to W$ linear.

Für einen Vektorraum V sei $\mathrm{Hom}_K(V, W) \subseteq \mathrm{Abb}(V, W)$ die Menge aller K-Vektorraumhomomorphismen.

Bemerkung 8.4: $\mathrm{Hom}_K(V,W)$ ist ein Untervektorraum von $\mathrm{Abb}(V,W)$.
Spezialfall: $V = W \to \mathrm{End}_K(V) = \mathrm{Hom}_K(V,V)$ ist die Menge der Endomorphismen von V. Dies ist eine Abelsche Gruppe unter $+$, und hat die binäre Abbildung $\circ : \mathrm{End}_K(V) \times \mathrm{End}_K(V) \to \mathrm{End}_K(V)$.

Proposition 8.5: *Für jeden K-Vektorraum V ist die Menge* $\mathrm{End}_K(V)$ *ein Ring mit* 1 *bzgl.* $+$ *und* $\circ$. *Falls* $\dim_K(V) > 1$, *dann ist* $\mathrm{End}_K(V)$ *nicht kommutativ.*

Bemerkung 8.6: Die Menge $M(n \times n, K)$ aller quadratischen $n \times n$-Matrizen ist ein Ring mit 1 bzgl. $+$ und $\cdot$. Einselement: Einheitsmatrix E_n.

Satz 8.7: *Für jeden Körper K und alle* $n \geq 1$ *ist die Abbildung* $M(n \times n, K) \to \mathrm{End}_K(K^n, K^n)$ $A \mapsto (A \cdot -, K^n \to K^n)$ *mit* $A \mapsto A \cdot x$ *ein Isomorphismus von Ringen.*

Definition 8.8: *Sei* $F : V \to W$ *eine lineare Abbildung zwischen K-Vektorräumen. Sei* $w \in W$. *Dann heißt* $\mathrm{Im}(F) = F(V) = \{F(v) : v \in V\}$ *das* **Bild** *von F.* $F^{-1}(w) = \{v \in V : F(v) = w\}$ *die* **Faser** *über w.* $\mathrm{Ker}(F) = F^{-1}(0) = \{v \in V : F(v) = 0\}$ *der* **Kern** *von F.*

Bemerkung 8.9: *a)* $\mathrm{Im}(F)$ und $\mathrm{Ker}(F)$ sind Untervektorräume von W bzw. V

b) F ist surjektiv $\Leftrightarrow \mathrm{Im}(F) = W$

c) F ist injektiv $\Leftrightarrow \mathrm{Ker}(F) = \{0\}$

d) Ist F injektiv und $(v_1, \ldots, v_n)$ linear unabhängig in V, dann ist $(F(v_1), \ldots, F(v_n))$ linear unabhängig in W.

Definition 8.10: *Sei* $A \in M(m \times n, K)$ *eine* $m \times n$*-Matrix und* $F = A \cdot - : K^n \to K^m$ *die zugehörige lineare Abbildung mit* $F(x) = Ax$. *Der* **Rang** *von A ist definiert als* $\mathrm{Rang}(A) = \dim(\mathrm{Im}(F)) = \dim(\mathrm{Im}(A \cdot -))$.

„Fasern $F^{-1}(w)$ sind parallel verschobene Kopien von $\mathrm{Ker}(F)$“

Bemerkung 8.11: Sei $F : V \to W$ linear und $w \in \mathrm{Im}(F)$. Dann ist für alle $u \in V$ mit $F(u) = w$ $F^{-1}(w) = u + \mathrm{Ker}(F) = \{u + v : v \in \mathrm{Ker}(F)\}$.

Definition 8.12: *Eine Teilmenge X eines K-Vektorraums V heißt* **affiner Untervektorraum**, *falls es ein* $v \in V$ *und einen Untervektorraum W von V gibt mit* $X = v + W = \{v + w : w \in W\}$.

Bemerkung 8.13: Sei X ein affiner Untervektorraum von V. Dann ist $X - X = \{v - w : v, w \in X\}$ ein Untervektorraum und für alle $u \in X$ gilt $X = u + (X - X)$.

Definition 8.14: *Sei X ein affiner Untervektorraum von V, etwa* $X = v + W$. *Dann ist* $\dim(X) = \dim(W)$ *die* **Dimension** *von X.*

Satz 8.15: *Sei* $F : V \to W$ *linear und V endlichdimensional. Seien* $(v_1, \ldots, v_k)$ *eine Basis von* $\mathrm{Ker}(F)$ *und* $(w_1, \ldots, w_r)$ *eine Basis von* $\mathrm{Im}(F)$. *Seien* $u_1 \in F^{-1}(w_1), \ldots, u_r \in F^{-1}(w_r)$ *beliebige Vektorurbilder. Dann ist* $(v_1, \ldots, v_k, u_1, \ldots, u_r)$ *eine Basis von V. Also ist* $\dim(V) = \dim(\mathrm{Ker}(F)) + \dim(\mathrm{Im}(F))$.

Korollar 8.16: *Sei V endlichdimensionaler K-Vektorraum und* $F : V \to W$ *linear. Dann gilt für alle nicht leeren Fasern von F:* $\dim(F^{-1}(w)) = \dim(V) - \dim(\mathrm{Im}(F))$.

Korollar 8.17: *Zwischen zwei endlichdimensionalen Vektorräumen V und W gibt es genau dann einen Isomorphismus, wenn* $\dim(V) = \dim(W)$

Korollar 8.18: *Seien V und W endlichdimensionale K-Vektorräume und $F : V \to W$ linear und* $\dim(V) = \dim(W)$*. Dann sind äquivalent:*

(i) *F ist bijektiv, also ein Isomorphismus.*

(ii) *F ist injektiv.*

(iii) *F ist surjektiv.*

Satz 8.19 Faktorisierungssatz: *Sei $F : V \to W$ linear und $(u_1, \ldots, u_r, v_1, \ldots, v_k)$ Basis von V. Sei* $\operatorname{span}(v_1, \ldots, v_k) = \operatorname{Ker}(F)$*. Wir definieren* $U = \operatorname{span}(u_1, \ldots, u_r)$*. Dann gilt:*

(i) $V = \operatorname{Ker}(F) \oplus U$*.*

(ii) *Die Einschränkung von F auf U ist ein Isomorphismus* $F_{|U} : U \to \operatorname{Im}(F)$*.*

(iii) *Sei $P : V = U \oplus \operatorname{Ker}(F) \to U$ die Projektion auf den ersten Summanden, d.h. für $v = u + v', u \in U, v' \in \operatorname{Ker}(F)$ ist $P(v) = u$. Dann gilt $F = (F_{|U}) \circ P$ Insgesamt kann F also geschrieben werden als folgende Komposition:*

$$V \xrightarrow{P} U \xrightarrow[F_{|U}]{\cong} \operatorname{Im}(F) \hookrightarrow W \qquad (V \xrightarrow{F} W)$$

(iv) *Jede nicht-leere Faser von F schneidet U in genau einem Element. Es gilt* $F^{-1}(F(v)) \cap U = \{P(v)\}$ *für alle $v \in V$.*