Lineare Algebra WS2017/18 + SS2018

Dozent: Prof. Dr. Arno Fehm

4. August 2018

Kapitel I

Grundbegriffe der Linearen Algebra

1. Logik und Mengen

Definition 1.1 (Teilmenge)
Sind X und Y zwei Mengen, so heißt X eine Teilmenge von Y, wenn jedes Element von X auch Element von Y ist, dass heißt wenn für alle x $(x \in X \Rightarrow x \in Y)$ gilt.

Definition 1.2 (Mengenoperationen)
Seien X und Y Mengen. Man definiert daraus weitere Mengen wie folgt (Mengenoperationen):

- $X \cup Y := \{x \mid x \in X \vee x \in Y\}$
- $X \cap Y := \{x \mid x \in X \wedge x \in Y\}$
- $X \backslash Y := \{x \in X \mid x \notin Y\}$
- $X \times Y := \{(x, y) \mid x \in X \wedge y \in Y\}$
- $\mathcal{P}(X) := \{Y \mid Y \subset X\}$

2. Abbildungen

Definition 2.1 (Einschränkung)
Sei $f : x \mapsto y$ eine Abbildung. Für $A \subset X$ definiert man die Einschränkung /Restrikton von f auf A als die Abbildung

$$f|_A : \begin{cases} A \to Y \\ a \mapsto f(a) \end{cases}$$

Das Bild von A unter f ist $f(A) := \{f(a) : a \in A\}$.
Das Urbild einer Menge $B \subset Y$ unter f ist $f^{-1} := \{x \in X : f(x) \in B\}$.
Man nennt $\mathrm{Im}(f) := f(X)$ das Bild von f.

Definition 2.2 (Komposition)
Sind $f : X \to Y$ und $g : Y \to Z$ Abbildungen, so ist die Komposition $g \circ f$ die Abbildung

$$g \circ f := \begin{cases} X \to Z \\ x \mapsto f(g(x)) \end{cases}$$

Man kann die Komposition auffassen als eine Abbildung $\circ : \mathrm{Abb}(Y, Z) \times \mathrm{Abb}(X, Y) \to \mathrm{Abb}(X, Z)$.

Definition 2.3 (Umkehrabbildung)
Ist $f : X \to Y$ bijektiv, so gibt es zu jedem $y \in Y$ genau ein $x_y \in X$ mit $f(x_y) = y$ (??), durch

$$f^{-1} : \begin{cases} Y \to X \\ y \mapsto x_y \end{cases}$$

wird also eine Abbildung definiert, die Umkehrabbildung zu f.

Definition 2.4 (Familie)
Seien I und X Mengen. Eine Abbildung $x : I \to X, i \mapsto x_i$ nennt man Familie von Elementen von X mit einer Indexmenge I (oder I-Tupel von Elementen von X) und schreibt diese auch als $(x_i)_{i \in I}$. Im Fall $I = \{1, 2, ..., n\}$ identifiziert man die I-Tupel auch mit den n-Tupeln aus Definition 1.1. Ist $(x_i)_{i \in I}$ eine Familie von Teilmengen einer Menge X, so ist

- $\bigcup X_i = \{x \in X \mid \exists i \in I(x \in X)\}$
- $\bigcap X_i = \{x \in X \mid \forall i \in I(x \in X)\}$
- $\prod X_i = \{f \in \text{Abb}(I, X) \mid \forall i \in I(f(i) \in X_i)\}$

Die Elemente von $\prod X_i$ schreibt man in der Regel als Familien $(x_i)_{i \in I}$.

Definition 2.5 (Graph)
Der Graph einer Abbildung $f : X \to Y$ ist die Menge

$$\Gamma f : \{(x, y) \in X \times Y \mid y = f(x)\}$$

3. Gruppen

Definition 3.1 ((Halb-)Gruppe)
Sei G eine Menge. Eine (innere, zweistellige) Verknüpfung auf G ist eine Abbildung $* : G \times G \to G, (x, y) \mapsto x * y$. Das Paar $(G, *)$ ist eine Halbgruppe , wenn das folgende Axiom erfüllt ist:

- (G1) Für $x, y, z \in G$ ist $(x * y) * z = x * (y * z)$.

Eine Halbgruppe $(G, *)$ ist ein Monoid , wenn zusätzlich das folgende Axiom gilt:

- (G2) Es gibt ein Element $e \in G$, welches für alle $x \in G$ die Gleichung $x * e = e * x = x$ erfüllt. Dieses Element heißt dann neutrales Element der Verknüpfung $*$.

Satz 3.2 (Eindeutigkeit des neutralen Elements)
Ein Monoid $(G, *)$ hat genau ein neutrales Element.

Beweis. Nach Definition besitzt $(G, *)$ mindestens ein neutrales Element. Seien $e_1, e_2 \in G$ neutrale Elemente. Dann ist $e_1 = e_1 * e_2 = e_2$. Damit besitzt $(G, *)$ höchstens ein neutrales Element, also genau ein neutrales Element. □

Definition 3.3 ((abelsche) Gruppe)
Eine Gruppe ist ein Monoid $(G, *)$ mit dem neutralen Element e, in dem zusätzlich das folgende Axiom gilt:

- (G3) Für jedes $x \in G$ gibt es ein $x' \in G$ mit $x' * x = x * x' = e$.

Gilt weiterhin

- (G4) Für alle $x, y \in G$ gilt $x * y = y * x$, so heißt diese Gruppe abelsch .

Satz 3.4 (Eindeutigkeit des Inversen)
Ist $(G, *)$ eine Gruppe, so hat jedes $x \in G$ genau ein inverses Element.

Beweis. Nach Definition hat jedes $x \in G$ mindestens ein Inverses. Seien $x', x'' \in G$ inverse Elemente zu x. Dann ist $x' = x' * e = x' * (x * x'') = (x' * x) * x'' = e * x'' = x''$. Es gibt also genau ein Inverses zu x. □

Definition 3.5 (Untergruppe)
Eine Untergruppe einer Gruppe $(G, \cdot)$ ist eine nichtleere Teilmenge $H \subset G$, für die gilt:

- (UG1) Für alle $x, y \in H$ ist $x \cdot y \in H$ (Abgeschlossenheit unter Multiplikation).
- (UG2) Für alle $x \in H$ ist $x^{-1} \in H$ (Abgeschlossenheit unter Inversen).

Definition 3.6 (erzeugte Untergruppe)
Ist G eine Gruppe und $X \subseteq G$, so nennt man diese kleinste Untergruppe von G, die X enthält, die von X erzeugte Untergruppe von G und bezeichnet diese mit $\langle X \rangle$, falls $X = \{x_1, x_2, ..., x_n\}$ enthält auch mit $\langle x_1, x_2, ..., x_n \rangle$. Gibt es eine endliche Menge $X \subset G$ mit $G = \langle X \rangle$, so nennt man G endlich erzeugt.

4. Ringe

Definition 4.1 (Ring)
Ein Ring ist ein Tripel $(R, +, \cdot)$ bestehend aus einer Menge R, einer Verknüpfung $+ : R \times R \to R$ (Addition) und einer anderen Verknüpfung $\cdot : R \times R \to R$ (Multiplikation), sodass diese zusammen die folgenden Axiome erfüllen:

- (R1) $(R, +)$ ist eine abelsche Gruppe.
- (R2) $(R, \cdot)$ ist eine Halbgruppe.
- (R3) Für $a, x, y \in R$ gelten die Distributivgesetze $a(x+y) = ax + ay$ und $(x+y)a = xa + ya$.

Ein Ring heißt kommutativ, wenn $xy = yx$ für alle $x, y \in R$.
Ein neutrales Element der Multiplikation heißt Einselement von R.
Ein Unterring eines Rings $(R, +, \cdot)$ ist eine Teilmenge, die mit der geeigneten Einschränkung von Addition und Multiplikation wieder ein Ring ist.

Theorem 4.2
Sei $b \neq 0 \in \mathbb{Z}$. Für jedes $a \in \mathbb{Z}$ gibt es eindeutig bestimmte $q, r \in \mathbb{Z}$ (r ist "Rest"), mit $a = qb + r$ und $0 \leq r < |b|$.

Beweis. Existenz und Eindeutigkeit

- Existenz: oBdA nehmen wir an, dass $b > 0$ (denn ist $a = qb + r$, so ist auch $a = (-q)(-b) + r$). Sei $q \in \mathbb{Z}$ die größte Zahl mit $q \leq \frac{a}{b}$, und sei $r = a - qb \in \mathbb{Z}$. Dann ist $a \leq \frac{a}{b} - q < 1$, woraus $0 \leq r < b$ folgt.
- Eindeutigkeit: Sei $a = qb + r = q'b + r'$ mit $q, q', r, r' \in \mathbb{Z}$ und $0 \leq r, r' < |b|$. Dann ist $(q - q')b = r - r'$ und $|r - r'| < |b|$. Da $q - q' \in \mathbb{Z}$ ist, folgt $r - r' = 0$ und daraus wegen $b \neq 0$, dann $q - q' = 0$. □

■ **Beispiel 4.3 (Restklassenring)**
Wir fixieren $n \in \mathbb{N}$. Für $a \in \mathbb{Z}$ sei $\overline{a} := a + n\mathbb{Z} := \{a + nx \mid x \in \mathbb{Z}\}$ die Restklasse von "a mod n".
Für $a, a' \in \mathbb{Z}$ sind äquivalent:

- $a + n\mathbb{Z} = a' + n\mathbb{Z}$
- $a' \in a + n\mathbb{Z}$
- n teilt $a' - a$ (in Zeichen $n|a' - a$), d.h. $a' = a + nk$ für $k \in \mathbb{Z}$

Beweis.
- 1) $\Rightarrow$ 2): klar, denn $0 \in \mathbb{Z}$
- 2) $\Rightarrow$ 3): $a' \in a + n\mathbb{Z} \Rightarrow a' = a + nk$ mit $k \in \mathbb{Z}$
- 3) $\Rightarrow$ 1): $a' = a + nk$ mit $k \in \mathbb{Z} \Rightarrow a + n\mathbb{Z} = \{a + nk + nx \mid x \in \mathbb{Z}\} = \{a + n(k + x) \mid x \in \mathbb{Z}\} = a + n\mathbb{Z}$

Insbesondere besteht $a + n\mathbb{Z}$ nur aus den ganzen Zahlen, die bei der Division durch n den selben Rest lassen wie a. □

Definition 4.4 (Charakteristik)
Sei R ein Ring mit Einselement. Man definiert die Charakteristik von R als die kleinste natürliche Zahl n mit $1 + 1 + ... + 1 = 0$, falls so ein n existiert, andernfalls ist die Charakteristik 0.

Definition 4.5 (Nullteiler)
Sei R ein Ring mit Einselement. Ein $0 \neq x \in R$ ist ein Nullteiler von R, wenn er ein $0 \neq y \in R$ mit $xy = 0$ oder $yx = 0$ gibt. Ein Ring ohne Nullteiler ist nullteilerfrei.

Definition 4.6 (Einheit)
Sei R ein Ring mit Einselement. Ein $x \in R$ heißt invertierbar (oder Einheit von R), wenn es ein $x' \in R$ mit $xx' = x'x = 1$ gibt. Wir bezeichnen die invertierten Elemente von R mit $R^\times$.

5. Körper

Definition 5.1 (Körper)
Ein Körper ist ein kommutativer Ring $(K, +, \cdot)$ mit Einselement $1 \neq 0$, in dem jedes Element $x \neq x \in K$ invertierbar ist.

Definition 5.2 (Teilkörper)
Ein Teilkörper eines Körpers $(K, +, \cdot)$ ist die Teilemenge $L \subset K$, die mit der geeigneten Einschränkung von Addition und Multiplikation wieder ein Körper ist.

■ **Beispiel 5.3 (Endliche Primkörper)**
Für jede Primzahl p ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper. Ist $\overline{a} \neq \overline{0}$, so gilt p teilt nicht a und somit gibt es nach ?? $b, k \in \mathbb{Z}$ mit

$$\begin{gathered} ab + kp = 1 \\ \overline{(ab + kp)} = \overline{1} = \overline{(ab)} = \overline{a} \cdot \overline{b} \end{gathered}$$

und somit ist $\overline{a}$ invertierbar in $\mathbb{Z}/p\mathbb{Z}$. Somit sind für $n \in \mathbb{N}$ äquivalent:

- $\mathbb{Z}/n\mathbb{Z}$ ist ein Körper
- $\mathbb{Z}/n\mathbb{Z}$ ist nullteilerfrei
- n ist Primzahl

Beweis.
- $1 \Rightarrow 2$: ??
- $2 \Rightarrow 3$: ??
- $3 \Rightarrow 1$: gegeben

Insbesondere ist $\mathbb{Z}/p\mathbb{Z}$ nullteilerfrei, d.h. aus $p|ab$ folgt $p|a$ oder $p|b$. □

6. Polynome

In diesem Abschnitt sei R ein kommutativer Ring mit Einselement.

Definition 6.1 (Polynom)
Sei $R[X]$ die Menge der Folgen in R (siehe ??), die fast überall 0 sind, also

$$R[X] := \{(a_k)_{k \in \mathbb{N}_0} \mid \forall k (a_k \in R) \land \exists n_0 : \forall k > n_0 (a_k = 0)\}$$

Wir definieren Addition und Multiplikation auf $R[X]$:

- $(a_k)_{k \in \mathbb{N}_0} + (b_k)_{k \in \mathbb{N}_0} = (a_k + b_k)_{k \in \mathbb{N}_0}$
- $(a_k)_{k \in \mathbb{N}_0} \cdot (b_k)_{k \in \mathbb{N}_0} = (c_k)_{k \in \mathbb{N}_0}$ mit $c_k = \sum_{j=0}^{k} a_j b_{k-j}$

Theorem 6.2 (Polynomdivision)
Sei K ein Körper und sei $0 \neq g \in K[X]$. Für jedes Polynom $f \in K[X]$ gibt es eindeutig bestimmte $g, h, r \in K[X]$ mit $f = gh + r$ und $\deg(r) < \deg(g)$.

Beweis. Existenz und Eindeutigkeit

- Existenz: Sei $n = \deg(f)$, $m = \deg(g)$, $f = \sum_{k=0}^{n} a_k X^k$, $g = \sum_{k=0}^{m} b_k X^k$
  Induktion nach n bei festem g.
  IA: Ist $n < m$, so wählt man $h = 0$ und $r = f$.
  IB: Wir nehmen an, dass die Aussage für alle Polynome vom Grad kleiner als n gilt.
  IS: Ist $n \geq m$, so betrachtet man $f_1 = f - \frac{a_n}{b_m} \cdot X^{n-m} \cdot g(X)$. Da $\frac{a_n}{b_m} \cdot X^{n-m} \cdot g(X)$ ein Polynom vom Grad $n - m + \deg(g) = n$ mit Leitkoeffizient $\frac{a_n}{b_m} \cdot b_m = a_n$ ist, ist $\deg(f_1) < n$. Nach IB gibt es also $h_1, r_1 \in K[X]$ mit $f_1 = gh_1 + r_1$ und $\deg(r) < \deg(g)$. Somit ist $f(X) = f_1(X) + \frac{a_n}{b_m} \cdot X^{n-m} \cdot g(X) = gh + r$ mit $h(X) = h_1(X) + \frac{a_n}{b_m} \cdot X^{n-m}, r = r_1$.
- Eindeutigkeit: Sei $n = \deg(f), m = \deg(g)$. Ist $f = gh + r = gh' + r'$ und $\deg(r), \deg(r') < m$, so ist $(h - h')g = r' - r$ und $\deg(r' - r) < m$. Da $\deg(h - h') = \deg(h' - h) + m$ muss $\deg(h - h') < 0$, also $h' - h = 0$ sein. Somit $h' = h$ und $r' = r$. □

Definition 6.3 (Nullstelle)
Sei $f(X) = \sum_{k \geq 0} a_k X^k \in \mathbb{R}[X]$. Für $\lambda \in \mathbb{R}$ definiert man die Auswertung von f in λ $f(\lambda) = \sum_{k \geq 0} a_k \lambda^k \in \mathbb{R}$. Das Polynom f liefert auf diese Weise eine Abbildung $\tilde{f} : \mathbb{R} \to \mathbb{R}$ und $\lambda \mapsto f(\lambda)$. Ein $\lambda \in \mathbb{R}$ $f(\lambda) = 0$ ist eine Nullstelle von f.

Definition 6.4 (algebraisch abgeschlossen)
Ein Körper K heißt algebraisch abgeschlossen , wenn er eine der äquivalenten Bedingungen erfüllt.

Theorem 6.5 (Fundamentalsatz der Algebra)
Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen.

Kapitel II

Vektorräume

1. Definition und Beispiele

In diesem Kapitel sei K ein Körper.

Definition 1.1 (Vektorraum)
Ein K-Vektorraum (auch Vektorraum über K) ist ein Tripel $(V, +, \cdot)$ bestehend aus einer Menge V, einer Verknüpfung $+ : V \times V \to V$, genannt Addition, und einer Abbildung $\cdot : K \times V \to V$, genannt Skalarmultiplikation, für die gelten:

- (V1): $(V, +)$ ist eine abelsche Gruppe
- (V2): Addition und Skalarmultiplikation sind verträglich:
  - $\lambda(x + y) = (\lambda \cdot x) + (\lambda \cdot y)$
  - $(\lambda + \mu) \cdot x = (\lambda \cdot x) + (\mu \cdot x)$
  - $\lambda(\mu \cdot x) = (\lambda \cdot \mu) \cdot x$
  - $1 \cdot x = x$

Definition 1.2 (Untervektorraum)
Sei V ein K-Vektorraum. Ein Untervektorraum (Untervektorraum) von V ist eine nichtleere Teilmenge $W \subseteq V$ mit:

- (UV1): Für $x, y \in W$ ist $x + y \in W$.
- (UV2): Für $x \in W$ und $\lambda \in K$ ist $\lambda \cdot x \in W$.

Definition 1.3 (Erzeugendensystem)
Ist V ein K-Vektorraum und $X \subseteq V$, so nennt man den kleinsten Untervektorraum von V, der X enthält den von X erzeugten Untervektorraum von V und bezeichnet diesen mit $\langle X \rangle$. Eine Mengen $X \subseteq V$ mit $\langle X \rangle = V$ heißt Erzeugendensystem von V. Der Vektorraum V heißt endlich erzeugt, wenn er ein endliches Erzeugendensystem besitzt.

2. Linearkombinationen

Sei V ein K-Vektorraum.

Definition 2.1 (Linearkombination)

- Sei $n \in \mathbb{N}_0$. Ein $x \in V$ ist eine Linearkombination eines n-Tupels $(x_1, ..., x_n)$ von Elementen von V, wenn es $\lambda_1, ..., \lambda_n \in K$ gibt mit $x = \lambda_1 \cdot x_1, ..., \lambda_n \cdot x_n$. Der Nullvektor ist stets eine Linearkombination von $(x_1, ..., x_n)$ auch wenn $n = 0$.
- Ein $x \in V$ ist eine Linearkombination einer Familie (x_i) von Elementen von V, wenn es $n \in \mathbb{N}_0$ und $i_1, ..., i_n \in I$ gibt, für die x Linearkombination von $(x \cdot i_1, ..., x \cdot i_n)$ ist.
- Die Menge aller $x \in V$, die Linearkombination von $\mathcal{F} = (x_i)$ sind, wird mit $\text{span}_K(\mathcal{F})$ bezeichnet.

Definition 2.2 (linear (un)abhängig)

- Sei $n \in \mathbb{N}_0$. Ein n-Tupel $(x_1, ..., x_n)$ von Elementen von V ist linear abhängig , wenn es $\lambda_1, ..., \lambda_n \in K$ gibt, die nicht alle 0 sind und $\lambda_1 \cdot x_1 + ... + \lambda_n \cdot x_n = 0$ (*) erfüllen. Andernfalls heißt das Tupel linear unabhängig .
- Eine Familie (x_i) von Elementen von V ist linear abhängig, wenn es $n \in \mathbb{N}_0$ und paarweise verschiedene $i_1, ..., i_n \in I$ gibt, für die $(x_{i_1}, ..., x_{i_n})$ linear abhängig ist. Andernfalls linear unabhängig.

3. Basis und Dimension

Definition 3.1 (Basis)
Eine Familie (x_i) von Elementen von V ist eine Basis von V, wenn gilt:

- (B1): Die Familie ist linear unabhängig.
- (B2): Die Familie erzeugt V, also $\text{span}_K(x_i) = V$.

Theorem 3.2 (Basisauswahlsatz)
Jedes endliche Erzeugendensystem von V besitzt eine Basis als Teilfamilie: Ist (x_i) ein endliches Erzeugendensystem von V, so gibt es eine Teilmenge $J \subseteq I$, für die $(x_i)_{i \in J}$ eine Basis von V ist.

Beweis. Sei (x_i) ein endliches Erzeugendensystem von V. Definiere $\mathcal{J} := \{J \subseteq I \mid (x_i)_{i\in J}$ J ist Erzeugendensystem von $V\}$. Da I endlich ist, ist auch $\mathcal{J}$ endlich. Da (x_i) Erzeugendensystem ist, ist $I \in J$, insbesondere $\mathcal{J} \neq \emptyset$. Es gibt deshalb ein bezüglich Inklusion minimales $J_0 \in \mathcal{J}$, d.h. $J_1 \in \mathcal{J}$ so gilt nicht $J_1 \subsetneq J_0$. Deshalb ist $(x_i)_{i\in J_0}$ eine Basis von V (??). □

Lemma 3.3 (Austauschlemma)
Sei $B = (x_1, ..., x_n)$ eine Basis von V. Sind $\lambda_1, ..., \lambda_n \in K$ und $y = \sum_{i=1}^n \lambda_i \cdot x_i$, so ist für jedes $j \in \{1, 2, ..., n\}$ mit $\lambda_j \neq 0$ auch $B' = (x_1, ..., x_{j-1}, y, x_{j+1}, ..., x_n)$ eine Basis von V.

Beweis. oBdA. sei $j = 1$, also $B' = (y, x_2, ..., x_n)$. Wegen $\lambda_1 \neq 0$ ist $x_1 = \lambda_1^{-1} \cdot y - \sum_{i=2}^n \lambda_i \cdot x_i \in \text{span}_K(y, x_2, ..., x_n)$ und somit ist B' ein Erzeugendensystem. Sind $\mu_1, ..., \mu_n \in K$ mit $\mu_1 \cdot y - \sum_{i=2}^n \mu_i \cdot x_i = 0$, so folgt $0 = \mu_1(\sum_{i=1}^n \lambda_i \cdot x_i + \sum_{i=2}^n \mu_i \cdot x_i) = \mu_1 \cdot \lambda_1 \cdot x_1 + \sum_{i=2}^n (\mu_1 \cdot \lambda_i + \mu_i) x_i$ und aus der linearen Unabhängigkeit von B somit $\mu_1 \cdot \lambda_1 = 0$, $\mu_1 \cdot \lambda_2 + \mu_2 = 0$, ..., $\mu_1 \cdot \lambda_n + \mu_n = 0$. Wegen $\lambda_1 \neq 0$ folgt $\mu_1 = 0$ und daraus $\mu_i = 0$. Folglich ist B' linear unabhängig. □

Theorem 3.4 (Steinitz'scher Austauschsatz)
Sei $B = (x_1, ..., x_n)$ eine Basis von V und $\mathcal{F} = (y_1, ..., y_r)$ eine linear unabhängige Familie in V. Dann ist $r \leq n$ und es gibt $i_1, ..., i_{n-r} \in \{1, ..., n\}$, für die $B' = (y_1, ..., y_r, x_{i_1}, ..., x_{i_{n-r}})$ eine Basis von V ist.

Beweis. Induktion nach r
Für $r = 0$ ist nichts zu zeigen.
Sei nun $r \geq 1$ und gelte die Aussage für $(y_1, ..., y_{r-1})$. Insbesondere ist $r - 1 \leq n$ und es gibt $i_1, .., i_{n-(r-1)} \in \{1, ..., n\}$ für die $B' = (y_1, ..., y_r, x_{i_1}, ..., x_{i_{n-(r-1)}})$ eine Basis von V ist. Da $y_r \in V = \text{span}_K(B')$ ist $y_r = \sum_{i=1}^{r-1} \lambda_i \cdot y_1 + \sum_{j=0}^{n-(r-1)} \mu_j \cdot x_{i_j}$. Da $(y_1, ..., y_r)$ linear unabhängig, ist $y_r \notin \text{span}_K(y_1, ..., y_{r-1})$. Folglich gibt es $j_0 \in \{1, ..., n - (r - 1)\}$ mit $\mu_{j_0} \neq 0$. Insbesondere ist $n - (r - 1) \geq 1$, also $r \leq n$. oBdA. $j_0 = 1$, dann ergibt sich mit dem Austauschlemma (Lemma 3.3), dass auch $(y_1, ..., y_{r-1}, y_r, x_{i_2}, ..., x_{i_{n-(r-1)}})$ eine Basis von V ist. □

Folgerung 3.5 (Basisergänzungssatz)
Ist V endlich erzeugt, so lässt sich jede linear unabhängige Familie zu einer Basis ergänzen: Ist

$(x_1, ..., x_n)$ linear unabhängig, so gibt es $m \geq n$ und $x_{n+1}, x_{n+2}, ..., x_m$ für die $(x_1, ..., x_n, x_{n+1}, ..., x_m)$ eine Basis von V ist.

Beweis. Nach dem Basisauswahlsatz (Theorem 3.2 und ??) besitzt V eine endliche Basis, die Behauptung folgt somit aus dem STEINITZ'schen Austauschsatz (Theorem 3.4). □

4. Summen von Vektorräumen

Sei V ein K-Vektorraum und (W_i) eine Familie von Untervektorräumen von V.

Definition 4.1 (Summe von Vektorräumen)
Die Summe der W_i ist der Untervektorraum

$$\sum_{i \in I} W_i := \operatorname{span}_K \left(\bigcup W_i \right)$$

Im Fall $I = \{1, ..., n\}$ schreibt man auch $W_1 + ... + W_n$ für $\sum_{i=1}^n W_i$.

Definition 4.2 (direkte Summe)
Ist jedes $x \in \sum W_i$ eindeutig als Summe von x_i mit $x_i \in W_i$ darstellbar, so sagt man, dass $\sum W_i$ die direkte Summe der Untervektorräume W_i ist und schreibt $\oplus W_i$ für $\sum W_i$. Im Fall $I = \{1, ..., n\}$ schreibt man auch $W_1 \oplus W_2 \oplus ... \oplus W_n$ für $\oplus W_i$.

Theorem 4.3 (Dimensionsformel)
Sei $\dim_K(V) < \infty$. Für Untervektorräume W_1, W_2 von V gilt:

$$\dim_K(W_1 + W_2) + \dim_K(W_1 \cap W_2) = \dim_K(W_1) + \dim_K(W_2)$$

Beweis. Da $\dim_K(V) < \infty$ haben alle Untervektorräume von V Basen. Sei also $B_0 = (X_1, ..., x_n)$ eine Basis von $W_1 \cap W_2$. Nach dem Basisergänzungssatz (Folgerung 3.5) können wir B_0 zu den Basen $B_1 = (x_1, ..., x_n, y_1, ..., y_p)$ von W_1 und $B_2 = (x_1, ..., x_n, z_1, ..., z_q)$ von W_2 ergänzen. Wir behaupten, dass $B = (x_1, ..., x_n, y_1, ..., y_p, z_1, ..., z_q)$ eine Basis von $W_1 + W_2$ ist. Offenbar ist B ein Erzeugendensystem von $W_1 + W_2$. Seien nun $\lambda_1, ..., \lambda_n, \mu_1, ..., \mu_p, \eta_1, ..., \eta_q \in K$ mit $\sum_{i=1}^n \lambda_i x_i + \sum_{j=1}^p \mu_j y_j + \sum_{k=1}^q \eta_k z_k = 0$. Dann ist $\sum_{i=1}^n \lambda_i x_i + \sum_{j=1}^p \mu_j y_j = -\sum_{k=1}^q \eta_k z_k \in W_1 \cap W_2$. Da $\operatorname{span}_K(B_0) = W_1 \cap W_2$ und B_1 linear unabhängig ist, ist $\mu_j = 0$. Analog zeigt man auch, dass $\eta_k = 0$. Aus B_0 linear unabhängig folgt dann auch, dass $\lambda_i = 0$. Somit ist B linear unabhängig. Wir haben gezeigt, dass B eine Basis von $W_1 + W_2$ ist.
$\Rightarrow \dim_K(W_1) + \dim_K(W_2) = |B_1| + |B_2| = (n+p) + (n-q) = (n+p+q) + n = |B| + |B_0| = \dim_K(W_1 + W_2) + \dim_K(W_1 \cap W_2)$. □

Definition 4.4 (externes Produkt)
Das externe Produkt einer Familie (V_i) von K-Vektorräumen ist der K-Vektorraum $\prod V_i$ bestehend aus dem kartesischen Produkt der V_i mit komponentenweiser Addition und Skalarmultiplikation, $(x_i) + (x_i') := (x_i + x_i')$ und $\lambda(x_i) := (\lambda x_i)$.

Definition 4.5 (externe Summe)
Die externe Summe einer Familie (V_i) von K-Vektorräumen ist der Untervektorraum $\oplus V_i := \{(x_i) \in \prod V_i \mid x_i = 0; \text{ für fast alle } i\}$ des K-Vektorraum $\prod V_i$.

Kapitel III

Lineare Abbildungen

1. Matrizen

Sei K ein Körper.

Definition 1.1 (Matrix)
Seien $m, n \in \mathbb{N}_0$. Eine $m \times n$-Matrix über K ist ein rechteckiges Schema:

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & & \dots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

Man schreibt dies auch als $A = (a_{ij})_{i=1,\dots,n\ j=1,\dots,m}$ oder $A = (a_{ij})_{i,j}$, wenn m und n aus dem Kontext hervorgehen. Die a_{ij} heißen die Koeffizienten der Matrix A und wir definieren $A_{i,j} = a_{ij}$. Die Menge der $m \times n$-Matrizen über K wird mit $\mathrm{Mat}_{m\times n}(K)$ oder $K^{m\times n}$ bezeichnet. Man nennt das Paar (m, n) auch den Typ von A. Ist $m = n$, so spricht man von quadratisch en Matrizen und schreibt $\mathrm{Mat}_n(K)$. Zu einer Matrix $A = (a_{ij}) \in \mathrm{Mat}_{m\times n}(K)$ definiert man die zu A transponierte Matrix $A^t := (a_{ij})_{j,i} \in \mathrm{Mat}_{n\times m}(K)$.

Definition 1.2 (Addition und Skalarmultiplikation)
Seien $A = (a_{ij})$ und $B = (b_{ij})$ desselben Typs und $\lambda \in K$. Man definiert auf $\mathrm{Mat}_{m\times n}(K)$ eine koeffizientenweise Addition und Skalarmultiplikation .

Definition 1.3 (Matrizenmultiplikation)
Seien $m, n, r \in \mathbb{N}_0$. Sind $A = (a_{ij}) \in \mathrm{Mat}_{m\times n}(K)$, $B = (b_{jk}) \in \mathrm{Mat}_{n\times r}(K)$ so definieren wir die Matrizenmultiplikation $C = AB$ als die Matrix $C = (c_{ik}) \in \mathrm{Mat}_{m\times r}(K)$ mit $c_{ik} = \sum_{j=1}^{n} a_{ij} \cdot b_{jk}$. Kurz geschrieben "Zeile · Spalte".

Definition 1.4 (invertierbar)
Eine Matrix $A \in \mathrm{Mat}_n(K)$ heißt invertierbar oder regulär , wenn sie im Ring $\mathrm{Mat}_n(K)$ invertierbar ist, sonst singulär . Die Gruppe $\mathrm{GL}_n(K) = \mathrm{Mat}_n(K)^\times$ der invertierbaren $n \times n$ -Matrizen heißt allgemeine Gruppe .

2. Homomorphismen von Gruppen

Seien G, H zwei multiplikativ geschriebene Gruppen.

Definition 2.1 (Gruppenhomomorphismus)
Eine Abbildung $f : G \to H$ ist ein Gruppenhomomorphismus , wenn gilt:

- (GH): $f(xy) = f(x) \cdot f(y)$

Die Menge der Homomorphismen $f : G \to H$ bezeichnet man mit $\mathrm{Hom}(G, H)$.

Definition 2.2 (Arten von Homomorphismen)
Ein Homomorphismus ist

- ein Monomorphismus , wenn f injektiv ist
- ein Epimorphismus , wenn f surjektiv ist
- ein Isomorphismus , wenn f bijektiv ist.

Die Gruppen G und H heißen isomorph , in Zeichen $G \cong H$, wenn es einen Isomorphismus $G \to H$ gibt.

Definition 2.3 (Kern)
Der Kern eines Gruppenhomomorphismus $f : G \to H$ ist $\mathrm{Ker}(f) := f^{-1}(\{1\}) = \{x \in G \mid f(x) = 1_H\}$.

Definition 2.4 (Normalteiler)
Ist $N \leq G$ mit $x^{-1}y \in N$ für alle $x \in G$ und $y \in N$, so nennt man N einen Normalteiler von G und schreibt $N \lhd G$.

3. Homomorphismen von Ringen

Seien R, S und T Ringe.

Definition 3.1 (Ringhomomorphismus)
Eine Abbildung $f : R \to S$ ist ein Ringhomomorphismus , wenn für $x, y \in R$ gilt:

- (RH1:) $f(x + y) = f(x) + f(y)$
- (RH2:) $f(xy) = f(x) \cdot f(y)$

Die Menge der Ringhomomorphismen $f : R \to R$ wird mit $\mathrm{Hom}(R, S)$ bezeichnet. Ein Homomorphismus $f : R \to S$ ist ein Mono-, Epi- oder Isomorphismus, wenn f injektiv, surjektiv oder bijektiv ist. Gibt es einen Isomorphismus $f : R \to S$, so nennt man R und S isomorph und schreibt $R \cong S$. Die Elemente von $\mathrm{End}(R) := \mathrm{Hom}(R, R)$ nennt man Endomorphismen . Der Kern eines Ringhomomorphismus $f : R \to S$ ist $\mathrm{Ker}(f) := f^{-1}(\{0\})$.

Definition 3.2 (Ideal)
Ist I eine Untergruppe von $(R, +)$ und $xa, ax \in I$ mit $x \in R$ und $a \in I$, so nennt man I ein Ideal von R und schreibt $I \trianglelefteq R$.

4. Homomorphismen von Vektorräumen

Seien U, V, W drei K-Vektorraum.

Definition 4.1 (linear)
Eine Abbildung $f : V \to W$ heißt K-linear er Homomorphismus von K-Vektorraum, wenn für alle $x, y \in V$ und $\lambda \in K$ gilt:

- (L1): $f(x + y) = f(x) + f(y)$
- (L2): $f(\lambda x) = \lambda \cdot f(x)$

Die Menge der K-linearen Abbildungen $f : V \to W$ wird mit $\mathrm{Hom}_K(V, W)$ bezeichnet. Die Elemente von $\mathrm{End}_K(V) := \mathrm{Hom}_K(V, V)$ nennt man die Endomorphismen von V. Ein $f \in \mathrm{Hom}_K(V, W)$ ist ein Mono-, Epi- bzw. Isomorphismus, falls f injektiv, surjektiv bzw. bijektiv ist. Einen Endomorphismus der auch ein Isomorphismus ist, nennt man Automorphismus von V und bezeichnet die Menge der Automorphismen von V mit $\mathrm{Aut}_K(V)$. Der Kern einer linearen Abbildung $f : V \to W$ ist $\mathrm{Ker}(f) := f^{-1}(\{0\})$.

5. Der Vektorraum der linearen Abbildungen

Seien V und W zwei K-Vektorräume.

Definition 5.1 (Koordinatensystem)
Die Abbildung Φ_B heißt Koordinatensystem zu B. Für $v \in V$ ist $(x_1, ..., x_n)^t = \Phi_B^{-1}(v) \in K^n$ der Koordinatenvektor zu v bezüglich B und $(x_1, ..., x_n)$ sind die Koordinaten von v bezüglich B.

6. Koordinatendarstellung linearer Abbildungen

Seien V, W endlichdimensionale K-Vektorräume mit den Basen $B = (x_1, ..., x_n)$ und $C = (y_1, ..., y_m)$.

Definition 6.1 (darstellende Matrix)
Sei $f \in \mathrm{Hom}_K(V, W)$. Für $j = 1, ..., n$ schreiben wir $f(x_j) = \sum_{i=1}^m a_{ij} y_i$ mit eindeutig bestimmten $a_{ij} \in K$. Die Matrix $M_C^B(f) = (a_{ij}) \in \mathrm{Mat}_{m\times n}(K)$ heißt die darstellende Matrix von f bezüglich der Basen B und C.

Definition 6.2 (Transformationsmatrix)
Sind B und B' Basen von V, so nennt man $T_{B'}^B := M_{B'}^B(\mathrm{id}_V) \in \mathrm{GL}_(K)$ die Transformationsmatrix des Basiswechsels von B nach B'.

7. Quotientenräume

Seien V, W K-Vektorräume und $U \subseteq V$ ein Untervektorraum.

Definition 7.1 (affiner Unterraum)
Ein affiner Unterraum von V ist eine Teilmenge der Form

$$x + U := \{x + u \mid u \in U\} \subseteq V$$

wobei $U \subseteq V$ ein beliebiger Untervektorraum von V ist und $x \in V$.

Definition 7.2 (Quotientenraum)
Der Quotientenraum von V modulo U ist die Menge der affinen Unterräume

$$V/U := \{x + U \mid x \in V\}$$

mit der Addition $(x_1 + U) + (x_2 + U) = (x_1 + x_2) + U$ und der Multiplikation $\lambda(x + U) = \lambda x + U$. Dies ist wohldefiniert nach ??.

Wir definieren die Abbildung $\pi_U : V \to V/U$ durch $\pi_U(x) = x + U$.

▶ **Bemerkung 7.3**
Die Untervektorraum sind also genau die Kerne linearer Abbildungen! Ist $f : V \to W$ linear, so ist $\mathrm{Ker}(f) \subseteq V$ ein Untervektorraum. Ist $U \subseteq V$ ein Untervektorraum, so ist $\pi_U : V \to V/U$ linear mit Kern U.

Theorem 7.4 (Homomorphiesatz)
Sei $f \in \mathrm{Hom}_K(V, W)$ mit $U \subseteq \mathrm{Ker}(f)$. Dann gibt es genau eine lineare Abbildung $\tilde{f} : {}^V\!/\!_U \to W$ mit $f = \tilde{f} \circ \pi_U$, d.h. es kommutiert:

$$\begin{tikzcd} V \arrow[rr, "f"] \arrow[dr, "\pi_U"'] & & W \\ & {}^V\!/\!_U \arrow[ur, dashed, "\tilde{f}"'] & \end{tikzcd}$$

Diese erfüllt $\mathrm{Ker}(\tilde{f}) = {}^{\mathrm{Ker}(f)}\!/\!_U = \{x + U \mid x \in \mathrm{Ker}(f)\} \subseteq {}^V\!/\!_U$.

Beweis. Ist $f = \tilde{f} \circ \pi_U$, so gilt $\tilde{f}(x + U) = \tilde{f}(\pi_U) = f(x)$ $(*)$, somit ist $\tilde{f}$ dann eindeutig bestimmt. Umgekehrt wird durch $(*)$ eine wohldefinierte Abbildung $\tilde{f}$ erklärt: Sind $x, x' \in V$ mit $x + U = x' + U$, so ist $x - x' \in U \subseteq \mathrm{Ker}(f)$ und deshalb $f(x) = f(x')$.

- Linearität: Für $x, y \in V$ und $\lambda \in K$ ist $\tilde{f}(\lambda(x + U) + \mu(y + U)) = \tilde{f}(\lambda\pi_U(x) + \mu\pi_U(y)) = \lambda\tilde{f}(x + U) + \mu\tilde{f}(y + U)$.
- Kern: $\tilde{f}(x + U) = 0 \iff f(x) = 0 \iff x \in \mathrm{Ker}(f)$. □

8. Rang

Seien V, W zwei endlichdimensionale K-Vektorräume und $f \in \mathrm{Hom}_K(V, W)$.

Definition 8.1 (Rang)
Der Rang von f ist $\mathrm{rk}(f) = \dim_K(\mathrm{Im}(f))$.

Definition 8.2 (Rang einer Matrix)
Der Rang einer Matrix $A \in \mathrm{Mat}_{m\times n}(K)$ ist $\mathrm{rk}(A) = \mathrm{rk}(f_A)$, wobei $f_A : K^n \to K^m$ die durch A beschriebene lineare Abbildung ist.

9. Lineare Gleichungssysteme

Sei $A \in \mathrm{Mat}_{m\times n}(K)$ und $b \in K^m$.

Definition 9.1 (Lineares Gleichungssystem)
Unter einem Linearen Gleichungssystem verstehen wir eine Gleichung der Form $Ax = b$. Diese heißt homogen , wenn $b = 0$, sonst inhomogen und $L(A, b) = \{x \in K^n \mid Ax = b\}$ ist sein Lösungsraum .

Definition 9.2 (Zeilenstufenform)
Die Matrix $A = (a_{ij})$ hat Zeilenstufenform , wenn es ganze Zahlen $0 \leq r \leq m$ und $1 \leq k_1 < ... < k_r \leq n$ gibt mit:

- für $1 \leq i \leq r$ und $1 \leq j < k_i$ ist $a_{ij} = 0$
- für $1 \leq i \leq r$ ist $a_{ik_i} \neq 0$ (sogenannte Pivotelemente)
- für $r < i \leq m$ und $1 \leq j \leq n$ ist $a_{ij} = 0$

$$\begin{pmatrix} 0 & \dots & 0 & a_{1k_1} & * & \dots & \dots & * \\ 0 & \dots & \dots & 0 & a_{2k_2} & * & \dots & * \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & \dots & \dots & \dots & \dots & \dots & a_{rk_r} \\ 0 & \dots & \dots & \dots & \dots & \dots & \dots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \dots & \dots & \dots & \dots & \dots & \dots & 0 \end{pmatrix}$$

Definition 9.3 (Elementarmatrizen)
Für $i, j \in \{1, ..., m\}$, $\lambda \in K^\times$ und $\mu \in K$ definieren wir $m \times m$-Matrizen, die sogenannten Elementarmatrizen :

- $S_i(\lambda) := \mathbb{1}_m + (\lambda - 1)E_{ii}$
- $Q_{ij}(\mu) := \mathbb{1}_m + \mu E_{ij}$
- $P_{ij} := \mathbb{1}_m + E_{ij} + E_{ji} - E_{ii} - E_{jj}$

Theorem 9.4 (Eliminierungsverfahren nach Gauß)
Zu jeder Matrix $A \in \mathrm{Mat}_{m\times n}(K)$ gibt es $l \in \mathbb{N}_0$ und Elementarmatrizen $E_1, ..., E_l$ vom Typ II und III für die $E_l \cdot ... \cdot E_1 \cdot A$ in Zeilenstufenform ist.

Beweis. Seien $a_1, ..., a_n$ die Spalten von A.
Ist $A = 0$ so ist nichts zu tun.
Sei nun $A \neq 0$ und sei k_1 minimal mit $a_{k_1} \neq 0$. Es gibt also ein i mit $a_{ik_1} \neq 0$. Durch Vertauschen der ersten und der i-ten Zeile erreichen wir, dass $a_{1k_1} = 0$, d.h. wir multiplizieren A mit $E_1 = P_{1i}$. Nun addieren wir für $i = 2, .., m$ ein geeignetes Vielfaches der ersten Zeile zur i-ten Zeile, um $a_{ik_1} = 0$, d.h. wir multiplizieren A mit $E_i = Q_{i1}(\mu_i)$ für $\mu_i = \frac{a_{ik_1}}{a_{1k_1}}$. Nach diesen Umformungen haben wir eine Matrix der Form:

$$\begin{pmatrix} 0 & \dots & 0 & a_{1k_1} & * & \dots & * \\ 0 & \dots & \dots & 0 & * & \dots & * \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & \dots & 0 & * & \dots & * \end{pmatrix}$$

und können nun mit dem Rest der Matrix $A =: A'$ von vorne beginnen. Die nun folgenden Zeilenumformungen werden die erste Zeile und die ersten k_1 Spalten nicht mehr ändern, und weil A' weniger Zeilen und Spalten als A hat, bricht das Verfahren nach endlich vielen Schritten ab. □

Kapitel IV

Determinanten

1. Das Vorzeichen einer Permutation

In diesem Kapitel sei K ein Körper und R ein kommutativer Ring mit Einselement.

Definition 1.1 (Fehlstand, Vorzeichen)
Sei $\sigma \in S_n$.

- Ein Fehlstand von σ ist ein Paar (i,j) mit $1 \leq i < j \leq n$ und $\sigma(i) > \sigma(j)$.
- Das Vorzeichen (oder Signum) von σ ist $\operatorname{sgn}(\sigma) = (-1)^{f(\sigma)} \in \{-1, 1\}$, wobei $f(\sigma)$ die Anzahl der Fehlstände von σ ist.
- Man nennt σ gerade , wenn $\operatorname{sgn}(\sigma) = 1$, sonst ungerade .

2. Determinante einer Matrix

Definition 2.1 (Determinantenabbildung)
Eine Abbildung $\delta : \operatorname{Mat}_n(R) \to R$ heißt Determinantenabbildung , wenn gilt:

- (D1): δ ist linear in jeder Zeile: sind $a_1, ..., a_n$ die Zeilen von A und ist $i \in \{1, ..., n\}$ und $a_i = \lambda' a_i' + \lambda'' a_i''$ mit $\lambda', \lambda'' \in R$ und den Zeilenvektoren a_i', a_i'', so ist $\delta(A) = \lambda' \cdot \delta(a_1, ..., a_i', ..., a_n) + \lambda'' \cdot \det(a_1, ..., a_i'', ..., a_n)$.
- (D2): δ ist alternierend: sind $a_1, ..., a_n$ die Zeilen von A und $i, j \in \{1, ..., n\}$, $i \neq j$ mit $a_i = a_j$, so ist $\delta(A) = 0$.
- (D3): δ ist normiert: $\delta(\mathbb{1}_n) = 1$.

Theorem 2.2
Es gibt genau eine Determinantenabbildung $\delta : \operatorname{Mat}_n(R) \to R$ und diese ist gegeben durch die Leibnitzformel

$$\det(a_{ij}) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \cdot \prod_{i=1}^{n} a_{i,\sigma(i)} = \sum_{\sigma \in A_n} \prod_{i=1}^{n} a_{i,\sigma(i)} - \sum_{\sigma \in S_n \setminus A_n} \prod_{i=1}^{n} a_{i,\sigma(i)}$$

Beweis. Eindeutigkeit der Abbildung folgt wegen D3 aus ??. Bleibt nur noch zu zeigen, dass det auch die Axiome D1 bis D3 erfüllt.
D1: klar
D3: klar
D2: Seien $\mu \neq v$ mit $a_\mu = a_v$. Mit $\tau = \tau_{\mu v}$ ist $S_n \setminus A_n = A_n \tau$, somit

$$\begin{aligned}\det(a_{ij}) &= \sum_{\sigma \in A_n} \prod_{i=1}^{n} a_{i,\sigma(i)} - \sum_{\sigma \in A_n \tau} \prod_{i=1}^{n} a_{i,\sigma\tau(i)} \\ &= \sum_{\sigma \in A_n} \left(\prod_{i=1}^{n} a_{i,\sigma(i)} - \prod_{i=1}^{n} a_{i,\sigma\tau(i)} \right)\end{aligned}$$

nach ??. Da $a_{ij} = a_{\tau(i),j}$ für alle i, j ist

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

für jedes $\sigma \in S_n$, woraus $\det(a_{ij}) = 0$ folgt. □

Theorem 2.3 (Determinantenmultiplikationssatz)
Für $A, B \in \mathrm{Mat}_n(R)$ ist

$$\det(AB) = \det(A) \cdot \det(B)$$

Beweis. Fixiere A und betrachte die Abbildung $\delta : \mathrm{Mat}_n(R) \to R$ mit $B \mapsto \det(AB^{-1})$. Diese Abbildung erfüllt die Axiome D1 und D2. sind $b_1, ..., b_n$ die Zeilen von B, so hat AB^{-1} die Spalten $Ab_1^t, ..., Ab_n^t$, es werden die Eigenschaften von det auf δ übertragen.
$\Rightarrow \det(AB) = \delta(B^t) = \delta(\mathbb{1}_n) \cdot \det(B^t) = \det(A) \cdot \det(B)$. □

3. Minoren

Seien $m, n \in \mathbb{N}$.

Definition 3.1 (adjungierte Matrix)
Sei $A = (a_{ij}) \in \mathrm{Mat}_n(R)$. Für $i, j \in \{1, ..., n\}$ definieren wir die $n \times n$-Matrix:

$$A_{ij} = \begin{pmatrix} a_{11} & \dots & a_{1,j-1} & 0 & a_{1,j+1} & \dots & a_{1n} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{i-1,1} & \dots & a_{i-1,j.1} & 0 & a_{i-1,j+1} & \dots & a_{i-1,n} \\ 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ a_{i+1,1} & \dots & a_{i+1,j.1} & 0 & a_{i+1,j+1} & \dots & a_{i+1,n} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{n,j-1} & 0 & a_{n,j+1} & \dots & a_{nn} \end{pmatrix}$$

die durch Ersetzen der i-ten Zeile und der j-ten Spalte durch e_j aus A hervorgeht, sowie die $(n-1) \times (n-1)$- Matrix:

$$A'_{ij} = \begin{pmatrix} a_{11} & \dots & a_{1,j-1} & a_{1,j+1} & \dots & a_{1n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{i-1,1} & \dots & a_{i-1,j.1} & a_{i-1,j+1} & \dots & a_{i-1,n} \\ a_{i+1,1} & \dots & a_{i+1,j.1} & a_{i+1,j+1} & \dots & a_{i+1,n} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{n,j-1} & a_{n,j+1} & \dots & a_{nn} \end{pmatrix}$$

die durch Streichen der i-ten Zeile und der j-ten Spalten entsteht. Weiterhin definieren wir die zu A adjungierte Matrix als $A^{\#} = (a_{ij}^{\#}) \in \mathrm{Mat}_n(R)$, wobei $a_{ij}^{\#} = \det(A_{ji})$.

Lemma 3.2
Sei $A \in \mathrm{Mat}_n(R)$ mit Spalten $a_1, ..., a_n$. Für $i, j \in \{1, .., n\}$ gilt:

- $\det(A_{ij}) = (-1)^{i+j} \cdot \det(A'_{ij})$
- $\det(A_{ij}) = \det(a_1, ..., a_{j-1}, e_i, a_{j+1}, ..., a_n)$

Beweis.
- Durch geeignete Permutation der ersten i Zeilen und der ersten j Zeilen erhält man

$$\begin{aligned}\det(A_{ij}) &= (-1)^{(i-1)+(j-1)} \cdot \det(\begin{pmatrix} 1 & 0 & ... & 0 \\ 0 & & & \\ \vdots & & A'_{ij} & \\ 0 & & & \end{pmatrix}) \\ &\overset{??}{=} (-1)^{i+j} \cdot \det(\mathbb{1}_n) \cdot \det(A'_{ij})\end{aligned}$$

- Man erhält A_{ij} aus $(a_1, ..., e_i, ..., a_n)$ durch elementare Spaltenumformungen vom Typ II. □

Satz 3.3
Für $A \in \mathrm{Mat}_n(R)$ ist

$$A^{\#} \cdot A = A \cdot A^{\#} = \det(A) \cdot \mathbb{1}_n \tag{1}$$

Beweis.

$$\begin{aligned}(A^{\#}A)_{ij} &= \sum_{k=1}^{n} a^{\#}_{ik} \cdot a_{kj} \\ &= \sum_{k=1}^{n} a_{kj} \cdot \det(A_{kj}) \\ &\overset{3.2}{=} \sum_{k=1}^{n} a_{kj} \cdot \det(a_1, ..., a_{i-1}, a_j, a_{i+1}, ..., a_n) \\ &= \det(a_1, ..., a_{i-1}, \sum_{k=1}^{n} a_{kj} e_k, a_{i+1}, ..., a_n) \\ &= \det(a_1, ..., a_{i-1}, a_j, a_{i+1}, ..., a_n) \\ &= \delta_{ij} \cdot \det(A) \\ &= (\det(A) \cdot \mathbb{1}_n)_{ij}\end{aligned}$$

Analog bestimmt man die Koeffizienten von $AA^{\#}$, wobei man $\det(A_{jk}) = \det(A^t_{jk}) = \det((A^t)_{kj})$ benutzt. □

Folgerung 3.4
Es ist $\mathrm{GL}_n(R) = \{A \in \mathrm{Mat}_n(R) \mid \det(A) \in R^{\times}\}$ und für $A \in \mathrm{GL}_n(R)$ ist $A^{-1} = \frac{1}{\det(A)} \cdot A^{\#}$.

Beweis. Satz 3.3 und ?? □

Satz 3.5 (Laplace'scher Entwicklungssatz)
Sei $A = (a_{ij}) \in \mathrm{Mat}_n(R)$. Für jedes $i, j \in \{1, .., n\}$ gilt die Formel für die Entwicklung nach der i-ten Zeile:

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} \cdot a_{ij} \cdot \det(A'_{ij})$$

Gleiches gilt auch für Spalten.

Beweis. Nach Satz 3.3 ist

$$\begin{aligned} \det(A) = (AA^{\#})_{ij} &= \sum_{j=1}^{n} a_{ij} \cdot a^{\#}_{ij} \\ &= \sum_{j=1}^{n} a_{ij} \cdot \det(A_{ij}) \\ &= \sum_{j=1}^{n} a_{ij} \cdot (-1)^{i+j} \cdot \det(A'_{ij}) \end{aligned}$$

Analog auch für Spalten. □

Satz 3.6 (Cramer'sche Regel)
Sei $A \in \mathrm{GL}_n(R)$ mit Spalten $a_1, ..., a_n$ und sei $b \in R^n$. Weiter sei $x = (x_1, ..., x_n)^t \in R^n$ die eindeutige Lösung des Linearen Gleichungssystems $Ax = b$. Dann ist für $i = 1, ..., n$

$$x_i = \frac{\det(a_1, ..., a_{i-1}, b, a_{i+1}, ..., a_n)}{\det(A)}$$

Beweis.

$$\begin{aligned} x_i &= (A^{-1}b)_i \\ &= \sum_{j=1}^{n} (A^{-1})_{ij} \cdot b_j \\ &\overset{3.4}{=} \frac{1}{\det(A)} \cdot \sum_{j=1}^{n} a^{\#}_{ij} \cdot b_j \\ &\overset{3.2}{=} \frac{1}{\det(A)} \cdot \sum_{j=1}^{n} b_j \cdot \det(a_1, ..., a_{i-1}, e_i, a_{i+1}, ..., a_n) \\ &= \frac{1}{\det(A)} \cdot \det(a_1, ..., a_{i-1}, b_j, a_{i+1}, ..., a_n) \end{aligned}$$

□

Definition 3.7 (Minor)
Sei $A = (a_{ij}) \in \mathrm{Mat}_{m\times n}(R)$ und $1 \leq r \leq m$, $1 \leq s \leq n$. Eine $r \times s$- Teilmatrix von A ist eine Matrix der Form $(a_{i\mu,jv})_{\mu,v} \in \mathrm{Mat}_{r\times s}(R)$ mit $1 \leq i_1 < ... < i_r \leq m$ und $1 \leq j_1 < ... < j_s \leq n$. Ist A' eine $r \times r$-Teilmatrix von A, so bezeichnet man $\det(A')$ als einen r-Minor von A.

■ **Beispiel 3.8**
Ist $A \in \mathrm{Mat}_n(R)$ und $i, j \in \{1, ..., n\}$, so ist A'_{ij} eine Teilmatrix und $\det(A'_{ij}) = (-1)^{i+j} \cdot a^{\#}_{ji}$ ein $(n-1)$-Minor von A.

Satz 3.9
Sei $A \in \mathrm{Mat}_n(R)$ und $r \in \mathbb{N}$. Genau dann ist $\mathrm{rk}(A) \geq r$, wenn es eine $r \times r$- Teilmatrix A' von A mit $\det(A') \neq 0$ gibt.

Beweis.
- Hinrichtung: Ist $\mathrm{rk}(A) \geq r$, so hat A r linear unabhängige Spalten $a_1, ..., a_r$. Die Matrix $\tilde{A} = (a_1, ..., a_r)$ hat den Rang r und deshalb r linear unabhängige Zeilen $\widetilde{a_1}, ..., \widetilde{a_r}$. Die $r \times r$-Matrix A hat dann Rang r, ist also invertierbar, und $\det(A) \neq 0$.
- Rückrichtung: Ist A' eine $r \times r$-Teilmatrix von A mit $\det(A') \neq 0$, so ist $\mathrm{rk}(A) \geq \mathrm{rk}(A') = r$. □

Folgerung 3.10
Sei $A \in \mathrm{Mat}_{m \times n}(K)$. Der Rang von A ist das größte $r \in \mathbb{N}$, für das A einen von Null verschiedenen r-Minor hat.

4. Determinante und Spur von Endomorphismen

Sei $n \in \mathbb{N}$ und V ein K-Vektorraum mit $\dim_K(V) = m$.

Satz 4.1
Sei $f \in \mathrm{Hom}_K(V, W)$, A' eine Basis von V und $A = M_{A'}(f)$. Sei weiter $B \in \mathrm{Mat}_n(K)$. Genau dann gibt es eine Basis B' von V mit $B = M_{B'}(f)$, wenn es $S \in \mathrm{GL}_n(K)$ mit $B = SAS^{-1}$ gibt.

Beweis. Ist B' eine Basis von V mit $B = M_{B'}(f)$, so ist $B = SAS^{-1}$ mit $S = T_{B'}^{A'}$. Sei umgekehrt $B = SAS^{-1}$ mit $S \in \mathrm{GL}_n(K)$. Es gibt eine Basis B' von V mit $T_{B'}^{A'} = S$, also $M_{B'}(f) = T_{B'}^{A'} \cdot M_{A'}(f) \cdot (T_{B'}^{A'})^{-1} = SAS^{-1} = B$: Mit $B' = (\Phi_{A'}(f_s^{-1}(e_1)), ..., \Phi_{A'}(f_s^{-1}(e_n)))$ ist $\Phi_{A'} \circ f_s^{-1} = \mathrm{id}_V \circ \Phi_{B'}$, also $T_{B'}^{A'} = M_{A'}^{A'}(\mathrm{id}_V) = S^{-1}$. Folglich ist $T_{B'}^{A'} = (T_{A'}^{B'})^{-1} = (S^{-1})^{-1} = S$ nach ??. □

Definition 4.2 (Ähnlichkeit)
Zwei Matrizen $A, B \in \mathrm{Mat}_n(R)$ heißen <u>ähnlich</u> , wenn (in Zeichen $A \sim B$) es $S \in \mathrm{GL}_n(R)$ mit $B = SAS^{-1}$ gibt.

Satz 4.3
Ähnlichkeit von Matrizen ist eine Äquivalenzrelation auf $\mathrm{Mat}_n(R)$.

Beweis.
- Reflexivität: $A = \mathbb{1}_n \cdot A \cdot (\mathbb{1}_n)^{-1}$
- Symmetrie: $B = SAS^{-1} \Rightarrow A = S^{-1}BS = S^{-1}B(S^{-1})^{-1}$
- Transitivität: $B = SAS^{-1}$, $C = TBT^{-1} \Rightarrow C = TSAS^{-1}T^{-1} = (TS)A(ST)^{-1}$ □

Satz 4.4
Seien $A, B \in \mathrm{Mat}_n(R)$. Ist $A \sim B$, so ist

$$\det(A) = \det(B)$$

Beweis. $B = SAS^{-1}$, $S \in \mathrm{GL}_n(R)$, $\det(B) = \det(S) \cdot \det(A) \cdot \det(S)^{-1} = \det(A)$ nach Theorem 2.3 und ?? □

Definition 4.5 (Determinante eines Endomorphismus)
Die <u>Determinante</u> eines Endomorphismus $f \in \mathrm{End}_K(V)$ ist

$$\det(f) = \det(M_B(f))$$

wobei B eine Basis von V ist. (Diese ist wohldefiniert nach Satz 4.1 und Satz 4.4)

Satz 4.6
Für $f, g \in \mathrm{End}_K(V)$ gilt:

- $\det(\mathrm{id}_V) = 1$
- $\det(f \circ g) = \det(f) \cdot \det(g)$
- Genau dann ist $\det(f) \neq 0$, wenn $f \in \mathrm{Aut}_K(V)$. In diesem Fall ist $\det(f^{-1}) = \det(f)^{-1}$

Beweis.
- klar
- folgt aus ?? und Theorem 2.3
- folgt aus ?? und ?? □

Definition 4.7 (Spur einer Matrix)
Die Spur einer Matrix $A = (a_{ij}) \in \mathrm{Mat}_n(R)$ ist

$$\mathrm{tr}(A) = \sum_{i=1}^{n} a_{ii}$$

Mathematica/WolframAlpha-Befehle (Spur einer Matrix)
Auch für die Spur einer Matrix hat Mathematica bzw. WolframAlpha eine Funktion:

```
Tr[{{1, 2, 3}, {4, 5, 6}, {7, 8, 9}}]
```

Lemma 4.8
Seien $A, B \in \mathrm{Mat}_n(R)$

- $\mathrm{tr} : \mathrm{Mat}_n(R) \to R$ ist R-linear
- $\mathrm{tr}(A^t) = \mathrm{tr}(A)$
- $\mathrm{tr}(AB) = \mathrm{tr}(BA)$

Beweis. in den Übungen bereits behandelt □

Satz 4.9
Seien $A, B \in \mathrm{Mat}_n(R)$. Ist $A \sim B$, so ist $\mathrm{tr}(A) = \mathrm{tr}(B)$.

Beweis. $B = SAS^{-1}$, $S \in \mathrm{GL}_n(R) \Rightarrow \mathrm{tr}(B) = \mathrm{tr}(SAS^{-1}) \overset{4.8}{=} \mathrm{tr}(AS^{-1}S) = \mathrm{tr}(A)$ □

Definition 4.10 (Spur eines Endomorphismus)
Die Spur eines Endomorphismus $f \in \mathrm{End}_K(V)$ ist

$$\mathrm{tr}(f) = \mathrm{tr}(M_B(f))$$

wobei B eine Basis von V ist (Diese ist wohldefiniert nach Satz 4.1 und Satz 4.9)

▶ **Bemerkung 4.11**
Im Fall $K = \mathbb{R}$ kann man wie in ?? den Absolutbetrag der Determinante eines $f \in \mathrm{End}_K(K^n)$ geometrisch interpretieren, nämlich als das Volumen von $f(Q)$, wobei $Q = [0,1]^n$ der Einheitsquader ist, und somit als Volumenänderung durch f. Auch das Vorzeichen von $\det(f)$ hat eine Bedeutung: Es gibt an, ob f orientierungserhaltend ist. Für erste Interpretationen der Spur siehe A100.

Kapitel V
Endomorphismen

1. Eigenwerte

Definition 1.1 (Eigenwert, Eigenvektor, Eigenraum)
Sind $0 \neq x \in V$ und $\lambda \in K$ mit $f(x) = \lambda x$ so nennt man λ einen Eigenwert von f und x einen Eigenvektor von f zum Eigenwert λ. Der Eigenraum zu $\lambda \in K$ ist $\mathrm{Eig}(f, \lambda) = \{x \in V \mid f(x) = \lambda x\}$.

Definition 1.2 (EW und EV für Matrizen)
Sei $A \in \mathrm{Mat}_n(K)$. Man definiert Eigenwerte, Eigenvektoren, etc von A als Eigenwerte, Eigenvektoren von $f_A \in \mathrm{End}_K(K^n)$.

2. Das charakteristische Polynom

Definition 2.1 (charakteristisches Polynom)
Das charakteristische Polynom einer Matrix $A \in \mathrm{Mat}_n(K)$ ist die Determinante der Matrix $t \cdot \mathbb{1}_n - A \in \mathrm{Mat}_n(K[t])$.

$$\chi_A(t) = \det(t \cdot \mathbb{1}_n - A) \in K[t]$$

Das charakteristische Polynom eines Endomorphismus $f \in \mathrm{End}_K(V)$ ist $\chi_f(t) = \chi_{M_B(f)}(t)$, wobei B eine Basis von V ist.

Definition 2.2 (normiertes Polynom)
Ein Polynom $0 \neq P \in K[t]$ mit Leitkoeffizient 1 heißt normiert .

3. Diagonalisierbarkeit

Definition 3.1 (diagonalisierbar)
Man nennt f diagonalisierbar , wenn V eine Basis B besitzt, für die $M_B(f)$ eine Diagonalmatrix ist.

Definition 3.2 (*a* teilt *b*)
Sei R ein kommutativer Ring mit seien $a, b \in R$. Man sagt, a teilt b (in Zeichen $a \mid b$), wenn es $x \in R$ mit $b = ax$ gibt.

Definition 3.3 (Vielfachheit)
Für $0 \neq P \in K[t]$ und $\lambda \in K$ nennt man $\mu(P, \lambda) = \max\{r \in \mathbb{N}_{>0} \mid (t - r)^r \mid P\}$ die Vielfachheit der Nullstelle λ von P.

Definition 3.4 (algebraische und geometrische Vielfachheit)
Man nennt $\mu_a(f, \lambda) = \mu(\chi_f, \lambda)$ die algebraische Vielfachheit und $\mu_g(f, \lambda) = \dim_K(\mathrm{Eig}(f, \lambda))$ die geometrische Vielfachheit des Eigenwertes λ von f.

4. Trigonalisierbarkeit

Definition 4.1
Man nennt f trigonalisierbar , wenn V eine Basis B besitzt, für die $M_B(f)$ eine obere Dreiecksmatrix ist.

Definition 4.2 (invariant)
Ein Untervektorraum $W \leq V$ ist f-invariant , wenn $f(W) \leq W$.

5. Das Minimalpolynom

Definition 5.1
Für ein Polynom $P(t) = \sum_{i=0}^{n} c_i t^i \in K[t]$ definieren wir $P(f) = \sum_{i=0}^{m} c_i f^i \in \mathrm{End}_K(V)$, wobei $f^0 = \mathrm{id}_V$, $f^1 = f$, $f^2 = f \circ f$, ...

Analog definiert man $P(A)$ für $A \in \mathrm{Mat}_n(K)$.

Definition 5.2 (Minimalpolynom)
Das eindeutig bestimmte normierte Polynom $0 \neq P \in K[t]$ kleinsten Grades mit $P(f) = 0$ nennt man das Minimalpolynom P_f von f.

Analog definiert man das Minimalpolynom $P_A \in K[t]$ einer Matrix $A \in \mathrm{Mat}_n(K)$.

Definition 5.3 (f-zyklisch)
Ein f-invarianter UVR $W \leq V$ heißt f-zyklisch , wenn es ein $x \in W$ mit $W = \mathrm{span}_K(x, f(x), f^2(x), ...)$ gibt.

6. Nilpotente Endomorphismen

Definition 6.1 (nilpotent)
Ein $f \in \mathrm{End}_K(V)$ heißt nilpotent , wenn $f^k = 0$ für ein $k \in \mathbb{N}$. Analog heißt $A \in \mathrm{Mat}_n(K)$ nilpotent, wenn $A^k = 0$ für $k \in \mathbb{N}$. Das kleinste k mit $f^k = 0$ bzw. A^k heißt die Nilpotenzklasse von f bzw. A.

Definition 6.2 (Jordan-Matrix)
Für $k \in \mathbb{N}$ definieren wir die JORDAN-Matrix

$$J_k = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & 1 \\ 0 & \dots & \dots & \dots & 0 \end{pmatrix} \in \mathrm{Mat}_k(K)$$

weiter setzen wir für $\lambda \in K$ $J_k(\lambda) := \lambda \mathbb{1} + J_k$.

7. Die Jordan-Normalform

Definition 7.1 (Hauptraum)
Der Hauptraum von f zum EW λ der Vielfachheit $r = \mu_a(f, \lambda)$ ist

$$\mathrm{Hau}(f, \lambda) = \mathrm{Ker}\left((f - \lambda\, \mathrm{id}_V)^r\right)$$

Kapitel VI

Skalarprodukte

In diesem ganzen Kapitel seien

- $K = \mathbb{R}$ oder $K = \mathbb{C}$
- $n \in \mathbb{N}$
- V ein n-dimensionaler K-VR

1. Das Standardskalarprodukt

Sei zunächst $K = \mathbb{R}$.

Definition 1.1 (Standardskalarprodukt in $\mathbb{R}$)
Auf den Standardraum $V = \mathbb{R}^n$ definiert man das Standardskalarprodukt in $\mathbb{R}$ $\langle . \rangle : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ durch

$$\langle x, y \rangle = x^t y = \sum_{i=1}^{n} x_i y_i$$

Sei nun $K = \mathbb{C}$.

Definition 1.2 (komplexe Konjugation, Absolutbetrag)
Für $x, y \in \mathbb{R}$ und $z = x + iy \in \mathbb{C}$ definiert man $\overline{z} = x - iy$ heißt komplexe Konjugation .. Man definiert den Absolutbetrag von z als

$$|z| = \sqrt{z\overline{z}} = \sqrt{x^2 + y^2} \in \mathbb{R}_{\geq 0}$$

Für $A = (a_{ij})_{i,j} \in \mathrm{Mat}_{m \times n}(\mathbb{C})$ sehen wir

$$\overline{A} = (\overline{a_{ij}})_{i,j} \in \mathrm{Mat}_{m \times n}(\mathbb{C})$$

Definition 1.3 (Standardskalarprodukt in $\mathbb{C}$)
Auf $K = \mathbb{C}^n$ definiert man das Standardskalarprodukt in $\mathbb{C}$ $\langle \cdot, \cdot \rangle : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$ durch

$$\langle x, y \rangle = x^t \overline{y} = \sum_{i=1}^{n} x_i \overline{y}_i$$

Definition 1.4 (euklidische Norm in $\mathbb{C}$)
Auf $V = \mathbb{C}$ definiert man die euklidische Norm in $\mathbb{C}$ $\| \cdot \| : \mathbb{C}^n \to \mathbb{R}_{\geq 0}$ durch

$$\|x\| = \sqrt{\langle x, x \rangle}$$

2. Bilinearformen und Sesquilinearformen

Sei $K = \mathbb{R}$ oder $K = \mathbb{C}$.

Definition 2.1 (Bilinearform, Sesquilinearform)
Eine Bilinearform ($K = \mathbb{R}$) bzw. Sesquilinearform ($K = \mathbb{C}$) ist eine Abbildung $s : V \times V \to K$ für die gilt:

- Für $x, x', y \in V$ ist $s(x + x', y) = s(x, y) + s(x', y)$
- Für $x, y, y' \in V$ ist $s(x, y + y') = s(x, y) + s(x, y')$
- Für $x, y \in V$, $\lambda \in K$ ist $s(\lambda x, y) = \lambda s(x, y)$
- Für $x, y \in V$, $\lambda \in K$ ist $s(x, \lambda y) = \overline{\lambda} s(x, y)$

Definition 2.2
Sei s eine Sesquilinearform auf V und $B = (v_1, ..., v_n)$ eine Basis von V. Die darstellende Matrix von s bzgl. B ist

$$M_B(s) = (s(v_i, v_j))_{i,j} \in \mathrm{Mat}_n(K)$$

Definition 2.3 (ausgeartet)
Eine Sesquilinearform s auf V heißt ausgeartet , wenn eine der äquivalenten Bedingungen aus ?? erfüllt ist, sonst nicht-ausgeartet.

Definition 2.4 (symmetrisch, hermitesch)
Eine Sesquilinearform s auf V heißt symmetrisch , wenn bzw. hermitesch , wenn

$$s(x, y) = \overline{s(y, x)} \quad \text{für alle } x, y \in V$$

Eine Matrix $A \in \mathrm{Mat}_n(K)$ heißt symmetrisch bzw. hermitesch, wenn $A = A^* = \overline{A}^t = \overline{A^t}$.

3. Euklidische und unitäre Vektorräume

Definition 3.1 (quadratische Form)
Sei s eine hermitesche Sesquilinearform auf V. Die quadratische Form zu s ist die Abbildung

$$q_s : \begin{cases} V \to \mathbb{R} \\ x \mapsto s(x, x) \end{cases}$$

Definition 3.2 ((semi)definit, euklidischer VR, unitärer VR)
Sei s eine hermitesche Sesquilinearform auf V. Ist $s(x, x) \geq 0$ für alle $x \in V$, so heißt s positiv semidefinit . Ist $s(x, x) > 0$ für alle $0 \neq x \in V$, so heißt s positiv definit (oder ein Skalarprodukt).

Eine hermitesche Matrix $A \in \mathrm{Mat}_n(K)$ heißt positiv (semi)definit, wenn s_A dies ist.

Einen endlichdimensionalen K-VR zusammen mit positiv definiten hermiteschen Sesquilinearformen nennt man einen euklidischen bzw. unitären VR (oder auch Prähilbertraum). Wenn nicht anderes angegeben, notieren wir die Sesquilinearform mit $\langle \cdot, \cdot \rangle$.

Definition 3.3
Ist V ein unitärer VR, so definiert man die Norm von $x \in V$ als

$$\|x\| = \sqrt{\langle x, x \rangle} \in \mathbb{R}_{\geq 0}$$

4. Orthogonalität

Sei V ein euklidischer bzw. unitärer Vektorraum.

Definition 4.1 (orthogonal, orthogonales Komplement)
Zwei Vektoren $x, y \in V$ heißen orthogonal, in Zeichen $x \perp y$, wenn $\langle x, y \rangle = 0$. Zwei Mengen $X, Y \subseteq V$ sind orthogonal, in Zeichen $X \perp Y$, wenn $x \perp y$ für alle $x \in X$ und $y \in Y$.

Für $U \subseteq V$ bezeichnet

$$U^{\perp} = \{x \in V \mid x \perp u \text{ für alle } u \in U\}$$

das orthogonale Komplement zu U.

Definition 4.2 (orthonormal)
Eine Familie $(x_i)_{i \in I}$ von Elementen von V ist orthogonal, wenn $x_i \perp x_j$ für alle $i \neq j$, und orthonormal, wenn zusätzlich $\|x_i\| = 1$ für alle i. Eine orthogonale Basis nennt man eine Orthogonalbasis, eine orthonormale Basis nennt man eine Orthonormalbasis.

5. Orthogonale und unitäre Endomorphismen

Sei V ein euklidischer bzw. unitärer Vektorraum und $f \in \mathrm{End}_K(V)$.

Definition 5.1 (orthogonale, unitäre Endomorphismen)
f ist orthogonal bzw. unitär, wenn

$$\langle f(x), f(y) \rangle = \langle x, y \rangle \quad \forall x, y \in V$$

Definition 5.2 (orthogonale, unitäre Matrizen)
Eine Matrix $A \in \mathrm{Mat}_n(K)$ heißt orthogonal bzw. unitär, wenn

$$A^* A = \mathbb{1}_n$$

6. Selbstadjungierte Endomorphismen

Sei V ein euklidischer bzw. unitärer Vektorraum und $f \in \mathrm{End}_K(V)$.

Definition 6.1 (selbstadjungiert)
f ist selbstadjungiert, wenn

$$\langle f(x), y \rangle = \langle x, f(y) \rangle \quad \forall x, y \in V$$

7. Hauptachsentransformation

Sei V ein euklidischer bzw. unitärer Vektorraum und s eine hermitesche Sesquilinearform auf V.

Definition 7.1 (Ausartungsraum)
Der Ausartungsraum von s ist

$$V_0 = \{x \in V \mid s(x, y) = 0 \quad \forall y \in V\}$$

Definition 7.2 (Signatur)
Die Signatur von s ist das Tripel

$$(r_+(s), r_-(s), r_0(s))$$

wobei $r_0(s) = \dim_K(V_0)$.

8. Quadriken

Sei $n \in \mathbb{N}$.

Definition 8.1 (Quadrik)
Eine Quadrik ist eine Teilmenge von $\mathbb{R}^n$ mit

$$Q = \{x \in \mathbb{R}^n \mid x^t A x + 2b^t x + c = 0\}$$

mit $A \in \mathrm{Mat}_n(\mathbb{R})$ symmetrisch, $b^t \in \mathbb{R}^n$ und $c \in \mathbb{R}$.

Definition 8.2 (Typen von Quadriken)
Sei Q gegeben durch (A, b, c) wie in Definition 8.1. Q heißt

- vom kegeligen Typ , wenn $\mathrm{rk}(A) = \mathrm{rk}(A, b) = \mathrm{rk}(\tilde{A})$
- eine Mittelpunktsquadrik , wenn $\mathrm{rk}(A) = \mathrm{rk}(A, b) < \mathrm{rk}(\tilde{A})$
- vom parabolischen Typ , wenn $\mathrm{rk}(A) < \mathrm{rk}(A, b)$
- ausgeartet , wenn $\det(\tilde{A}) = 0$

Definition 8.3 (Isometrie)
Eine Isometrie des $\mathbb{R}^n$ ist $f \in \mathrm{Aff}_{\mathbb{R}}(\mathbb{R}^n)$ mit

$$f(x) = Ax + b$$

mit $b \in \mathbb{R}^n$ und $A \in \mathrm{GL}_n(\mathbb{R})$ ist orthogonal.

Kapitel VII

Dualität

1. Das Lemma von Zorn

Sei K ein Körper und U, V, W seien K-Vektorräume. Zudem sei X eine Menge.

Definition 1.1 (Relation)
Eine Relation ist eine Teilmenge $R \subseteq X \times X$. Man schreibt $(x, x') \in R$ als xRx'. R heißt

- reflexiv , wenn $\forall x \in X$: xRx
- transitiv , wenn $\forall x, y, z \in X$: xRy und $yRz \Rightarrow xRz$
- symmetrisch , wenn $\forall x, y \in X$: $xRy \Rightarrow yRx$
- antisymmetrisch , wenn $\forall x, y \in X$: xRy und $yRx \Rightarrow y = x$
- total , wenn $\forall x, y \in X$: $(x, y) \notin R \Rightarrow (y, x) \in R$

Definition 1.2 (Halbordnung)
Eine Halbordnung (oder partielle Ordnung) ist eine reflexive, transitive und antisymmetrische Relation $\leq$. Eine totale Halbordnung heißt Totalordnung oder lineare Ordnung . Man schreibt $x < y$ für $x \leq y \wedge x \neq y$.

Definition 1.3 (Kette)
Sei $(X, \leq)$ eine Halbordnung, $Y \subseteq X$. Y heißt Kette , wenn $(Y, \leq|_Y)$ total ist.

$x \in Y$ heißt ein minimales Element von Y, wenn $\forall x' \in Y$: $x < x'$.

$x \in Y$ heißt untere Schranke von Y, wenn $\forall y \in Y$: $y \geq x$.

$x \in Y$ heißt kleinstes Element von Y, wenn x untere Schranke von Y ist.

Analog: maximales Element , obere Schranke , größtes Element .

Theorem 1.4 (Das Lemma von Zorn)
Sei $(X, \leq)$ eine Halbordnung, die nicht leer ist. Wenn jede Kette eine obere Schranke hat, dann hat X ein maximales Element.

Beweis. Das Lemma von Zorn hat axiomatischen Charakter - es ist äquivalent zum Auswahlaxiom, seine Gültigkeit ist somit abhängig von unseren grundlegenden mengentheoretischen Annahmen. Für einen Beweis des Lemmas von Zorn aus dem Auswahlaxiom siehe die Vorlesung *Mengenlehre*. Wir zeigen hier zumindest die andere Richtung, nämlich dass das Auswahlaxiom aus dem Lemma von Zorn folgt. □

Folgerung 1.5 (Auswahlaxiom)
Zu jeder Familie (x_i), nicht leer, gibt es eine Auswahlfunktion , das heißt eine Abbildung:

$$f : I \to \bigcup_{i \in I} X_i \text{ mit } f(i) \in X_i \quad \forall i$$

Beweis. Sei $\mathcal{F}$ die Menge der Paare (J, f) bestehend aus einer Teilmenge $J \subseteq I$ und einer Abbildung $f : I \to \bigcup_{i \in I} X_i$ mit $f(i) \in X_i \quad \forall i \in J$. Definieren wir $(J, f) \leq (J', f') \iff J \subseteq J'$ und $f'|_J = f$, so ist $\leq$ eine Halbordnung auf $\mathcal{F}$. Da $(\emptyset, \emptyset) \in \mathcal{F}$ ist $\mathcal{F}$ nichtleer. Ist $\mathcal{G} \subseteq \mathcal{F}$ eine nichtleere Kette, so wird auf $J' := \bigcup_{(J,f) \in \mathcal{G}} J$ durch $f'(j) = f(j)$ falls $(J, f) \in \mathcal{G}$ und $j \in J$ eine wohldefinierte Abbildung $f' : J \to \bigcup_{i \in J} X_i$ mit $f'(i) \in X_i \quad \forall i \in J'$ gegeben. Das Paar (J', f') ist eine obere Schranke der Kette $\mathcal{G}$. Nach dem Lemma von Zorn besitzt $\mathcal{F}$ ein maximales Element (J, f). Wir behaupten, dass $J = I$. Andernfalls nehmen wir ein $i' \in I \backslash J$ und ein

$x' \in X_{i'}$ und definieren $J' := U \cup \{i'\}$ und $f' : J' \to \bigcup_{i \in J'} X_i$, $j \mapsto \begin{cases} f(j) & j \in J \\ x' & j = i' \end{cases}$. Dann ist $(J', f') \in \mathcal{F}$ und $(J, f) < (J', f')$ im Widerspruch zur Maximalität von (J, f). □

Folgerung 1.6 (Basisergänzungssatz)
Sei V ein K-Vektorraum. Jede linear unabhängige Teilmenge $X_0 \subseteq V$ ist in einer Basis von V enthalten.

Beweis. Sei $\mathfrak{X} = \{X \subseteq V \mid X \text{ ist linear unabhängig}, X_0 \subseteq X\}$ geordnet durch Inklusion. Dann ist $X_0 \in \mathfrak{X}$, also $\mathfrak{X} \neq \emptyset$. Ist $\mathcal{Y}$ eine nichtleere Kette in $\mathfrak{X}$, so ist auch $Y = \bigcup \mathcal{Y} \subseteq V$ linear unabhängig. Sind $y_1, ..., y_n \in Y$ paarweise verschieden, so gibt es $Y_1, ..., Y_n \in \mathcal{Y}$ mit $y_i \in Y_i$ für $i = 1, ..., n$. Da $\mathcal{Y}$ total geordnet ist, besitzt $\{Y_1, ..., Y_n\}$ ein größtes Element, o.E. Y_1. Also sind $y_1, ..., y_n \in Y_1$ und somit linear unabhängig. Folglich ist $Y_1 \in \mathfrak{X}$ eine obere Schranke von $\mathcal{Y}$. Nach dem Lemma von Zorn besitzt $\mathfrak{X}$ ein maximales Element X. Das heißt, X ist eine maximal linear unabhängige Teilmenge von V, nach LAAG1 II.3.5 also eine Basis von V. □

2. Der Dualraum

Sei V ein K-Vektorraum.

Definition 2.1 (Dualraum)
Der Dualraum zu V ist der K-Vektorraum

$$V^* = \mathrm{Hom}_K(V, K) = \{\varphi : V \to K \text{ linear}\}$$

Die Elemente von V^* heißen Linearformen auf V.

Definition 2.2 (duale Basis)
Ist $B = (x_i)_{i \in I}$ eine endliche Basis von V, so nennt man $B^* = (x_i^*)_{i \in I}$ die zu B duale Basis .

Definition 2.3 (Bidualraum)
Der Bidualraum zu V ist der K-Vektorraum

$$V^{**} = (V^*)^* = \mathrm{Hom}_K(V^*, K)$$

Definition 2.4 (Annulator)
Für eine Teilmenge $U \subseteq V$ bezeichne

$$U^0 = \{\varphi \in V^* \mid \varphi(x) = 0 \quad \forall x \in U\}$$

den Annulator von U.

3. Die duale Abbildung

Sei $f \in \mathrm{Hom}_K(V, W)$.

Definition 3.1 (duale Abbildung)
Die zu f duale Abbildung ist

$$f^* : \begin{cases} W^* \to V^* \\ \varphi \mapsto \varphi \circ f \end{cases}$$

4. Die adjungierte Abbildung

Sei $K = \mathbb{R}$ oder $K = \mathbb{C}$ und V ein endlichdimensionaler unitärer K-Vektorraum.

Definition 4.1 (weitere Skalarmultiplikation)
Wir definieren auf V eine Skalarmultiplikation

$$\lambda * x = \overline{\lambda} \cdot x$$

und schreiben $\overline{V} = (V, +, *)$.

Definition 4.2 (adjungierter Endomorphismus)
Die Abbildung f^{adj} heißt der zu f adjungierte Endomorphismus .

5. Der Spektralsatz

Sei V ein endlichdimensionaler unitärer K-Vektorraum und $f \in \mathrm{End}_K(V)$.

Definition 5.1 (normaler Endomorphismus, normale Matrix)
Der Endomorphismus f heißt normal , wenn

$$f \circ f^{adj} = f^{adj} \circ f$$

Entsprechend heißt $A \in \mathrm{Mat}_n(K)$ normal , wenn

$$AA^* = A^*A$$

Theorem 5.2 (Spektralsatz)
Sei $f \in \mathrm{End}_K(V)$ ein Endomorphismus, für den χ_f in Linearfaktoren zerfällt. Genau dann besitzt V eine Orthonormalbasis aus Eigenvektoren von f, wenn f normal ist.

Beweis.

- Hinrichtung: Ist B eine Orthonormalbasis aus Eigenvektoren von f, so ist $A = M_B(f)$ eine Diagonalmatrix. Dann ist auch $M_B(f^{adj}) \overset{??}{=} A^*$ eine Diagonalmatrix und $AA^* = A^*A$. Somit ist f normal.
- Rückrichtung: Sei f normal und $\chi_f(t) = \prod_{i=1}^n (t - \lambda_i)$. Beweis nach Induktion nach $n = \dim_K(V)$.
  $\underline{n = 0}$: klar
  $\underline{n - 1 \to n}$: Wähle Eigenvektor zum Eigenwert λ_1, o.E. $\|x_1\| = 1$. Sei $U = K \cdot x_1$. Nach ?? ist $f^{adj}(x_1) = \overline{\lambda_1} x_1$, insbesondere ist U f-invariant und f^{adj}-invariant. Für $x \in U^\perp$ ist

  $$\langle f(x), x_1 \rangle = \left\langle x, f^{adj}(x_1) \right\rangle = \left\langle x, \overline{\lambda_1} x_1 \right\rangle = \lambda_1 \langle x, x_1 \rangle = 0$$

  also $f(x) \in U^\perp$ und

  $$\left\langle f^{adj}(x), x_1 \right\rangle = \langle x, f(x_1) \rangle = \langle x, \lambda_1 x_1 \rangle = \overline{\lambda_1} \langle x, x_1 \rangle = 0$$

  also $f^{adj}(x) \in U^\perp$. Somit ist $V = U \oplus U^\perp$ eine Zerlegung in Untervektorräume, die sowohl f-invariant als auch f^{adj}-invariant sind. Insbesondere st $f^{adj}|_{U^\perp} = (f|_{U^\perp})^{adj}$, woraus folgt, dass auch $f|_{U^\perp}$ normal ist:

  $$f|_{U^\perp} \circ (f|_{U^\perp})^{adj} = f \circ f^{adj}|_{U^\perp} = f^{adj} \circ f|_{U^\perp} = f^{adj}|_{U^\perp} \circ f|_{U^\perp} = (f|_{U^\perp})^{adj} \circ f|_{U^\perp}$$

  Außerdem zerfällt auch $\chi_{f|_{U^\perp}} = \prod_{i=2}^n (t - \lambda_i)$ in Linearfaktoren. Nach Induktionshypothese existiert eine Orthonormalbasis $(x_2, ..., x_n)$ von $U^\perp$ bestehend aus Eigenvektoren von $f|_{U^\perp}$ und $(x_1, ..., x_n)$ ist dann eine Orthonormalbasis von V aus Eigenvektoren von f. □

6. Tensorprodukte

Definition 6.1 (billineare Abbildung)
Eine Abbildung $\xi : V \times W \to U$ ist bilinear , wenn für jedes $v \in V$ die Abbildung

$$\begin{cases} W \to U \\ w \mapsto \xi(v, w) \end{cases}$$

und für jedes $w \in W$ die Abbildung

$$\begin{cases} V \to U \\ v \mapsto \xi(v, w) \end{cases}$$

linear sind.

Wir definieren

$$\mathrm{Bil}_K(V, W, U) = \{\xi \in \mathrm{Abb}(V \times W, U) \mid \xi \text{ bilinear}\}$$

Definition 6.2 (Tensorprodukt)
Ein Tensorprodukt von V und W ist ein Paar (T, τ) bestehend aus einem K-Vektorraum T und einer bilinearen Abbildung $\tau \in \mathrm{Bil}_K(V, W, T)$ welche die folgende universelle Eigenschaft erfüllt: *Ist U ein weiterer K-Vektorraum und $\xi \in \mathrm{Bil}_K(V, W, U)$ so gibt es genau ein $\xi_\otimes \in \mathrm{Hom}_K(T, U)$ mit $\xi = \xi_\otimes \circ \tau$.*

$$\begin{tikzcd} V \times W \arrow[r, "\tau"] \arrow[dr, "\xi"'] & T \arrow[d, dashed, "\xi_\otimes"] \\ & U \end{tikzcd}$$

Definition 6.3 (Vektorraum mit Basis X)
Sei X eine Menge. Der K-Vektorraum mit Basis X ist der Untervektorraum $V = \mathrm{span}_K((\delta_x)_{x \in X})$ des K-Vektorraum $\mathrm{Abb}(X, K)$ mit $\delta_x(y) = \delta_{x,y} = \begin{cases} 1 & x = y \\ 0 & x \neq y \end{cases}$

Kapitel VIII
Moduln

In diesem ganzen Kapitel sei R ein kommutativer Ring mit Einselement.

1. Moduln

Definition 1.1
Ein R-Modul ist ein Tripel $(M, +, \cdot)$ bestehend aus einer Menge M, einer Verknüpfung $+ : M \times M \to M$ und der Abbildung $\cdot : R \times M \to M$ (Skalarmultiplikation) für die gelten:

- (M1): $(M, +)$ ist eine abelsche Gruppe
- (M2): Addition und Skalarmultiplikation sind verträglich. Für alle $x, y \in M$ und $a, b \in R$ gelten
  1. $a(x + y) = ax + ay$
  2. $(a + b)x = ax + bx$
  3. $a \cdot bx = ab \cdot x$
  4. $1 \cdot x = x$

■ **Beispiel 1.2**

1. Ist $R = K$ ein Körper, so sind die R-Moduln genau die K-Vektorräume.
2. Ist $R = \mathbb{Z}$, so sind die R-Moduln genau die abelschen Gruppen mit der einzig möglichen Skalarmultiplikation
$$\mathbb{Z} \times A \to A, (k, a) \mapsto ka = \underbrace{1 + ... + 1}_{k\text{-mal}} a = \underbrace{a + ... + a}_{k\text{-mal}}$$
vergleiche Laag 1 III.2.3
3. Jedes Ideal $M \subseteq R$ ist ein R-Modul mit Einschränkung der Multiplikation als Skalarmultiplikation.
4. Ist K ein Körper, V ein K-Vektorraum und $f \in \mathrm{End}_K(V)$, so wird V durch $P(t) \cdot x := P(f)(x)$ zu einem Modul über dem Ring $R = K[t]$, siehe auch V.5.2

Definition 1.3 (Homomorphismus von *R*-Moduln)
Seien M, M' R-Moduln. Eine Abbildung $f : M \to M'$ ein Homomorphismus von R-Moduln (oder R-Homomorphismus oder R-linear), wenn
$$f(x + y) = f(x) + f(y)$$
$$f(ax) = a \cdot f(x)$$
Wir bezeichnen die Menge der R-Homomorphismen $f : M \to M'$ mit $\mathrm{Hom}_R(M, M')$. Wie üblich definiert man den Kern eines R-Homomorphismus, sowie die Begriffe Monomorphismus , Epimorphismus , Isomorphismus , Endomorphismus und Automorphismus von R-Moduln.

Definition 1.4 (Untermodul, Erzeugendensystem)
Ein Untermodul ist eine nichtleere Teilmenge $N \subseteq M$, für die gilt:

- Sind $x, y \in N$, so ist auch $x + y \in N$.
- Ist $a \in R$ und $x \in N$, so ist auch $ax \in N$.

Für eine Familie $(x_i)_{i \in I}$ ist

$$\sum_{i \in I} Rx_i = \{\sum_{i \in I} ax_i \mid a \in R, \text{ fast alle gleich } 0\}$$

der von $(x_i)_{i \in I}$ erzeugte Untermodul von M. Ist $\sum_{i \in I} Rx_i = M$, so ist $(x_i)_{i \in I}$ ein Erzeugendensystem von M. Der R-Modul M ist endlich erzeugt , wenn er ein endliches Erzeugendensystem besitzt.

Definition 1.5 (freie Familie, Basis)
Eine Familie $(x_i)_{i \in I}$ in M ist frei oder (R-linear unabhängig), wenn es keine Familie $(\lambda_i)_{i \in I}$ von Elementen von R, fast alle gleich 0, aber nicht alle gleich 0, mit $\sum_{i \in I} \lambda_i x_i = 0$ gibt.

Ein freies Erzeugendensystem heißt Basis . Besitzt M eine Basis, so nennt man M frei .

Definition 1.6 (Summen von Moduln)
Die Summe einer Familie $(N_i)_{i \in I}$ von Untermoduln von M ist

$$\sum_{i \in I} N_i = \left\{\sum_{i \in I} x_i \mid x_i \in N_i, \text{ fast alle gleich } 0\right\}$$

Lässt sich jedes $x \in \sum_{i \in I} N_i$ eindeutig als $\sum_{i \in I} x_i$ mit $x_i \in N_i$ schreiben, so nennt man die Summe direkt und schreibt dafür auch $\bigoplus_{i \in I} N_i$.

Ist $(M_i)_{i \in I}$ eine Familie von R-Moduln, so definiert man deren (externe) direkte Summe als das R-Modul

$$\bigoplus_{i \in I} M_i := \left\{(x_i)_{i \in I} \in \prod_{i \in I} M_i \mid x_i = 0 \text{ für fast alle } i \in I\right\}$$

mit komponentenweiser Addition und Skalarmultiplikation.

Definition 1.7 (Torsionsmodul)
Für $a \in R$ definiert man den a-Torsionsmodul von M als

$$M[a] := \{x \in M \mid ax = 0\}$$

Die Elemente des Torsionsmoduls

$$M_{tor} := \bigcup_{0 \neq a \in R} M[a] = \{x \in M \mid ax = 0 \text{ für ein } a \in R \backslash \{0\}\}$$

nennt man die Torsionselemente von M.

2. Teilbarkeit

Definition 2.1 (Teilbarkeit)
Seien $a, b \in R$.

1. a teilt b (in Zeichen $a \mid b$): Es existiert $x \in R$ mit $b = ax$.
2. a und b sind assoziiert (in Zeichen $a \sim b$): Es existiert $x \in R^\times$ mit $b = ax$.

Definition 2.2 (größter gemeinsamer Teiler, kleinstes gemeinsames Vielfaches)
Seien $a, b \in R$. Ein $c \in R$ ist ein größter gemeinsamer Teiler von a und b in Zeichen $c = \operatorname{ggT}(a, b)$, wenn gilt: $c \mid a$ und $c \mid b$ und ist $d \in R$ mit $d \mid a$ und $d \mid b$, so auch $d \mid c$.

Ein $c \in R$ ist ein kleinstes gemeinsames Vielfaches von a und b, in Zeichen $c = \operatorname{kgV}(a, b)$, wenn gilt: $a \mid c$ und $b \mid c$ und ist $d \in R$ mit $a \mid d$ und $b \mid d$, so ist $c \mid d$.

Definition 2.3 (Primzahl, irreduzibel)
Sei $x \in R$.

- x ist prim $\iff$ $x \notin R^\times \cup \{0\}$ und $\forall a, b \in R$ gilt $x \mid (ab) \Rightarrow x \mid a \vee x \mid b$.
- x ist irreduzibel $\iff$ $x \notin R^\times \cup \{0\}$ und $\forall a, b \in R$ gilt $x = ab \Rightarrow a \in R^\times \vee b \in R^\times$.

Definition 2.4 (erzeugtes Ideal, Hauptideal)
Sei $A \subseteq R$. Das von A erzeugte Ideal mit

$$\langle A \rangle := \left\{ \sum_{i=1}^{n} r_i a_i \mid n \in \mathbb{N}_0, a_1, ..., a_n \in A, r_1, ..., r_n \in R \right\}$$

Ist $A = \{a_1, ..., a_n\}$, so schreibt man auch $(a_1, ..., a_n)$ für $\langle A \rangle$. Ein Ideal der Form $I = (a)$ ist ein Hauptideal .

3. Hauptidealringe

Sei R nullteilerfrei.

Definition 3.1 (Hauptidealring)
Ein Ring R ist ein Hauptidealring , wenn R nullteilerfrei ist und jedes Ideal von R ein Hauptideal ist.

Beispiel 3.2
Ist $R = K$ ein Körper, so hat R nur die Ideale (0) und (1), und somit ist R ein Hauptidealring.

Definition 3.3 (euklidische Gradfunktion)
Eine euklidische Gradfunktion auf R ist eine Abbildung $\delta : R \backslash \{0\} \to \mathbb{N}_0$ für die gilt:
Für jedes $a \in R$ und $0 \neq b \in R$ gibt es $q, r \in R$ mit $a = bq + r$, wobei $r = 0$ oder $\delta(r) < \delta(b)$.

Ein nullteilerfreier Ring R ist euklidisch , wenn es eine euklidische Gradfunktion auf R gibt.

Lemma 3.4 (Lemma von Bézout)
Sei R ein Hauptidealring und $a, b \in R$. Es existiert ein $c \in R$ mit $c = \operatorname{ggT}(a, b)$ und $(c) = (a, b)$. Insbesondere gibt es $x, y \in R$ mit $c = ax + by$ und $\operatorname{ggT}(x, y) = 1$.

Beweis. R Hauptidealring $\Rightarrow \exists c \in R$ mit $(c) = (a, b)$, insbesondere $c = ax + by$ mit $x, y \in R$.

- $c = \operatorname{ggT}(a, b)$: $a, b \in (c) \Rightarrow c \mid a$ und $c \mid b$. Ist $d \in R$ mit $d \mid a$ und $d \mid b$, so ist $d \mid (ax + by) = c$
- $\operatorname{ggT}(x, y) = 1$: Ist $d \in R$ mit $d \mid x$ und $d \mid y$, so gelten $(cd) \mid (ax)$ und $(cd) \mid (by) \Rightarrow (cd) \mid (ax + by) = c \Rightarrow d \in R^\times$, also $d \sim 1$. □

4. Faktorielle Ringe

Sei R nullteilerfrei.

Definition 4.1 (faktorielle Ringe)
R ist faktoriell $\iff$ jedes $0 \neq x \in R \backslash R^\times$ ist ein Produkt von Primelementen.

■ **Beispiel 4.2**

1. Jedes $n \in \mathbb{N}$ lässt sich eindeutig als
$$n = \prod_{p \in \mathbb{P}} p^{n_p}$$
schreiben, wobei $\mathbb{P}$ die Menge der Primzahlen ist (Hauptsatz der Arithmetik).
2. Bezeichnet $\mathcal{M}$ die Menge der normierten irreduziblen Polynome in $K[t]$ (K Körper), so lässt sich jedes $0 \neq f \in K[t]$ eindeutig als
$$f = c \cdot \prod_{P \in \mathcal{M}} P^{n_p}$$
mit $c \in K^\times$ und $n_p \in \mathbb{N}_0$, fast alle gleich 0, schreiben.

5. Quotienten von Ringen und Moduln

Seien M und M' zwei R-Moduln und $N \subseteq M$ ein Untermodul.

Definition 5.1 (Quotientenmodul)
Für $x \in M$ schreiben wir
$$x + N := \{x + y \mid y \in N\}$$
Der Quotientenmodul (oder Faktormodul) von M modulo N ist
$$M/N := \{x + N \mid x \in M\}$$
zusammen mit der Addition
$$(x+N) + (y+N) := (x+y) + N \quad (x, y \in M)$$
und der Skalarmultiplikation
$$r \cdot (x+N) := rx + N \quad (x \in M, r \in R)$$
Sei $\pi_N : M \to M/N$ die Abbildung gegeben durch $x \mapsto x + N$.

Satz 5.2 (Homomorphiesatz für Moduln)
Sei $f \in \mathrm{Hom}_K(M, M')$ und $N \subseteq M$ ein Untermodul mit $N \subseteq \mathrm{Ker}(f)$. Dann gibt es genau ein $\overline{f} \in \mathrm{Hom}_K(M/N, M')$ mit $f = \overline{f} \circ \pi_N$.

$$\begin{tikzcd}
M \arrow[rr, "f"] \arrow[dr, "\pi_N"'] & & M' \\
& M/N \arrow[ur, dashed, "\overline{f}"'] &
\end{tikzcd}$$

Beweis. Analog zu LAAG 1 III.7.9. Man zeigt, dass jedes $\overline{f} \in \mathrm{Hom}_K(M/N, M')$
$$\overline{f}(x+N) = f(x) \quad (x \in M)$$
erfüllen muss, und dass dies wiederum eine wohldefinierte Abbildung liefert. □

Definition 5.3 (Quotientenring)
Sei $I \trianglelefteq R$ ein Ideal. Für $x \in R$ schreiben wir

$$x + I = \{x + a \mid a \in I\}$$

Dann ist

$$R/I = \{x + I \mid x \in R\}$$

der <u>Quotientenring</u> von R modulo I mit Addition und Skalarmultiplikation

$$(x+I) + (x'+I) = (x+x') + I \quad \forall x, x' \in R$$
$$(x+I) \cdot (x'+I) = (x \cdot x') + I \quad \forall x, x' \in R$$

Und wieder $\pi_I : R \to R/I$ mit $x \mapsto x + I$.

Satz 5.4 (Homomorphiesatz für Ringe)
Sei $\varphi : R \to R'$ ein Ringhomomorphismus, $I \trianglelefteq R$ ein Ideal mit $I \subseteq \mathrm{Ker}(\varphi)$. Dann gibt es genau einen Ringhomomorphismus mit $\overline{\varphi} : R/I \to R'$, sodass $\overline{\varphi} \circ \pi_I = \varphi$.

$$\begin{tikzcd}
M \arrow[rr, "\varphi"] \arrow[dr, "\pi_I"'] & & M' \\
& R/I \arrow[ur, dashed, "\overline{\varphi}"'] &
\end{tikzcd}$$

Beweis. Man sieht, dass

$$\overline{\varphi}(x + I) = \varphi(x) \quad \forall x \in R$$

gelten muss, und das dies auch ein wohldefinierter Ringhomomorphismus ist. □

6. Der Elementarteilersatz

Sei R Hauptidealring.

Definition 6.1
Seien $a, b, x, y \in R$. Für $i, j \in \{1, ..., n\}$ ist

$$E_{ij} = (\delta_{\sigma,i}, ..., \delta_{\mu,j})_{\sigma,\mu} \in \mathrm{Mat}_n(\mathbb{R})$$

Sei

$$E_{ij}(a,b,x,y) = \mathbb{1}_n - E_{ii} - E_{jj} + aE_{ii} + bE_{ij} + xE_{jj} + yE_{ji}$$

Theorem 6.2 (Elementarteilersatz für Matrizen, Smith-Normalform)
Sei $A \in \mathrm{Mat}_{m\times n}(\mathbb{R})$. Es gibt $0 \leq r \leq \min\{n, m\}$, $S \in \mathrm{GL}_m(R)$, $T \in \mathrm{GL}_n(R)$ mit

$$SAT = \begin{pmatrix} d_1 & & & \\ & \ddots & & \\ & & d_r & \\ & & & \mathbb{0} \end{pmatrix}$$

$$\mathbb{0} \in \mathrm{Mat}_{m-r\times n-r}$$

wobei $d_i \in R\backslash\{0\}$ mit $d_i \mid d_{i+1}$ für $i = 1, ..., n-1$

Beweis. Induktion nach $\min\{m, n\}$. Für $a \in R$ sei $\delta(a) \in \mathbb{N}_0 \cup \{\infty\}$ die Anzahl der Primelemente in der Primfaktorzerlegung von a, mit $\delta(0) := \infty$, und $\delta(A) := \min_{ij}\{\delta(a_{ij})\}$. Wir können annehmen, dass $\delta(A) \leq \delta(SAT)$ für alle $S \in \mathrm{GL}_m(R)$ und $T \in \mathrm{GL}_n(R)$. Durch Zeilen- und Spaltenvertauschungen erreichen wir, dass $\delta(a_{11}) = \delta(A)$.

- 1. Behauptung: $a_{11} \mid a_{i1}$ für alle i. Gäbe es ein $i \geq 1$ für dass $a_{11} \nmid a_{i1}$, so sei $c = \mathrm{ggT}(a_{11}, a_{i1}) = xa_{11} + ya_{i1}$ mit $\mathrm{ggT}(x, y) = 1$, also $ax - by = 1$ mit $a, b \in R$. Multiplikation mit $E_{1i}(x, y, a, b)$ von links erzeugt an der Position $(1, 1)$ das Element c, und $\delta(c) < \delta(a_{11}) = \delta(A)$, im Widerspruch zur Minimalität von $\delta(A)$. Analog zeigt man, dass $a_{11} \mid a_{1j}$ für alle j. Durch Zeilen- und Spaltenumformungen können wir deshalb nun $a_{i1} = 0$ für alle $i > 1$ und a_{1j} für alle $j > 1$ erreichen.
- 2. Behauptung: $a_{11} \mid a_{ij}$ für alle i, j. Gäbe es $i > 1$ und $j > 1$ mit $a_{11} \nmid a_{ij} := b$, so können wir die j-te Spalte zur ersten Spalte addieren, was a_{11} nicht ändert und $a_{1i} = b$ bewirkt. Wider können wir Behauptung 1 anwenden und erhalten den Widerspruch, dass $a_{11} \mid b$. Damit ist nach diesem Umformungen

$$A = \begin{pmatrix} a_{11} & \\ & a_{11} \cdot A' \end{pmatrix}$$

mit $A' \in \mathrm{Mat}_{(m-1)\times(n-1)}(R)$. Wir wenden nun die Induktionshypothese auf A' an und sind fertig. □

Satz 6.3 (Elementarteilersatz für Moduln)
Sei R ein Hauptidealring, $M \cong R^m$ ein endlich erzeugter freier R-Modul, $N \subseteq M$ ein Untermodul. Dann existiert $r \in \mathbb{N}$, eine Basis $B' = (x'_1, ..., x'_m)$ von M und $d_1, ..., d_r \in R\backslash\{0\}$ mit $d_i \mid d_{i+1}$ für $i = 1, ..., r-1$ für die $(d_1x'_1, ..., d_rx'_r)$ eine Basis von N ist.

Beweis. Sei $B = (x_1, ..., x_m)$ eine Basis von M. Nach ?? ist N endlich erzeugt, also

$$N = \sum_{j=1}^{n} Ry_j \quad \text{mit} \quad y_j = \sum_{i=1}^{m} a_{ij}x_i \quad a_{ij} \in R$$

Wir betrachten die lineare Abbildung $f : R^n \to M$ gegeben durch $f(e_j) = y_j$. Dann ist $\mathrm{Im}(f) = N$ und

$$M_B^{\mathcal{E}}(f) = A = (a_{ij}) \in \mathrm{Mat}_{m\times n}(R)$$

Nach Theorem 6.2 existieren $S \in \mathrm{GL}_m(R)$, $T \in \mathrm{GL}_n(R)$ mit

$$SAT = D = \mathrm{diag}(d_1, ..., d_r, \mathbb{0})$$

Es gibt somit Basen $\mathcal{E}' = (e'_1, ..., e'_n)$ von R^n, $B' = (x'_1, ..., x'_m)$ von M mit $M_{B'}^{\mathcal{E}'}(f) = D$. Somit ist $N = \mathrm{Im}(f) = \sum_{i=1}^{n} R \cdot f(e'_i) = \sum_{j=1}^{r} Rd_jx'_j$. Da $(x'_1, ..., x'_r)$ frei und R nullteilerfrei ist, ist auch $(d_1x'_1, ..., d_rx'_r)$ frei, also eine Basis von N. □

Theorem 6.4 (Hauptsatz über endlich erzeugte Moduln über Hauptidealringen)
Sei R ein Hauptidealring und M ein endlich erzeugter R-Modul. Dann ist

$$M = F \oplus M_{tor}$$

wobei $F \cong R^r$ ein endlich erzeugter freier R-Modul ist und

$$M_{tor} \cong \bigoplus_{i=1}^{n} {}^{R}/_{Rd_i}$$

mit Nichteinheiten $d_1, ..., d_n \in R \backslash \{0\}$, die $d_i \mid d_{i+1}$ für $i = 1, ..., n-1$ erfüllen.

Beweis. Sei $M = \sum_{j=1}^{m} Ry_j$. Betrachte die lineare Abbildung $f : R^m \to M$ gegeben durch $f(e_j) = y_j$ und dem Untermodul $N = \mathrm{Ker}(f) \subseteq R^m$. Nach Satz 6.3 existiert eine Basis $(x_1, ..., x_s)$ von R^m, $n \leq s$ und $d_1, ..., d_n \in R \backslash \{0\}$ mit $d_i \mid d_{i+1}$ für die $(d_1 x_1, ..., d_n x_n)$ eine Basis von N ist. Nach dem Homomorphiesatz ist

$$\begin{aligned} M = \mathrm{Im}(f) \cong {}^{R^m}/_{N} &= {}^{\bigoplus_{i=1}^{s} Rx_i}/_{\bigoplus_{i=1}^{n} Rd_i x_i} \\ &\cong {}^{R^s}/_{\bigoplus_{i=1}^{n} Rd_i e_i} \\ &\cong \bigoplus_{i=1}^{n} {}^{R}/_{Rd_i} \oplus \underbrace{R^{s-n}}_{F} \end{aligned}$$

Ist $d_i \in R^\times$, so ist ${}^{R}/_{Rd_i} = 0$, wir können diese i daher weglassen. Dabei ist $\bigoplus_{i=1}^{n} {}^{R}/_{Rd_i}$ genau der Torsionsmodul M_{tor}:

- "$\subseteq$": Mit $d := d_1 \cdot ... \cdot d_n \in R \backslash \{0\}$ ist $d \cdot (x_i)_{1,...,n} = (dx_i)_{1,...,n} = (0, ..., 0)$ (Vielfache von Rd_i machen das Element zu 0)
- "$\supseteq$": Ist $d \in R \backslash \{0\}$, $x \in \bigoplus_{i=1}^{n} {}^{R}/_{Rd_i}$, $y \in R^{s-n}$ mit $d \cdot (x, y) = 0$, so ist $d \cdot y = 0$ und deshalb $y = 0$. □

7. Zyklische Vektorräume

Sei K ein Körper, V ein n-dimensionaler K-Vektorraum, $f \in \mathrm{End}_K(V)$.

Folgerung 7.1 (Frobenius-Normalform)
Es gibt eine Basis B von V, für die

$$M_B(f) = \mathrm{diag}(M_{P_1}, ..., M_{P_m})$$

mit $P_1, ..., P_m \in K[t]$ normiert, die $P_i \mid P_{i+1}$ erfüllen.