LAAG I/II - Zusammenfassung

Jan-Cornelius Molnar, Version: 1. Oktober 2008 17:16

1 Allgemeines

- *Eine binäre Operation ist eine Abbildung $B : A \times A \to A$.*

- *Eine nichtleere Menge A zusammen mit einer binären, assoziativen Operation heißt Gruppe, falls ein neutrales Element und zu jedem Element $a \in A$ ein Inverses existiert.*

- *Ist A Gruppe und die Operation außerdem kommutativ, heißt A abelsche Gruppe.*

- *Eine nichtleere Menge $\mathbb{K}$ mit zwei binären Operationen $+$ und $\cdot$ heißt Körper, falls K bezüglich $+$ eine abelsche Gruppe mit neutralem Element 0 und $K \setminus \{0\}$ eine abelsche Gruppe bezüglich $\cdot$ bildet und die Multiplikation distributiv über der Addition ist.*

- *Ein Ring ist eine abelsche Gruppe $(R, +)$ mit einer assoziativen, binären Operation $R \times R \to R, (r, s) \to r \cdot s$ genannt Multiplikation, die auf beiden Seiten distributiv über der Addition ist.*
Hat R ein neutrales Element bezüglich dieser Multiplikation wird er Ring mit Eins genannt. Ein Ring mit kommutativer Multiplikation wird kommutativer Ring genannt.

- *Ein K-Vektorraum ist eine abelsche Gruppe $(V, +)$ mit einer kommutativen skalaren Multiplikation mit Elementen aus K, die distributiv über der Addition ist.*

- *Eine K-Algebra ist ein K-Vektorraum A, der zugleich ein Ring mit Eins ist, sodass gilt*

$$\lambda(ab) = (\lambda a)b = a(\lambda b), \ \forall\ a, b \in A, \lambda \in K.$$

- *Sei A eine K-Algebra oder Ring mit Eins, dann heißt $a \in A$ invertierbar oder Einheit, falls es ein multiplikatives Inverses zu a gibt, d.h. falls es ein Element b in A gibt, sodass $ab = ba = 1_A$ ist. Die Menge der invertierbaren Elemente wird mit $U(A)$ bezeichnet.*

- *Sei $\mathbb{K}$ Körper und $\mathbb{K}[x]$ die Menge der formalen Ausdrücke*

$$f(x) = \sum_{i=0}^{n} \alpha_i x^i,$$

mit $\alpha_i \in \mathbb{K}$. Dann nennt man $f(x)$ Polynom.

2 Vektorräume

- *Seien $U, W \leqslant V$, dann ist die Summe von U und W die Teilmenge*

$$U + W = \{x + y \,:\, x \in U, y \in W\}.$$

- *Zwei Unterräume $U, W \leqslant V$ komplementär, falls*

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

- *Sei $T \subseteq V$, dann ist $\langle T \rangle$ die Menge aller Linearkombinationen von T und heißt linearer Aufspann.*

- *Sei $\emptyset \neq T \subseteq V$, dann heißt T Erzeugendensystem von V, falls $\langle T \rangle = V$.*

- *$\langle \emptyset \rangle = (0) \leqslant V$, für alle V.*

- *Eine Teilmenge T von V heißt linear abhängig, falls es eine nichttriviale Darstellung der 0 mit Vektoren aus T gibt, sonst linear unabhängig.*

- *Ein minimales Erzeugendensystem von V heißt Basis von V.*

- *Eine geordnete Basis von V ist eine Basis $\mathcal{B}$ zusammen mit einer vollständigen Ordnung.*

- *Ist V endlich erzeugt, ist die Anzahl der Elemente einer Basis eindeutig bestimmt. Diese natürliche Zahl heißt Dimension von V und wird mit $\dim_K V$ bezeichnet.*

- Seien $U_i, i \in I$ ein System von K-Vektorräumen. Die direkte Summe der U_i ist definiert als

$$U = \bigoplus_{i \in I} U_i = \{(u_i)_{i \in I} : u_i \in U_i, u_i = 0 \text{ für fast alle } i \in I\}$$

- Sei $U \leqslant V$, dann wird durch $\sim$ eine Äquivalenzrelation auf V definiert

$$v \sim w \Leftrightarrow w - v \in U.$$

Ist $v \sim w$, schreibt man auch $v \equiv w \mod U$.

Die Äquivalenzklassen von $\sim$ heißen Restklassen modulo U und die Klasse, die v enhält, ist

$$\overline{v} = v + U = \{v + u : u \in U\}.$$

2.1 Sätze über unendlich dimensionale Vektorräume

- Ist $T \neq \emptyset$ und $U = \langle T \rangle$, so gilt für $u, v \in U, \lambda \in \mathbb{K}$, dass $u + v \in U$ und $\lambda u \in U$.
- Sei $\emptyset \neq U \subseteq V$, dann ist U genau dann Unterraum von V, falls gilt

$u, v \in U \Rightarrow u - v \in U$

$\lambda \in \mathbb{K}, u \in U \Rightarrow \lambda u \in U.$

- Sei $\emptyset \neq T \subseteq V$, dann ist $\langle T \rangle \leqslant V$ und es gilt

$$\langle T \rangle = \bigcap_{T \subseteq U \leqslant V} U,$$

der kleinste Unterraum von V, der T als Teilmenge enthält.

- Ist $T \subseteq S \subseteq V$, dann ist $\langle T \rangle \subseteq \langle S \rangle \subseteq V$.
- Ist $T \subseteq V$, dann ist $\langle \langle T \rangle \rangle = \langle T \rangle$ und ist $U \leqslant V$, dann ist $\langle U \rangle = U$.
- Seien $U, W \leqslant V$, dann ist $U + W \leqslant V$, der kleinste Unterraum von V, der U und W enthält und $U \cap W \leqslant V$, der größte Unterraum von V, der in U und W enthalten ist.
- Seien $U, W, X \leqslant V$, dann ist

$$U \cap (W + (U \cap X)) = (U \cap W) + (U \cap X).$$

Ist außerdem $X \subseteq U$, so gilt

$$U \cap (W + X) = (U \cap W) + X.$$

- $T \subseteq V$ ist genau dann Erzeugendensystem von V, falls T in keinem echten Unterraum von V enthalten ist.
- Sei T ein Erzeugendensystem für V, dann ist T minimal genau dann, wenn es linear unabhängig ist.
- $T \subseteq V$ ist Basis von V genau dann, wenn wenn T eine maximale linear unabhängige Teilmenge von V ist.
- Sei T Erzeugendensystem von V, dann ist T Basis von V genau dann, wenn sich jeder Vektor in V eindeutig als Linearkombination von Vektoren aus T darstellen lässt.
- Sei $V = U \bigoplus W$, dann ist $\dim_K V = \dim_K U + \dim_K W$.
- Der Faktorraum V/U ist ein Vektorraum.
- Sei $V = U \oplus W$ und $w, w' \in W$, dann ist $w \sim w' \Leftrightarrow w = w'$. Darüber hinaus enthält jede Nebenklasse $v + U = \overline{v}$ genau ein Element $w_v \in W$.

2.2 Sätze, die das Auswahlaxiom erfordern

- Jeder Vektorraum hat eine Basis.
- Jedes Erzeugendensystem enthält eine Basis.
- Jeder Unterraum U von V besitzt ein Komplement.
- Sei $U \leqslant V$, dann lässt sich jede Basis von U zu einer von V ergänzen.

2.3 Sätze für endlichdimensionale Vektorräume

- *Sei $\mathcal{B}$ Erzeugendensystem und $T = \{x_1, \ldots, x_k\}$ eine linear unabhängige Teilmenge von V, dann gibt es eine k-elementige Teilmenge C von $\mathcal{B}$, sodass $(\mathcal{B} \setminus C) \cup T$ den ganzen Raum V aufspannt.*

- *Eine linear unabhängige Teilmenge eines n-dimensionalen Vektorraums hat maximal n Elemente. Sie ist eine Basis genau dann, wenn sie n Elemente hat und linear abhängig, wenn sie aus mehr als n Elementen besteht.*

Dimensionsformel

$$\dim_K(U + W) + \dim_K(U \cap W) = \dim_K U + \dim_K W.$$

$$\dim_K V = \dim_K U + \dim_K V/U.$$

3 Homomorphismen

- *Seien V und W Vektorräume. Eine Abbildung $f : V \to W$ heißt Homomorphismus bzw. linear, falls gilt*

$$f(x + y) = f(x) + f(y), \quad \forall\, x, y \in V,$$
$$f(\lambda x) = \lambda f(x), \quad \forall\, x \in V, \lambda \in K.$$

- *Seien V und W Vektorräume. Ein injektiver Homomorphismus $f : V \to W$ wird Monomorphismus genannt. Ist f linear und surjektiv, spricht man von einem Epimorphismus und ist f bijektiv, von einem Isomorphismus.*

- *Der Kern einer Abbildung $f : V \to W$ ist die Menge*

$$\ker f = f^{-1}(0) = \{v \in V : f(v) = 0\}.$$

- *Das Bild einer Abbildung $f : V \to W$ ist die Menge*

$$\operatorname{im} f = \{w \in W : \exists\, v \in V f(v) = w\}.$$

- *Die Matrix $\mathfrak{M}_f(C, \mathcal{B})$ ist die Zuordnungsvorschrift eines Homomorphismus. Sie gibt an, wie Elemente der Basis $\mathcal{B}$ auf Elemente der Basis C abgebildet werden.*

- *Die Menge der Homomorphismen $f : V \to W$ wird mit $\operatorname{Hom}_K(V, W)$ bezeichnet. Analog dazu $\operatorname{End}_K(V), \operatorname{Aut}_K(V)$.*

- *Die Menge der $m \times n$ Matritzen über K wird mit $M_{m\times n}(K)$ bezeichnet.*

- *Seien A, B Ringe und $f \in \operatorname{Hom}(A, B)$, dann heißt f Antihomomorphismus, falls $f(ab) = f(b)f(a)$.*

- *Äquivalenzrelation*

$$A \approx B \Leftrightarrow \exists\, f \in \operatorname{Hom}_K(V, W) : A, B \in \mathfrak{M}_f(-, -).$$

- *Sei $A \in M_{m\times n}$, dann ist der Spaltenrang von A die Dimension des von den Spaltenvektoren aufgespannten Unterraums des K^m. Analog ist der Zeilenrang von A definiert.*

- *Der Rang einer Matrix A wird mit $\operatorname{rg} A$ bezeichnet.*

3.1 Sätze über Homomorphismen auf Vektorräumen unendlicher Dimension

- *Sei $f : V \to W$ ein Isomorphismus, dann ist $f^{-1} : W \to V$ ebenfalls ein Isomorphismus.*

- *Die Komposition von (Mono-, Epi-, Iso-) Homomorphismen ist (Mono-, Epi-, Iso-) Homomorphismus.*

- *$\operatorname{Hom}_K(V, W)$ und $M_{m\times n}$ sind Vektorräume.*

- *Ein Homomorphismus ist vollständig durch seine Werte auf einem Erzeugendensystem bestimmt. D.h. Sind $f, g : V \to W$, $\langle T\rangle = V$ und $f(t) = g(t)\ \forall\, t \in T$, so gilt $f = g$.*

- *Sei $\mathcal{B}$ Basis von V und sei für jedes $b \in \mathcal{B}$ ein $w_b \in W$ gegeben, dann gibt es genau eine Abbildung $T : V \to W$ mit $T(b) = w_b$.*

- *Sei $f \in \operatorname{Hom}(V, W)$, dann ist $\ker f \leqslant V$ und $\operatorname{im} f \leqslant W$.*

- *Sei $f \in \operatorname{Hom}(V,W)$ und $\mathcal{B}$ Basis von V, dann ist $\langle f(\mathcal{B})\rangle = \operatorname{im} f$.*
- *Sei $U \leqslant V$, dann ist die Abbildung $T : V \to V/U : v \to \overline{v}$ ein Epimorphismus.*
- *Sei $f \in \operatorname{Hom}_K(V,W)$, dann ist f injektiv genau dann, wenn* $\ker f = (0)$.

1. Isomorphiesatz *Sei $f \in \operatorname{Hom}_K(V,W)$ und sei $U \leqslant \ker f$, dann faktorisiert f eindeutig über V/U.*

$$\begin{tikzcd}
V \arrow[rr, "f"] \arrow[dr, "\pi"'] & & W \\
& V/U \arrow[ur, "\exists ! \tilde{f}"'] &
\end{tikzcd}$$

- *Sei $f \in \operatorname{Hom}_K(V,W)$, dann induziert f einen Monomorphismus $\tilde{f} : V/\ker f \to W$. Insbesondere gilt $V/\ker f \cong \operatorname{im} f$.*
- *Sei $f \in \operatorname{Hom}_K(V,W)$ und sei $X \leqslant W$, dann ist $f^{-1}(X) = \{v \in V : f(v) \in X\}$ ein Unterraum von V, der $\ker f$ enthält.*
  Ist darüber hinaus $X \leqslant \operatorname{im} f$, so ist $f^{-1}(X)/\ker f \cong X$ und $X \to f^{-1}(X)$ definiert eine inklusionserhaltende Bijektion.

2. Isomorphiesatz *Seien $U, W \leqslant V$, dann ist $(U+W)/U \cong W/(U \cap W)$.*

3. Isomorphiesatz *Seien $U \leqslant W \leqslant V$, dann ist $W/U \leqslant V/U$ und es gilt*

$$(V/U)/(W/U) \cong V/W.$$

3.2 Sätze über Homomorphismen auf Vektorräumen endlicher Dimension

V, W seien endlich erzeugt mit $\dim_K V = n$ und $\dim_K W = m$ und $f, g \in \operatorname{Hom}_K(V,W)$.

- *Die Abbildung*

$$\mathfrak{M}\_(C,\mathcal{B}) : \operatorname{Hom}_K(V,W) \to M_{m\times n}(K), f \mapsto, \mathfrak{M}_f(C,\mathcal{B})$$

ein Isomorphismus mit Umkehrabbildung

$$f\_(C,\mathcal{B}) : M_{m\times n}(K) \to \operatorname{Hom}_K(V,W,A \to f_A(C,\mathcal{B}).$$

- *Seien $\mathcal{M}$ und $\mathcal{N}$ endlichen Mengen derselben Mächtigkeit und sei $f : \mathcal{M} \to \mathcal{N}$, dann ist f injektiv genau dann wenn f surjektiv ist.*
- *f ist genau dann Monomorphismus, wenn f Epimorphismus ist.*
- *Zwei Vektorräume sind isomorph genau dann, wenn sie dieselbe Dimension über K haben.*
- *Es gilt* $\dim_K M_{m\times n} = \dim_K \operatorname{Hom}_K(V,W) = mn$.
- *Es ist $\mathfrak{M}_f(-,-) = GL_m(K)\mathfrak{M}_f(\mathcal{B},\mathcal{A})GL_n(K)$ für jede Wahl von Basen $\mathcal{A}$ und $\mathcal{B}$.*
- *Es gilt entweder*

$$\mathfrak{M}_f(-,-) \cap \mathfrak{M}_g(-,-) = \varnothing \quad \textit{oder} \quad \mathfrak{M}_f(-,-) = \mathfrak{M}_g(-,-).$$

- *Sind $A, B \in M_{m\times n}$, dann ist $A \approx B$ genau, dann wenn $X \in GL_m(K)$ und $Y \in GL_n(K)$ existieren, sodass $B = XAY$.*
- *Sei $f \in \operatorname{Hom}_K(C,\mathcal{B})$ und $A = \mathfrak{M}_f(C,\mathcal{B})$. Seien $s_1, \ldots, s_n$ die Spaltenvektoren von A, dann ist* $\operatorname{im} f = \langle s_1, \ldots, s_n\rangle$.
- *Spaltenrang und Zeilenrang stimmen überein.*
- *Alle Matritzen in $\mathfrak{M}_f(-,-)$ denselben Spaltenrang und dieser entspricht* $\dim_K \operatorname{im} f$.
- *Ist $\operatorname{rg} f = k$, so ist $E_{m\times n}(k)$ in $\mathfrak{M}_f(-,-)$ enthalten.*
- *Es gilt* $\dim_K \operatorname{im} f + \dim_K \ker f = \dim_K V$.
- *Unter elementaren Operationen bleibt der Rang einer Matrix erhalten.*

- *Sei $A \in M_{m\times n}$, dann gibt es eine Reihe von elementaren Operationen, die $E_{m\times n}(k)$ erzeugen mit $k = \operatorname{rg} A$.*

- *Sei $A \in M_{m\times n}$, dann ist $\operatorname{rg} A = \operatorname{rg} A^t$.*

4 Multilineare Abbildungen

- *Eine Abbildung $f : V_1 \times \ldots \times V_k \to W$ heißt k-fach multilinear, wenn sie in jeder Komponente K-linear ist. Ist $W = K$ und $V_1 = \ldots = V_n$, so heißt f Multilinearform.*

- *Seien $I_1 = \{1,\ldots,n_1\}, I_2 = \{1,\ldots,n_2\},\ldots,I_k = \{1,\ldots,n_k\}$ endliche Indexmengen, dann wird $\underline{i} \in I_1 \times I_2 \times \ldots \times I_k$ Multiindex genannt.*

  (a) *Für $\underline{i},\underline{j} \in \mathbb{N}^{\times k}$ ist $\delta_{\underline{i},\underline{j}} = \prod_{l=1}^{k} \delta_{i_l,j_l}$*

  (b) *Für $\pi \in \sigma_k$ ist $\pi(\underline{i}) = (i_{\pi(1)},\ldots,i_{\pi(k)})$.*

  (c) *$e_{\underline{j}} : V^{\times k} \to K, v_{\underline{i}} \mapsto \delta_{\underline{j},\underline{i}}$.*

- *Sei $(w_1,\ldots,w_m)$ Basis von W, $\underline{i}$ Multiindex und $1 \le j \le m$, dann wird druch*

$$f_{\underline{i},j} : V_1 \times \ldots \times V_k \to W, v_{\underline{k}} \mapsto \begin{cases} w_j & \text{falls } \underline{i} = \underline{k}, \\ 0 & \text{sonst,} \end{cases}$$

eine multilineare Abbildung definiert.

- *Eine k-fache Linearform $f : V^{\times k} \to K$ heißt symmetrisch, falls $f(v_{\underline{i}}) = f(v_{\pi(\underline{i})})$ für jedes $\pi \in \sigma_k$.*

- *Eine k-fache Linearform $f : V^{\times k} \to K$ heißt alternierend, falls $f(u_1,\ldots,u_k) = 0$ für jedes linear abhängige Tupel $(u_1,\ldots,u_k)$.*

- *Die Menge der alternierenden k-fachen Linearformen auf V wird mit $\mathcal{A}_k(V)$ bezeichnet.*

4.1 Sätze für Multilinearformen

Sei V endlich dimensional mit $\dim_K V = n$ und Basis $\mathcal{B} = \{v_i \in V : 1 \le i \le n\}$.

- *Die Menge M der multilinearen Abbildungen $f : V_1 \times \ldots \times V_k \to W$ ist ein K-Vektorraum.*

- *Sei f multilinear, dann ist M endlichdimensional und es gilt*

$$\dim_K M = \prod_{i=1}^{k} \dim_K V_i \dim_K W.$$

- *$\mathcal{B} = \left\{f_{\underline{i},j} : \underline{i} \text{ Multiindex}, 1 \le j \le m\right\}$ ist eine Basis von M.*

- *Sei $0 \ne f : V^{\times n} \to K$ und $v_1,\ldots,v_n \in V$, dann ist $\mathcal{B} = (v_1,\ldots,v_n)$ Basis von V genau dann, wenn $f(\mathcal{B}) \ne 0$ ist.*

- *$\mathcal{A}_k(V)$ ist ein K-Unterraum von M.*

- *Sei $\underline{i} \in \mathbb{N}^{\times k}$ mit $1 \le i_1 < \ldots < i_k \le n$ und seien $u_1,\ldots,u_k \in V$ und $\pi \in \sigma_k$, dann ist $e_{\underline{i}}(u_{\pi(1)},\ldots,u_{\pi(k)}) = e_{\pi^{-1}(\underline{i})}(u_1,\ldots,u_k)$.*

- *$\left\{e_{\underline{j}} : \underline{j} \in \{1,\ldots,n\}^{\times k}\right\}$ ist Basis des Vektorraums aller k-fachen Multilinearformen auf V.*

- *Sei $a_{\underline{i}} = \sum_{\pi \in \sigma_k} (\operatorname{sign} \pi) e_{\pi(i)}$, dann ist $\left\{a_{\underline{i}} : \underline{i} = (i_1,\ldots,i_n) \in \mathbb{N}^{\times k}, 1 \le i_1 < \ldots < i_k \le n\right\}$ Basis von $\mathcal{A}_k(V)$.*

- *$\dim_K \mathcal{A}_k(V) = \binom{n}{k}$.*

- *Sei $f \in \mathcal{A}_n(V)$ und $u_i = \sum_{j=1}^{n} \lambda_{ij} v_j$ für $\lambda_{ij} \in K$, so ist*

$$f(u_1,\ldots,u_n) = \sum_{\pi \in \sigma_n} (\operatorname{sign} \pi) \prod_{i=1}^{n} \lambda_{i\pi(i)} f(v_1,\ldots,v_n) = \det(\lambda_{ij}) f(v_1,\ldots,v_n).$$

5 Endomorphismen

- *Eine lineare Abbildung $f : V \to V$ bezeichnet man als Endomorphismus. Ist f außerdem bijektiv, heißt f Automorphismus.*

- *Die Einheitengruppe $U(M_n(K))$ der K-Algebra $M_n(K)$ wird mit $GL_n(K)$ bezeichnet.*

- *Die Determinante* $\det A$ *einer Matrix A ist definiert als*

$$\det A = \sum_{\pi \in \sigma_n} \operatorname{sign}(\pi) \prod_{i=1}^{n} \alpha_{i\pi(i)}.$$

- *Die Determinante von $\phi \in \mathrm{End}_K(V)$ ist mit einer beliebigen $0 \neq f \in \mathcal{A}_n(V)$ definiert als*

$$\det \phi = \frac{f(\phi(v_1), \ldots, \phi(v_n))}{f(v_1, \ldots, v_n)},$$

wobei $\mathcal{B} = \{v_1, \ldots, v_n\}$ irgendeine Basis von V ist.

- *Ist $f \in \mathrm{End}_K(V)$, dann ist $\det f = \det \mathfrak{M}_f(\mathcal{B}, \mathcal{B})$ für eine beliebige Basis $\mathcal{B}$.*

- *Die spezielle lineare Gruppe ist die Menge aller $n \times n$ Matrizen mit Determinante 1 und wird mit $SL_n(K)$ bezeichnet.*

- *Zwei Matrizen heißen ähnlich, falls es eine invertierbare $n \times n$-Matrix P mit $B = P^{-1}AP$ gibt. Man schreibt $A \sim B$ und sagt A und B sind konjugiert in $GL_n(K)$.*

- *Die Adjunkte einer $n \times n$-Matrix $A = (\alpha_{ij})$ ist die $n \times n$-Matrix*

$$\operatorname{adj} A = \left((-1)^{j+i} \det A_{ji}\right)_{ij}$$

- *Die Summe der Diagonalenelemente einer Matrix A heißt Spur* $\operatorname{tr} A$.

5.1 Sätze für endliche Dimension

V, W seien endlich erzeugt mit $\dim_K V = n$ und $\dim_K W = m$ und $f, g \in \mathrm{Hom}_K(V, W)$.

- $\mathrm{End}_K(V)$ *mit der Komposition als Multiplikation und $M_n(K)$ mit der Matritzenmultiplikation sind K-Algebren.*

- *Sind A, B Ringe und $f : A \to B$ ein Ringhomomorphismus, so ist $f(U(A)) \subseteq U(B)$ und die Einschränkung $f|_{U(A)}$ ist ein Gruppenhomomorphismus. Ist f Isomorphismus, so auch $f|_{U(A)}$.*

- *Transponieren ist ein Antiautomorphismus. Seine Einschränkung auf invertierbare Matritzen ist ein Antiautomorphismus auf $GL_n(K)$ und es gilt*

$$(A^t)^{-1} = (A^{-1})^t, \text{ für } A \in GL_n(K).$$

5.2 Sätze für Endomorphismen

- *Sei $A \in M_n$, dann ist A genau dann invertierbar, wenn* $\operatorname{rg} A = n$ *ist.*

- *Jede invertierbare Matrix ist das Produkt von Elementarmatritzen.*

- *Sei $\phi \in \mathrm{End}_K(V)$, dann ist* $\det \phi$ *unabhängig von der Wahl der Basis $\mathcal{B}$ von V und unabhängig von der Wahl der Form $f \neq 0 \in \mathcal{A}_n(V)$.*

- *Seien $\phi, \psi \in \mathrm{End}_K(V)$, dann gilt*

  (a) $\det(\phi) \neq 0 \Leftrightarrow \phi \in \mathrm{Aut}_K(V)$.

  (b) $\det(\mathrm{id}) = 1$.

  (c) $\det(\phi \circ \psi) = \det(\phi)\det(\psi)$.

  (d) $\det(\phi^{-1}) = (\det(\phi))^{-1}$ *für* $\phi \in \mathrm{Aut}_K(V)$.

  (e) *Die Einschränkung* $\det : \mathrm{Aut}_K(V) \to K \setminus \{0\}$ *ist Gruppenhomomorphismus.*

- *Analoges gilt für Matritzen $A, B \in M_n(K)$*

  (a) $\det A = \det A^t$.

(b) $\det(AB) = \det A \det B$.

(c) $\det E = 1$.

(d) $\det(A^{-1}) = \frac{1}{\det A}$.

(e) *A invertierbar* $\Leftrightarrow \det A \neq 0$.

(f) *Hat A Nullspalte oder -zeile, gilt* $\det A = 0$.

(g) *Sind zwei Spalten/Zeilen in A linear abhängig ist* $\det A = 0$.

- *Für Diagonal-, obere und untere Dreiecksmatrizen ist die Determinante das Produkt der Diagonalelemente.*

- *Ist $A \sim B$, so gilt* $\det A = \det B$.

Laplace Entwicklung *Sei $k \in \{1, \ldots, n\}$ und $A = (\alpha_{ij})$ eine $n \times n$ Matrix mit Kofaktoren A_{ij}, dann ist*

$$\begin{aligned} \det A &= \sum_{i=1}^{n} (-1)^{i+k} \alpha_{ik} \det A_{ik} && \textit{Entwicklung nach der } k\textit{-ten Spalte} \\ &= \sum_{j=1}^{n} (-1)^{k+j} \alpha_{kj} \det A_{kj} && \textit{Entwicklung nach der } k\textit{-ten Zeile} \end{aligned}$$

- $A(\operatorname{adj} A) = \det A E_n$.

6 Lineare Gleichungssysteme

- *Ein lineares Gleichungssystem hat die Form $\mathfrak{B} : Ax = b$. Ist b der Nullvektor, so heißt das System homogen, andernfalls inhomogen. Falls $b \neq 0$, so heißt $\mathfrak{H} : Ax = 0$ das zu $\mathfrak{B}$ gehörende homogene System.*

6.1 Sätze zur Lösbarkeit von LGSn

- *Die Lösungsgesamtheit von $\mathfrak{H}$ ist* $\ker f_A$.

- *$\mathfrak{H}$ besitzt genau dann nichttriviale Lösungen, wenn f_A nicht injektiv ist.*

- *Für die Lösungsgesamtheit $\mathfrak{L}_{\mathfrak{H}}$ des homogenen Gleichungssystems gilt $\mathfrak{L}_{\mathfrak{H}} \leqslant K^n$ mit* $\dim_K \mathfrak{L}_{\mathfrak{H}} = n - \operatorname{rg} A$.

- *Ist $m < n$, so besitzt $\mathfrak{H}$ nichttriviale Lösungen.*

- *Für $A \in M_{m \times n}$ und $\mathfrak{B} : Ax = b$ sind folgenden Aussagen äquivalent*

  (a) *$\mathfrak{B}$ besitzt eine Lösung,*

  (b) $b \in \operatorname{im} f_A$,

  (c) $\operatorname{rg} A = \operatorname{rg} A|b$.

- *Ist x_0 beliebige Lösung von $\mathfrak{B}$, dann ist die Gesamtheit der Lösungen* $x_0 + \ker f_A$.

- *Ist $\operatorname{rg} A = \operatorname{rg} A|b = n$, so bestitzt $\mathfrak{B}$ eine eindeutige Lösung.*

- *Sei $A \in M_n(K)$, dann so besitzt $\mathfrak{B}$ eine eindeutige Lösung, falls A invertierbar ist.*

- *Sei $A \in M_n(K)$, dann so besitzt $\mathfrak{B}$ eine eindeutige Lösung, falls $\det A \neq 0$ ist. Diese ist gegeben durch*

$$x_j = \frac{1}{\det A} \sum_{i=1}^{n} \beta_i (-1)^{i+j} \det A_{ij}.$$

7 Eigenwerte

- *Sei $U \leqslant V$ und $f \in \operatorname{End}_K(V)$, dann heißt f U invariant, falls für alle $u \in U$ gilt $f(u) \in U$.*

- *Ein Vektor $0 \neq v \in V$ heißt Eigenvektor zum Eigenwert $\lambda \in K$, falls $f(v) = \lambda v$.*

- *Eine Diagonalmatrix mit den Diagonaleinträgen $\lambda_1, \ldots, \lambda_n$ wird mit $\operatorname{diag}\{\lambda_1, \ldots, \lambda_n\}$ bezeichnet.*

- *Für t beliebig, ist $(-1)^n \det(f - l_t)$ ein Polynom $\chi_f(t) \in K[t]$ der Form*

$$\chi_f(t) = t^n + \beta_{n-1} t^{n-1} + \ldots + \beta_0,$$

und wird als charakteristisches Polynom bezeichnet.

- *Die Eigenvektoren von f zum Eigenwert λ bestehen aus $\ker(f - l_\lambda) \setminus \{0\}$. Der Unterraum $\ker(f - l_\lambda)$ von V wird Eigenraum genannt und mit $V_\lambda(f)$ bezeichnet.*

7.1 Sätze für endlichdimensionale Vektorräume

Sei V ein Vektorraum mit $\dim_K V = n$ und $f \in \mathrm{End}_K(V)$.

- *Sei $\mathcal{B} = (v_1, \ldots, v_n)$ geordnete Basis von V, dann ist $\mathfrak{M}_f(\mathcal{B}) = \mathrm{diag}\,\{\lambda_1, \ldots, \lambda_n\}$, genau dann, wenn v_i EV zum EW λ_i ist.*
- *Sei $\mathcal{B}$ beliebige Basis von V, dann ist $\mathfrak{M}_{l_\lambda} = \lambda E_n$.*
- *λ ist genau dann Eigenwert von f, wenn $\det(f - l_\lambda) = 0$.*
- *Ähnliche Matritzen haben dasselbe charakteristische Polynom.*
- *Es gilt $\beta_0 = (-1)^n \det f$ und $-\beta_{n-1} = \mathrm{tr}\, f$.*
- *Die Abbildung $\mathrm{tr} : \mathrm{End}_K(V) \to K$ ist ein Homomorphismus und für $f, g \in \mathrm{End}_K(V)$ gilt $\mathrm{tr}(fg) = \mathrm{tr}(gf)$.*
- *Die Eigenwerte von f sind genau die Nullstellen von $\chi_f(t)$.*
- *Die Dimension des Eigenraums $V_\lambda(f)$ ist kleiner gleich der Vielfachheit von λ als Nullstelle von $\chi_f(t)$.*
- *Eine quadratische Matrix A ist genau dann zu einer Dreiecksmatrix ähnlich, wenn $\chi_A(t)$ in Linearfaktoren zerfällt.*
- *Eigenvektoren zu paarweise verschiedenen Eigenräumen sind linear unabhängig.*
- *Eine Matrix A ist genau dann diagonalisierbar, wenn V eine Basis bestehenden aus Eigenvektoren von A besitzt.*
- *f ist genau dann diagonalisierbar, wenn*

$$\sum_{i=1}^{k} \dim V_{\lambda_i}(f) = n.$$

- *Ist A eine obere Blockmatrix, gilt $\det A = \prod_{i=1}^{k} \det A_i$, sowie $\chi_A(t) = \prod_{i=1}^{k} \chi_{A_i}(t)$.*

8 Euklidische und Unitäre Vektorräume

- *Eine Norm auf einem Vektorraum V ist eine Abbildung*

$$\|\cdot\| : V \to \mathbb{R},$$

mit den Eigenschaften

(a) *$\|x\| \geq 0$ für alle $x \in V$ und $\|x\| = 0$, wenn $x = 0$.*

(b) *$\|\lambda x\| = |\lambda|\,\|x\|$ für alle $x \in V, \lambda \in \mathbb{K}$.*

(c) *$\|x + y\| \leq \|x\| + \|y\|$ für alle $x, y \in V$.*

- *Ein Skalarprodukt ist eine symmetrische, homogene, postiv definite Bilinearform.*
- *Eine hermitische Form ist eine Abbildung $\langle \cdot, \cdot \rangle : V \times V \to \mathbb{C}$ mit den Eigenschaften*

(a) *$\langle x + y, z \rangle = \langle x, z \rangle + \langle y, z \rangle$,*

(b) *$\langle \lambda x, y \rangle = \lambda \langle x, y \rangle$,*

(c) *$\langle x, y \rangle = \overline{\langle y, x \rangle}$.*

- *Zwei Vektoren $x, y \in V$ heißen orthogonal, falls $\langle x, y \rangle = 0$ ist.*
- *Ein orthonormales System ist eine eine nichtleere Teilmenge von V deren Elemente verschieden vom Nullvektor und jeweils paarweise orthogonal sind. Ein orthonormales System, das V erzeugt, heißt Orthonormalbasis (ONB).*

- *Eine Abbildung $f \in \mathrm{Hom}_{\mathbb{R}}(V,W)$ heißt orthogonale Abbildung, falls*

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

- *Eine Abbildung $f \in \mathrm{Hom}_{\mathbb{C}}(V,W)$ heißt unitär, falls*

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

- *Ein orthogonaler Isomorphismus heißt Isometrie.*
- *Eine Matrix A heißt unitär (orthogonal), falls $A^{-1} = A^*$ ($A = A^{-1}$).*
- *Eine Matrix A heißt hermitsch (symmetrisch), falls $A = A^*$ ($A = A^t$).*
- *Eine Matrix A heißt normal, falls $AA^* = A^*A$.*
- *Zwei Endomorphismen $f, g \in End_K(V)$ heißen orthogonal äquivalent, falls es einen orthogonalen Automorphismus p von V mit $g = p^{-1} \circ f \circ p$ gibt.*
- *Die zu einer Matrix A adjungierte Matrix wird mit $A^* = \overline{A}^t$ bezeichnet.*
- *Der zu $f \in \mathrm{End}_{\mathbb{C}}(V)$ adjungierte Endomorphismus ist definiert als*

$$f^*(v_j) = \sum_{i=1}^{n} \overline{\alpha_{ji}} v_i.$$

8.1 Sätze für unendlich dimensionale Vektorräume

Seien V ein Vektorraum höchstens abzählbarer Dimension, $\mathcal{B}$ eine geordnete Basis von V und $\mathcal{E}$ die natürliche Basis.

- *Ein System orthogonaler Vektoren ist linear unabhängig.*

Gram-Schmidt *Für $k \leq n$ sei $\mathcal{B}_k = (v_1, \ldots, v_k)$ und $U_k = \langle \mathcal{B}_k \rangle$. Dann ist $\mathcal{E}_k = (e_1, \ldots, e_k)$ eine ONB von U_k und $\mathcal{E}$ ist eine ONB von V. Die Basiswechselmatrix $\mathfrak{M}_{\mathrm{id}_V}(\mathcal{B}_k, \mathcal{E}_k)$ ist eine obere Dreiecksmatrix mit postivier Determinante.*

- *Sei $x \in V$, dann ist $x = \sum_i \langle x, e_i\rangle e_i$.*
- *Seien $M, N \leqslant V$, M und N orthogonal, so ist $M \cap N = (0)$. Ist M endlichdimensional, so ist $V = M \bigoplus M^{\perp}$.*
- *Ist $W \leqslant V$ endlich dimensional mit orthonormaler Basis $(e_1, \ldots, e_k)$ und ist $y \in V$, dann gibt es genau ein $z \in W^{\perp}$ mit*

$$y = \sum_{i=1}^{k} \langle y, e_i\rangle e_i + z.$$

Der Vektor $y_1 = \sum_{i=1}^{k} \langle y, e_i\rangle e_i$ ist der eindeutig bestimmte Vektor von W, der y am nächsten ist, d.h.

$$||y - u|| \geq ||y - y_1||\,,\ \forall\ u \in U.$$

- *Ist $W \leqslant V$, so ist $\dim_K V = \dim_K W + \dim_K W^{\perp}$.*
- *Ist $M \leqslant M$, so ist $(M^{\perp})^{\perp} = M$.*

8.2 Sätze für endliche Dimension

- *Seien $x, y \in V$ Eigenvektoren zu verschiedenen Eigenwerten λ, μ, dann gilt $x^t y = 0$.*

8.3 Sätze für unendlich dimensionale Vektorräume $\mathbb{C}^n$

- *Sei W beliebiger Vektorraum und $f \in \mathrm{Hom}_{\mathbb{C}}(V,W)$, dann sind folgende Aussagen äquivalent*

(a) *f ist unitären (bzw. orthogonale) Abbildung.*

(b) $\|x\| = 1 \Rightarrow ||f(x)|| = 1$.

(c) $\|x\| = ||f(x)||$.

(d) *Ist $\mathcal{E}$ ein orthonormales System, dann ist $f(\mathcal{E})$ ein ebensolches.*

(e) *Es gibt eine ONB $\mathcal{B}$ von V, sodass $f(\mathcal{B})$ ein orthonormales System ist.*

- *Eine unitäre Abbildung ist injektiv. Gilt darüber hinaus* $\dim V = \dim W$*, so ist* f *Isometrie.*

- *Die Menge der Isometrien eines unitären Vektorraums* V *in sich ist eine Untergruppe der* $GL_{\mathbb{C}}(V)$*, die orthogonale Gruppe* $O_{\mathbb{C}}(V)$*.*

8.4 Sätze für endliche Dimension im $\mathbb{C}^n$

- *Sei* $f : V \to \mathbb{C}^n : \sum_{i=1}^n \alpha_i x_i \mapsto (\alpha_1, \ldots, \alpha_n)$*, dann ist* f *Isometrie.*

- *Sie* A *eine Matrix, dann ist die natürliche Basis von* V *orthonormal und* f_A *eine unitäre Abbildung genau dann, wenn* A *unitäre Matrix ist.*

- *Sei* $\mathcal{E}$ *eine ONB von* V*, dann ist* $\mathcal{B}$ *genau dann eine ONB, wenn* $MaM_{\mathrm{id}_V}(\mathcal{E}, \mathcal{B})$ *unitär ist.*

- *Die Spalten- bzw. Zeilenvektoren einer komplexen* $n \times n$ *Matrix bilden genau dann eine orthonormale Basis von* $\mathbb{C}^n$*, wenn*

$$AA^* = A^*A = E_n \Leftrightarrow A^{-1} = A^*.$$

- *Für* $A, B \in M_n(\mathbb{C})$ *gilt*

(a) $A^{**} = A$

(b) $(A + B)* = A^* + B^*$

(c) $(\lambda A)^* = \overline{\lambda} A^*$

(d) $(AB)^* = B^* A^*$

- *Unitäre und hermitische Matritzen sind normal.*

- *Sei* $f \in \mathrm{End}_{\mathbb{C}}(V)$*, dann ist* f *unitär genau dann, wenn* $\mathfrak{M}_f(\mathcal{B}, \mathcal{B})$ *für jede ONB* $\mathcal{B}$ *unitäre Matrix ist.*

- *Sei* $f \in \mathrm{End}_{\mathbb{C}}(V)$ *und seien* $x, y \in V$*, dann ist* $\langle f(x), f(y) \rangle = \langle x, f^*(y) \rangle$*.*

- *Sei* $f \in \mathrm{End}_{\mathbb{C}}(V)$*, dann ist* f *normal genau dann, wenn*

$$\langle f(x), f(y) \rangle = \langle f^*(x), f^*(y) \rangle .$$

- *Sei* $f \in \mathrm{End}_{\mathbb{C}}(V)$ *normal und* x *sei Eigenvektor zum Eigenwert* λ*, dann ist* $f^*(x) = \overline{\lambda} x$*. Insbesondere ist* $V_\lambda(f) = V_{\overline{\lambda}}(f^*)$*.*

Hauptachsentheorem *Jede normale Matrix* $A \in M_n(\mathbb{C})$ *ist unitär-äquivalent zu einer Diagonalmatrix.*

- *Sei* $f \in \mathrm{End}_{\mathbb{C}}(V)$ *hermitisch, dann sind alle Eigenwerte von* f *reell und* V *hat eine ONB bestehend aus Eigenvektoren von* f*.*

- *Sei* A *eine hermitisch, dann sind die Eigenvektoren zu verschiedenen Eigenwerten paarweise orthogonal.*

- *Die Determinante einer unitären (orthogonalen) Abbildung* f_A *ist* ± 1*.*

8.5 Sätze für unendlich dimensionale Vektorräume $\mathbb{R}^n$

- *Die Menge der Isometrien eines euklidischen Vektorraums* V *in sich ist eine Untergruppe der* $GL_{\mathbb{R}}(V)$*, die orthogonale Gruppe* $O_{\mathbb{R}}(V)$*.*

8.6 Sätze für endliche Dimension im $\mathbb{R}^n$

Hauptachsentheorem *Jede relle symmetrische* $n \times n$ *Matrix ist orthogonal äquivalent zu einer Diagonalmatrix.*

- *Die Eigenwerte symmetrischer Matritzen sind alle reell.*

- *Sei* A *eine relle symmetrische Matrix, dann besitzt* $\mathbb{R}^n$ *eine Basis aus Eigenvektoren von* A*.*

9 Körper

- *Sei K Körper, dann heißt $F \subseteq K$ Unterkörper, falls F mit Addition und Multiplikation von K eingeschränkt auf F wieder einen Körper bildet.*
- *Sei K ein Körper. Den kleinsten Unterkörper von K nennt man Primkörper von K.*
- *Sei K ein Körper. Die Charakteristik $\operatorname{char}(K)$ von K ist definiert als*

  (a) $\operatorname{char}(K) = p$, *falls p die kleinste natürliche Zahl ist mit $\sum_{i=1}^{p} 1_K = 0_K$.*

  (b) $\operatorname{char}(K) = 0$, *falls es keine solche Zahl gibt.*

9.1 Sätze über Körper

- *Seien $0 < p, q \in \mathbb{Z}$ und $d \in \mathbb{N}$ ihr größter gemeinsamer Teiler, dann gibt es $a, b \in \mathbb{Z}$ sodass gilt*

$$ap + bq = d.$$

- *Ist K Unterkörper von F, dann ist $1_F = 1_K$ und $0_F = 0_K$.*
- *Sei K ein Körper, dann besitzt K einen kleinsten Unterkörper bezüglich $\subseteq$.*
- *Die Körper $\mathbb{Q}$ und $\mathbb{Z}/(p)$ besitzten keine echten Unterkörper.*

9.2 Sätze über endliche Kröper

- *$\mathbb{Z}/(n)$ ist genau dann ein Kröper, wenn n eine Primzahl ist.*
- $|GL_n(\mathbb{Z})| = \prod_{i=0}^{n-1} (q^n - q^i)$.
- *Ist $\operatorname{char}(K) \neq 0$, so ist $\operatorname{char}(K)$ prim.*
- *Ist $\operatorname{char}(K) = 0$, dann ist der Primkörper von K isomorph zu $\mathbb{Q}$.*
- *Ist $\operatorname{char}(K) = p$, dann ist der Primkörper von K isomorph zu $\mathbb{Z}/(p)$.*
- *Ist K endlicher Körper, so existiert eine Primzahl p und ein $n \in \mathbb{N}$, sodass $|K| = p^n$.*

10 Dualraum

- *Der Vektorraum $\operatorname{Hom}_K(V, K)$ wird mit V^* bezeichnet und der zu V duale Raum genannt.*
- *Sei $\mathcal{B} = \{v_i : i \in \mathcal{I}\}$ Basis von V, dann ist die Linearform $v_i^* \in V^*$ gegeben durch*

$$v_i^*(v_j) = \delta_{ij}.$$

- *Sei $U \leqslant V$, dann ist*

$$U^\perp = \{f \in V^* : f(U) = (0)\},$$

ein Unterraum von V^*, das duale Komplement von U in V^*.

10.1 Sätze für unendlich dimensional

- *Sei $f \in \operatorname{Hom}_K(V, U)$, dann wird durch*

$$f^* : U^* \to V^*, h \mapsto f^*(h) = h \circ f \in V^*,$$

ein Homomorphismus definiert.

10.2 Sätze für endlich dimensional

Sei V endlich dimensional mit $\dim_K V = n$ und Basis $\mathcal{B} = \{v_i \in V : 1 \leq i \leq n\}$.

- *$\mathcal{B}^* = \left\{v_i^* \in V : 1 \leq i \leq n\right\}$ ist eine Basis von V^*, insbesondere sind V und V^* isomorph. Der Isomorphismus*

$$^* : V \to V^*, \sum_{i=1}^{n} \lambda_i v_i \mapsto \sum_{i=1}^{n} \lambda_i v_i^*,$$

hängt dabei ganz wesentlich von $\mathcal{B}$ ab.

- *Sei $f \in V^*$, dann ist $f = \sum_i f(v_i)v_i^*$.*
- *Ist $(v_1, \ldots, v_k)$ Basis von U, dann ist $(v_{k+1}^*, \ldots, v_n^*)$ Basis von $U^\perp$. Insbesondere gilt*

$$\dim_K U^\perp = \dim_K V - \dim_K U.$$

- *Sei $v \in V$. Definiere*

$$f_v : V^* \to K, f_v(x) = x(v),$$

dann ist $f_v \in V^{**}$ ein Homomorphismus. Die Abbildung

$$\mathcal{E} : V \to V^{**}, v \mapsto f_v,$$

ist ein Isomorphismus.

- *Ist $b \in B$, dann gilt $b^{**} = f_b$.*
- *Sei $f \in \mathrm{Hom}_K(V,U)$ und $f^* \in \mathrm{Hom}_K(U^*,V^*)$ der zugehörige Homomorphismus, dann gilt*

(a) $\ker f^* = (\mathrm{im}\, f)^\perp$.

(b) $\dim_K(\mathrm{im}\, f) = \dim_K(\mathrm{im}\, f^*)$.

(c) *f^* ist surjektiv $\Leftrightarrow$ f ist injektiv*

(d) *f^* ist injektiv $\Leftrightarrow$ f ist surjektiv*

(e) *Das Diagramm kommutiert*

$$\begin{tikzcd} V \arrow[r, "f"] \arrow[d, "**"'] & U \arrow[d, "**"] \\ V^* & U^* \arrow[l, "f^{**}"'] \end{tikzcd}$$

(f) *Ist $g \in \mathrm{Hom}_K(U,W)$, dann gilt $(g \circ f)^* = f^* \circ g^*$.*

- *Sei $f \in \mathrm{Hom}_K(V,U)$ und $C = \{u_i : 1 \le i \le m\}$ Basis von u. Sei $A = \mathfrak{M}_f(C, \mathcal{B})$, dann ist $\mathfrak{M}_{f^*}(\mathcal{B}^*, C^*) = A^t$.*

11 Bilinearformen

- *Sei $\mathcal{B} = \{v_i \in V : i \in \mathcal{I}\}$ Basis von V und sei $f : \langle\cdot,\cdot\rangle : V \times V \to K$ eine Bilinearform, dann ist f durch die Angabe der Skalare $\lambda_{ij} = \left\langle v_i, v_j \right\rangle$ eindeutig bestimmt. Die Matrix (λ_{ij}) heißt Grammatrix $\mathcal{G}$ der Bilinearform f bezüglich der Basis $\mathcal{B}$.*
- *Sei $\langle x, y\rangle = 0$, so heißt x linksorthogonal zu y und y rechtsorthogonal zu x.*
- *Linksradikal und Rechtsradikal einer Bilinearform f sind definiert als*

$$\mathrm{rad}_l(f) = \{x \in V : f(x,y) = 0,\ \forall\ y \in V\},$$
$$\mathrm{rad}_r(f) = \{x \in V : f(y,x) = 0,\ \forall\ y \in V\}.$$

- *Sei f bilinear, dann wird durch*

$$E_l : V \to V^*, v \mapsto \lambda_v, \quad \lambda_v : V \to K, x \mapsto f(v,x),$$

der zu f assoziierte kanonische Linkshomomorphismus definiert. Analog dazu wird $E_r(v) = \rho_v$ mit $\rho_v(w) = f(w,v)$ definiert.

11.1 Sätze für Bilinearformen

Sei V Vektorraum und f bilinearform.

- $\mathrm{rad}_l(f), \mathrm{rad}_r(f) \leqslant V$.
- $\mathrm{rad}_l(f) = \ker E_l$ *und* $\mathrm{rad}_r(f) = \ker E_r$.
- *$f \to E_l^f$ und $f \to E_r^f$ definieren Bijektionen zwischen der Menge der Bilinearformen auf V und $\mathrm{Hom}_K(V,V^*)$.*

Sei V endlich dimensional mit $\dim_K V = n$ und Basis $\mathcal{B} = \{v_i \in V : 1 \le i \le n\}$.

- $\mathrm{rad}_l(f) = \ker \mathcal{G}_f(\mathcal{B})^t$, $\mathrm{rad}_r(f) = \ker \mathcal{G}_f(\mathcal{B})$.
- *Sei $\mathcal{B}^*$ die duale Basis, dann ist*

$$\mathfrak{M}_{E_r}(\mathcal{B}^*, \mathcal{B}) = \mathcal{G}_f(\mathcal{B}) = \mathfrak{M}_{E_l}(\mathcal{B}^*, \mathcal{B})^t$$

- *Ist f alternierend oder symmetrisch, so ist $x \perp y \Leftrightarrow y \perp x$ und es gilt* $\mathrm{rad}_l(f) = \mathrm{rad}_r(f)$.

- *Ist f symmetrisch, dann ist $E_l = E_r$.*

- *Ist f alternierend, dann ist $E_l = -E_r$.*

- *Ist* $\mathrm{char}\, K = 2$, *dann ist symmetrisch $\Leftrightarrow$ alternierend.*

- *f ist symmetrisch $\Leftrightarrow$ $\mathcal{G}_f(\mathcal{B})$ ist bezüglich einer Basis $\mathcal{B}$ symmetrisch.*

- *f ist alternierend $\Leftrightarrow$ $\mathcal{G}_f(\mathcal{B})$ ist bezüglich einer Basis $\mathcal{B}$ schiefsymmetrisch ($A^t = -A$).*

12 Tensorprodukt

- *Der freie Vektorraum $\mathcal{F}(V \times W)$ ist der K-Vektorraum, bestehnd aus Folgen von Elementen von K, die mit $V \times W$ indiziert sind.*

$$\mathcal{F}(V \times W) = \{(k_{vw}) \,:\, \textit{fast alle } k_{vw} = 0\}\,.$$

- *Ein K-Vektorraum W zusammen mit einer k-fachen linearen Abbildkung $\iota : V_1 \times \ldots \times V_k \to W$ heißt Tensorprodukt, falls folgende universelle Eigenschaft erfüllt ist:*
Ist $f : V_1 \times \ldots \times V_k \to U$ multilinear, so gibt es genau eine Abbildung $\hat{f} \in \mathrm{Hom}_K(W, U)$ *mit $\hat{f} \circ \iota = f$. Für W schreiben wir $V_1 \otimes \ldots \otimes V_k$.*

$$\begin{tikzcd}
V_1 \times \ldots \times V_k \arrow[rr, "\iota"] \arrow[drr, "f"'] & & W \arrow[d, "\exists\, !\hat{f}"] \\
& & U
\end{tikzcd}$$

12.1 Unendliche Dimension

Seien V, W K-Vektorräume und $\mathcal{B} = \{v_i \in V \,:\, i \in \mathcal{I}\}$, $\mathcal{C} = \left\{w_j \in W \,:\, j \in \mathcal{J}\right\}$ Basen.

- *Existieren ι und W, so ist W eindeutig bis auf Isomorphie.*

- *W wird von Elementen der Form $\{v_1 \otimes \ldots \otimes v_k = \iota(v_1, \ldots, v_k) \,:\, v_i \in V_i 1 \leq i \leq k\}$ erzeugt.*

- *$W \cong \mathcal{F}(V_1 \times \ldots \times V_k)/I$, wobei I der von der multilinearen Relation erzeugte Unterraum ist.*

- *Ein Spezialfall: $V \otimes K \cong V$.*

- *Seien U, V, W K-Vektorräume, dann gilt*

  (a) $V \otimes W \cong W \otimes V$.

  (b) $(U \otimes V) \otimes W \cong U \otimes (V \otimes W) \cong U \otimes V \otimes W$.

- *Das Tensorprodukt ist eine assoziative, kommutative Operation auf der Klasse der K-Vektorräume.*

- *Das Tensorprodukt ist distributiv über $\bigoplus$. Seien I, J Indexmengen und $V_i, i \in I$ und $W_j, j \in J$ K-Vektorräumge, dann gilt*

$$\left(\bigoplus_{i \in I} V_i\right) \otimes \left(\bigoplus_{j \in J} W_j\right) \cong \bigoplus_{i,j} \left(V_i \otimes W_j\right).$$

- *Ist $\mathcal{B}_i = (v_{i1}, \ldots, v_{in_i})$ Basis von V_i, so ist*

$$\mathcal{B} = \mathcal{B}_1 \otimes \ldots \otimes \mathcal{B}_k = \left\{v_{1i_1} \otimes \ldots \otimes v_{ki_k} \,:\, 1 \leq i_v \leq n_v, 1 \leq v \leq k\right\}$$

Basis von $V_1 \otimes \ldots \otimes V_k$.

- *Sind* $\phi_v \in \mathrm{Hom}_K(V_v, X_v)$ *($1 \leq v \leq k$), so wird durch*

$$\begin{aligned}
&\phi = \phi_1 \otimes \ldots \otimes \phi_k : V_1 \otimes \ldots \otimes V_k \to X_1 \otimes \ldots \otimes X_k \textit{ mit} \\
&\phi\left(\sum \lambda_{i_1 \ldots i_k} v_{i1} \otimes \ldots \otimes v_{ik}\right) = \sum \phi_1(v_{i1}) \otimes \ldots \otimes \phi_k(v_{ik}),
\end{aligned}$$

eine K-lineare Abbildung definiert.

12.2 Endliche Dimension

- *Sei $Y = \{f : V \times W \to K : f \text{ bilinear}\}$, dann ist die Abbildung $j : V \times W \to Y^*$, $j(v,w) = \alpha_{v,w}$ mit $\alpha_{v,w}(g) = g(v,w)$ bilinear.*

- *Sei $f : V \times W$ bilinear, dann existiert genau eine Abbildung $\hat{f} : Y^* \to U$, sodass $\hat{f} \circ j = f$. Es gilt also $V \bigotimes W \cong Y^*$.*

13 Symmetrische Gruppen

- *Sei G eine Gruppe, $|G| < \infty$ und $g \in G$, dann gibt es ein $k \in \mathbb{N}$, dass $g^k = 1_G$. Die kleinste natürliche Zahl für die dies gilt heißt Ordnung $|g|$ von $g \in G$.*

Sei $\pi \in \sigma_n$ und $1 \leq i \leq n$.

- *Es existiert eine kleinste Zahl $k \in \mathbb{N}$ für die gilt $\pi^j(i) = i$. Die Elemente aus $B = \left\{\pi^k(i) : 0 \leq j \leq k-1\right\}$ paarweise verschieden und B heißt Bahn von i unter π oder Zykel. k ist die Länge der Bahn.*

- *Ein Zykel ist eine Permutation π mit höchstens einer Bahn der Länge $l > 1$.*

- *Ein Zykel der Länge 2 heißt Transposition. Eine Transposition der Form $(k, k+1)$ heißt Fundamentaltransposition.*

- *Ein reduzierter Ausdruck von π ist ein Produkt von Fundamentaltranspositionen $\pi = (i_1, i_1+1)\dots(i_l+i_l+1)$, sodass l minimal ist. l nennt man die Länge der Permutation π und bezeichnet sie mit $l(\pi)$.*

- *Die Menge der Fehlstände von π ist definiert als*

$$\{[i,j] : 1 \leq i < j \leq n \text{ und } \pi(i) > \pi(j)\}.$$

Die Anzahl der Fehlstände wird mit $n(\pi)$ bezeichnet.

- *Eine Permutation heißt gerade bzw. ungerade, wenn $l(\pi)$ gerade, also $\operatorname{sign}\pi = 1$ bzw. ungerade, also $\operatorname{sign}\pi = -1$ ist.*

- *Zwei Elemente $x, y \in G$ heißen konjugiert, falls es ein $g \in G$ gibt, sodass $x = gyg^{-1}$. Für $x \in G$ heißt die Menge $\{gxg^{-1} : g \in G\}$ Konjugationsklasse von x.*

- *Eine Partition von $n \in \mathbb{N}$ ist eine Folge (λ_i) mit $\lambda_i \in \mathbb{N}_0$, $\lambda_i \geq \lambda_{i+1}$ und $\sum_i \lambda_i = n$.*

- *Der Zykeltyp von π ist die Partition von n, die entsteht, wenn man π als Produkt von disjunkten Zykeln schreibt und die Länge der Zykel absteigend ordnet.*

13.1 Sätze ...

Sei $\pi \in \sigma_n$ und $\mathfrak{M} = \{i : 1 \leq i \leq n\}$.

- *$s \sim t \Leftrightarrow \pi^k(s) = t$ für ein $k \in \mathbb{N}_0$, definiert für $s, t \in \mathfrak{M}$ eine Äquivalenzrelation auf $\mathfrak{M}$. Die Äquivalenzklassen sind gerade die Bahnen $s^{[\pi]}$ unter π.*

- *$\mathfrak{M}$ ist disjunkt zerlegt in Bahnen bezüglich π.*

- *Disjunkte Zykler kommutieren.*

- *Jedes $\pi \in \sigma_n$ kann bis auf die Reihenfolge der Faktoren eindeutig als Produkt aus disjunkten Zykeln geschrieben werden.*

- *$|\pi|$ ist das kleinste gemeinsame Vielfache der Länge der Bahnen von π.*

- *Jede Permutation $\pi \in \sigma_n$ kann als Produkt von Transpositionen geschrieben werden.*

- *Jede Transposition kann als Produkt von Fundamentaltranspositionen geschrieben werden.*

- $n(\pi(k,k+1)) = \begin{cases} n(\pi)+1, & \text{falls } \pi(k) < \pi(k+1), \\ n(\pi)-1, & \text{falls } \pi(k) > \pi(k+1). \end{cases}$

- $l(\pi) = n(\pi)$.

- *Kein Produkt einer geraden Anzahl von (Fundamental-)transpositionen ist gleich einem Produkt einer ungeraden Anzahl.*

- $\operatorname{sign} : \sigma_n \to \{-1, 1\}, \pi \mapsto \operatorname{sign}(\pi)$ *ist ein Gruppenhomomorphismus.*

- *Die Relation $\sim$ gegeben durch $x \sim y$ genau dann, wenn ein $g \in G$ existiert, sodass $x = gyg^{-1}$ ist eine Äquivalenzrelation.*
- *Sei $\sigma = (a_1, \dots, a_n)$ ein Zykel, dann ist $\pi\sigma\pi^{-1} = (\pi(a_1), \dots, \pi(a_n))$.*
- *Zwei Elemente von σ_n sind genau dann konjugiert, wenn sie vom selben Zykeltyp sind.*
- *Es gibt eine Bijektion zwischen den Konjugationsklassen der σ_n und den Partitionen von n. Die Bijektion bildet eine Konjugationsklasse π^{σ_n} ab auf den Zykeltyp von π.*

14 Jordansche Normalform

Sei V endlich dimensional und $f \in \mathrm{End}_K(V)$.

- *Sei $x \in V$, dann nennt man $W = \left\langle f^i(x) : i \geq 0 \right\rangle$, den von x erzeugten f-zyklischen Unterraum von V.*
- *Sei $p(t) \in K[t]$ ein Polynom, dann erfüllt f $p(t)$, falls $p(f) \equiv 0$.*
- *Ein Jordanblock $J_\lambda(k)$ ist eine $k \times k$-Matrix mit 1 auf der Neben- und λ auf der Diagonalen. Eine Matrix ist in Jordanform, falls ihre Blöcke auf der Diagonalen Jordanblöcke sind.*
- *Sei f so, dass $\chi_f(t)$ in Linearfaktoren zerfällt. Eine Jordanbasis von f ist eine Basis $\mathcal{B}_f$ von V, sodass $\mathfrak{M}_f(\mathcal{B}_f)$ in Jordanform ist.*
- *Der Unterraum $\mathcal{V}_\lambda(f)$ heißt verallgemeinerter Eigenraum zum Eigenwert λ von f. Seine Elemente heißen verallgemeinerte Eigenvektoren.*

$$\mathcal{V}_\lambda(f) = \cup_{i=1}^{\infty} \ker(f - \ell_\lambda)^i = \{v \in V : \ \exists\, p \in \mathbb{N} : (f - l_\lambda)^p(v) = 0\}.$$

- *Sei v verallgemeinerter Eigenvektor zu λ und $p \in \mathbb{N}$, sodass $(f - \ell_\lambda)^p(v) = 0$, dann ist*

$$\mathcal{B} = ((f - \ell_\lambda)^{p-1}(v), (f - \ell_\lambda)^{p-2}(v), \dots, (f - \ell_\lambda)(v), v)$$

eine Basis von des von v erzeugten f-zyklischen Unterraums von V. Wir nennen $\mathcal{B}$ λ-Zykel von f. Dabei heißt v Anfangs- und $(f - \ell_\lambda)^{p-1}(v)$ Endvektor des Zykels.

- *Eine Fahne der Länge k in V ist eine aufsteigende Kette*

$$\mathfrak{F} : (0) = U_0 \lneq U_1 \lneq \dots \lneq U_{k-1} \lneq U_k = V$$

von Unterräumen U_i von V. Eine Basis $\mathcal{B} = (v_1, \dots, v_n)$ von V heißt an $\mathfrak{F}$ angepasst, falls $(v_1, \dots, v_{m_i})$ eine Basis von U_i ist, wobei $m_i = \dim_K U_i$ für $i = 1, \dots, k$ gesetzt wird.

14.1 Sätze für Endomorphismen

- *Sei $U \leqslant V$ f-invariant und $\hat{f} = f|U$, dann gilt $\chi_{\hat{f}}(t) | \chi_f(t)$.*
- *Ein f-zyklischer Unterraum ist f-invariant.*

Sei $x \in V$ und W der von x erzeugte f-zyklische Unterraum von V mit $1 \leq k = \dim_K(W)$.

- *$\mathcal{B}_W = (x, f(x), f^2(x), \dots, f^{k-1}(x))$ ist eine Basis von W.*
- *Sei $f^k(x) = -\alpha_0 x - \alpha_1 f(x) - \dots - \alpha_{k-1} f^{k-1}(x)$, dann ist $\chi_{\hat{f}}$ für $\hat{f} = f|U$ gegeben als $\chi_{\hat{f}}(t) = t^k + \alpha_{k-1} t^{k-1} + \dots + \alpha_0$.*

Cayley-Hamilton *Sei $f \in \mathrm{End}_K(V)$, dann erfüllt f sein charakteristisches Polynom.*

- *$\ker(f - l_\lambda) \leqslant \ker(f - l_\lambda)^2 \leqslant \dots \leqslant \ker(f - l_\lambda)^i \leqslant \dots$ ist eine aufsteigende Kette von Unterräumen von V, die terminiert.*
- *Sei λ ein Eigenwert von $f \in \mathrm{End}_K(V)$, dann ist $\mathcal{V}_\lambda(f)$ ein f-invarianter Unterraum von V, der $V_\lambda(f)$ enthält.*
- *Sei $\mathcal{B}$ ein λ-Zykel, dann ist $\mathcal{B}$ Basis des vom Anfangsvektor erzeugten, $(f - \ell_\lambda)$-zyklischen Unterraums von W und dieser ist f-invariant. Die Einschränkung von f auf W besitzt genau einen eindimensionalen Eigenraum und dieser wird vom Endvektor des Zykels $\mathcal{B}$ erzeugt.*
- *Ist $\mathcal{B}$ Basis, dann ist $\mathcal{B}$ genau dann Jordanbasis von f, wenn sie eine disjunkte Vereinigung von Zykeln verallgemeinerter Eigenvektoren von f ist.*

- *Zerfällt $\chi_f(t)$ in Linearfaktoren, dann ist V die direkte Summe seiner verallgemeinerten Eigenräume*

$$V = \bigoplus_\lambda \mathcal{V}_\lambda(f),$$

wobei λ die Menge der Eigenwerte von f durchläuft.

- *Seien $\lambda_1, \dots, \lambda_k$ die verschiendenen Eigenwerte von f. Sei $\mathcal{B}_i$ die Basis des verallgemeinerten Eigenraums $\mathcal{V}_{\lambda_i}$, $\mathcal{B} = \bigcup_{i=1}^k \mathcal{B}_i$ und sei f_i die Einschränkung von f auf $\mathcal{V}_i$, dann ist $\mathfrak{M}_f(\mathcal{B}) = \operatorname{diag}\{A_1, \dots, A_k\}$, wobei $A_i = \mathfrak{M}_{f_i}(\mathcal{B}_i)$ ist.*

- *Sei λ Eigenwert von f. Es seien λ-Zykeln Z_i alle mit derseleben Länge t gegeben $(1 \le i \le s)$ und es sei y_i der Anfangsvektor von Z_i. Ist die Menge $\{y_i : 1 \le i \le s\}$ linear unabhängig modulo $\ker(f - \ell_\lambda)^{t-1}$, so ist $Z = \bigcup_{i=1}^s Z_i$ linear unabhängig.*

- *Seien die Vektoren $\{y_i : 1 \le i \le s\} \subset \ker(f - \ell_\lambda)^t$ im Faktorraum $\ker(f - \ell_\lambda)^t / \ker(f - \ell_\lambda)^{t-1}$ linear unabhängig, dann sind die von den y_i erzeugten λ-Zykel paarweise disjunkt.*

- *Sei $\mathcal{N}_r = \mathcal{N}_{r+1}$, dann ist $\mathcal{N}_r = \mathcal{N}_{r+i}$ für jedes $i \in \mathbb{N}$.*

- *Sei $A \in M_n(K)$ und zerfällt $\chi_A(t)$ in Linearfaktoren, so gibt es eine Matrix $P \in GL_n(K)$, sodass $P^{-1}AP$ Jordanform hat.*

- *Zerfällt $\chi_f(t)$ in Linearfaktoren, so besitzt V eine Jordanbasis bezüglich f.*

- *Die Unterräume $\ker(f - \ell_\lambda)^i$ des $\mathcal{V}_\lambda(f)$ bilden eine Fahne. Die zugehörige Jordanbasis ist angepasst.*

- *Sei $A \in M_n(K)$ in Jordanform, dann existieren eine Diagonalmatrix D und eine nilpotente Matrix N, die kommutieren, sodass*

$$A = D + N, \quad DN = ND.$$

- *Seien $A, N \in M_n(K)$ ähnlich und N nilpotent (unipotent), dann ist A nilpotent (unipotent).*

Jordanzerlegung *Sei $A \in M_n(K)$ und $\chi_A(t)$ zerfallen in Linearfaktoren, dann gibt es eine diagonalisierbare Matrix S und eine nilpotente Matrix N mit*

$$A = S + N, \quad SN = NS.$$

14.2 Sätze für Jordankästchen

- *Sei $J = J_\lambda(k)$, dann ist $\dim_K \ker(J - \lambda E)^i = i$, für $1 \le i \le k$ und $\dim \ker(J - \lambda E)^i = k$ für $i > k$.*

- *Sei A eine Matrix in Blockdiagonalform, deren s Diagonalblöcke Jordankästchen $J_i = J_\lambda(i)$ sind. Sei $n_i = \dim_K(\ker(A - \lambda E)^i)$, und k_i sei die Anzahl der vorkommenden Kästchen J_i. Sei $n_{r-1} < n_r = n_{r+1}$, dann gilt $n_i - n_{i-1} = \sum_{l=i}^{r} k_l$.*

15 Ringtheorie

- *Sei $\emptyset \neq S \subseteq R$. Dann ist S ein Unterring von R genau dann, wenn gilt*
  (a) *$r - s \in S$ für alle $r, s \in S$ ($(S, +)$ ist abelsche Gruppe von $(R, +)$).*
  (b) *$rs \in S$ für alle $r, s \in S$.*

Ein Unterring muss kein Einselement haben, außerdem ist $1_R \neq 1_S$ möglich, ist aber $1_R \in S$, so ist $1_S = 1_R$ das Einselement von S.

- *Seien S, R Ringe und $f : R \to S$, dann heißt f Ringhomomorphismus, falls gilt*
  (a) *$f(a + b) = f(a) + f(b), \ \forall\ a, b \in R$.*
  (b) *$f(ab) = f(a)f(b), \ \forall\ a, b \in R$.*

Gilt $f(1_R) = 1_S$, sagt man f erhält das Einselement.
$\ker f = \{r \in R : f(r) = 0\}$ heißt Kern, $\operatorname{im} f = \{f(r) \in S : r \in R\}$ heißt Bild.

- *Ein Unterring S von R heißt Linksideal bzw. Rechtsideal, falls*

$$rs \in S (sr \in S) \ \forall\ r \in R, s \in S.$$

Ist S sowohl Links- als auch Rechtsideal, heißt S Ideal und man schreibt $S \trianglelefteq R$.

- *Alle Ideale von R außer (0) und R selbst heißen nichttrivial bzw. echt.*

- *Ein Ideal M heißt maximal, falls es kein größeres echtes Ideal gibt, also für alle Ideale I gilt $M \subseteq I \subsetneq R \Rightarrow M = I$.*

- *Sei $I \trianglelefteq R$, dann wird durch $r \sim s \Leftrightarrow r - s \in I$, für $r, s \in R$ eine Äquivalenzrelation definiert. R/I bezeichnet die Menge der Äquivalenzklassen.*

- *R/I wird zum Ring durch*

$$(r + I) + (s + I) = (r + s) + I,$$
$$(r + I) \cdot (s + I) = (rs) + I.$$

Diesen Ring nennt man Faktorring. Die natürliche Projektion $\pi : R \to R/I, r \mapsto r + I$ ist ein Ringhomomorphismus.

- *Ein Ideal I von R heißt endlich erzeugt, falls es eine endliche Teilmenge S von R gibt, so dass $\langle S \rangle = I$. S heißt dann Erzeugendensystem von I. Besteht S aus genau einem Element, so heißt I Hauptideal. In diesem Fall ist $I = sR = \{sr : r \in R\}$.*

- *Ein Ring in dem alle Ideale endlich erzeugt sind heißt noethersch.*

- *Seien $I, J \trianglelefteq R$. Das Produkt $I \cdot J$ ist das Ideal von R, das von der Menge $\{a \cdot b : a \in I, b \in J\}$ erzeugt wird.*

- *Der Polynomring $R[x]$ besteht aus formalen Summen $\sum\limits_{i=0}^{n} \alpha_i x^i$, wobei x Unbestimmte und $\alpha_i \in R$ ist. Ist $p(x)$ Polynom mit $\alpha_k \neq 0$ aber $\alpha_m = 0$ für $m > k$, so ist heißt k der Grad $\deg p(x)$ von $p(x)$.*

- *Ein Element $a \in R$ heißt Nullteiler, falls es ein $0 \neq b \in R$ gibt mit $ab = 0$. Besitzt R außer 0 keinen Nullteiler, so heißt R Integritätsbereich oder Nullteilerfrei.*

- *Ein Integritätsbereich R heißt Hauptidealring, falls jedes Ideal von R ein Hauptideal ist.*

- *Sei R Integritätsbereich. Auf der Menge $\{(a,b) \in R \times R : b \neq 0\}$ definieren wir eine Äquivalenzrelation durch $(a,b) \sim (c,d) \Leftrightarrow ad = bc$. Die Äquivalenzklasse von (a,b) wird mit $\frac{a}{b}$ bezeichnet. Wir definieren für $a,b,c,d \in R, b,d \neq 0$ eine Addition und eine Multiplikation durch*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Damit wird $K = \left\{\frac{a}{b} : b \neq 0\right\}$ ein Körper, der Quotientenkörper $Q(R)$ von R. Die Abbildung $R \to K, r \mapsto \frac{r}{1}$ ist ein Ringmonomorphismus.

- *Ein Integritätsbereich R heiß euklidischer Ring, falls es eine Abbildung $\deg : R \to \mathbb{N} \cup \{-1\}$ gibt, sodass*
  (a) *Für alle $r \in R$ mit $r \neq 0$ gilt $\deg(0) < \deg(r)$.*
  (b) *Für $f, g \in R$ mit $g \neq 0$ gibt es $q, r \in R$ mit $\deg(r) < \deg(g)$, sodass $f = qg + r$ ist.*

- *$a, b \in R$ heißen assoziiert, falls es eine Einheit $u \in U(R)$ gibt, sodass $a = bu$.*

- *Sei R Integritätsbereich und $a, b \in R$ $c \in R$ heißt größter gemeinsamer Teiler von a und b $\mathrm{ggT}(a,b)$, falls gilt*
  (a) *$c|a$ und $c|b$*
  (b) *Ist $d \in R$ mit $d|a$ und $d|b$, so gilt $d|c$.*

- *Sei R Integritätsbereich und $a, b \in R$. $c \in R$ heißt kleinstes gemeinsames Vielfaches von a und b $\mathrm{kgV}(a,b)$, falls gilt*
  (a) *$a|c$ und $b|c$*
  (b) *Ist $d \in R$ mit $a|d$ und $b|d$, so gilt $c|d$.*

- *Sei R kommutativer Ring mit 1.*
  (a) *Sei $\mathcal{P} \trianglelefteq R$, dann heißt $\mathcal{P}$ Primideal, falls gilt. Sind $x, y \in R$ mit $xy \in \mathcal{P}$, so ist $x \in \mathcal{P}$ oder $y \in \mathcal{P}$.*
  (b) *$0 \neq a \in R$ heißt irreduzibel, falls*
  $a \notin U(R)$ und $a = xy$ für $x, y \in R \Rightarrow x \in U(R)$ oder $y \in U(R)$.
  (c) *$0 \neq a \in R$ heißt Primelement, falls aR Primideal ist, d.h. $a|xy \Rightarrow a|x$ oder $a|y$.*
  (d) *$0 \neq a \in R$ besitzt eine Zerlegung in irreduzible Faktoren, falls $a = \varepsilon \prod_{i=1}^{r} \pi_i$, mit $\varepsilon \in U(R)$ und π_i irreduzibel.*
  a besitzt eine eindeutige Zerlegung in irreduzibel Faktoren, falls zusätzlich gilt ist $a = \varepsilon' \prod_{i=1}^{r} \pi_i'$ mit $\varepsilon' \in U(R)$ und π_i' irreduzibel, dann gibt es eine Umordnung, sodass π_i und π_i' assoziiert sind.

- *Ein Integritätsbereich heißt faktoriell oder UFD unique factorisation domain, falls jedes Element $0 \neq a \in R$ eine eindeutige Zerlegung in irreduzible Elemente bestizt.*

15.1 Ringtheorie Sätze

Seien R, S Ringe, $f : R \to S$ Ringhomomorphismus und $I, J \trianglelefteq R$.

- *Die Menge der invertierbaren Elemente $U(A)$ eines Rings mit 1 oder einer K-Algebra A ist multiplikativ abgeschlossen und bildet mit der Multiplikation eine Gruppe.*
- *Seien R, S Ringe, $f : R \to S$ Ringhomomorphismus, dann gilt*
  (a) $(0), R \trianglelefteq R$. *Alle anderen Ideale heißen echt.*
  (b) *f ist surjektiv $\Leftrightarrow \operatorname{im} f = S$ und f ist injektiv $\Leftrightarrow \ker f = (0)$.*
  (c) $\ker f \trianglelefteq R$. *Ist f surjektiv, so gilt $\operatorname{im} f \trianglelefteq S$.*
  (d) *Der Durchschnitt von beliebig vielen Idealen von R ist Ideal von R.*
  (e) *Sei $A \subseteq R$, dann ist $\langle A \rangle$ das kleinste Ideal, das A enthält.*
  (f) *$I + J = \langle I \cup J \rangle$ das eindeutig bestimmte, kleinste Ideal, das I und J enthält.*
  (g) *Die Isomorphiesätze I - III gelten ebenfalls für Ringe.*
- *Ist $J \subseteq I$, dann ist J Ideal von I.*
- *Durch $r \sim s \Leftrightarrow r - s \in I$, für $r, s \in R$ wird eine Äquivalenzrelation definiert.*
- *R/I genau dann ein Körper, wenn I ein maximales Ideal ist.*
- *Sei R ein Ring, dann sind folgenden Bedingungen äquivalent*
  (a) *R ist noethersch.*
  (b) *Jede aufsteigende Kette von Idealen in R wird stationär.*
  (c) *Jede nichtleere Menge von Idealen besitzt maximale Elemente.*
- $I \cdot J \subseteq I \cap J$.
- *{Euklidische Ringe} ⊆ {HIRs} ⊆ {UFDs}.*

15.2 Sätze für Integritätsbereiche

Sei R Integritätsbereich.

- *Seien $a, b \in R$, dann sind $\mathrm{ggT}(a,b)$ und $\mathrm{kgV}(a,b)$ falls sie existieren, bis auf Assoziiertheit eindeutig bestimmt.*
- *R ist Integritätsbereich $\Leftrightarrow (0)$ ist Primideal von R.*
- *$\mathcal{P} \trianglelefteq R$ ist Primideal $\Leftrightarrow R/\mathcal{P}$ ist Integritätsbereich.*
- *M ist maximales Ideal $\Rightarrow M$ ist Primideal.*
- *$p \in R$ ist Primelement $\Rightarrow p$ ist irreduzibel.*
- *Sei R UFD und $p \in R$ irreduzibel, dann ist p Primelement.*
- *R ist UFD genau dann, wenn beiden Eigenschaften gelten*
  (a) *Jede aufsteigende Kette von Hauptidealen wird stationär.*
  (b) *Jedes irreduzibel Element von R ist Primelement.*

15.3 Sätze für HIR

- *Sei $a \in R$, dann ist $aR = R$ genau dann, wenn $a \in U(R)$.*
- *Euklidische Ringe sind Hauptidealringe.*
- *$\mathbb{Z}$ und $K[x]$ sind HIRs.*
- *Sind $a, b \in R$, dann gilt $a|b \Leftrightarrow bR \subseteq aR$.*
- *Assoziiert sein ist eine Äquivalenzrelation.*
- *$a, b \in R$ assoziiert $\Leftrightarrow aR = bR \Leftrightarrow a|b$ und $b|a$.*
- *Seien $a, b \in R$, dann existieren $\mathrm{ggT}(a,b)$ und $\mathrm{kgV}(a,b)$ und es gilt*
  (a) $aR + bR = \mathrm{ggT}(a,b)R$.
  (b) $aR \cap bR = \mathrm{kgV}(a,b)R$.

(c) $(aR) \cdot (bR) = (ab)R$.

▪ *Jedes Primideal $\mathcal{P} \neq (0)$ von R ist maximal und daher ist R/P ein Körper.*

15.4 Für K-Algebren

Sei R K-Algebra.

▪ *Durch $k \mapsto k \cdot 1_R$ wird ein Ringhomomorphismus definiert, der 1_K auf 1_R abbildet. Insbesondere ist dieser Homomorphismus nicht die Nullabbildung und daher injektiv, da K keine echten Ideale besitzt.*

▪ *Jedes Ideal von R ist abgeschlossen gegenüber skalarer Multiplikation mit Elementen aus K und deshalb automatisch ein K-Vektorraum.*

▪ *Man braucht nicht zwischen Ring- und Algebraidealen zu unterscheiden.*

15.5 Für Polynome $K[t]$

▪ *Seien $h, g \in K[t]$ und sei $\deg g \leq \deg h$, dann gibt es Polynome $q, r \in K[t]$ mit $\deg r < \deg g$, sodass $h(t) = q(t)g(t) + r(t)$.*

▪ *Sei $I \trianglelefteq K[t]$ und $p \in I$ ein nichttriviales Polynom minimalen Grades in I. Dann ist $I = pK[t]$ und wir haben $I = rK[t]$ für ein $r \in K[t]$ genau dann, wenn $r = \beta p$ für $0 \neq \beta \in K$ ist. Daher gibt es genau ein normiertes Polynom $q \in I$, sodass $I = qK[t]$.*

▪ *Der Polynomring $K[x_1, \ldots, x_n]$ über K hat folgende universelle Eigenschaft*

(a) *Es gibt eine Abbildung $\iota : \{1, \ldots, n\} \to K[x_1, \ldots, x_n]$. (Gegeben durch $\iota(i) = x_i$)*

(b) *Ist R eine kommutative K-Algebra mit 1 und $f : \{1, \ldots, n\} \to R$, dann gibt es genau einen K-Algebraautomorphismus $\hat{f} : K[x_1, \ldots, x_n] \to R$ mit $\hat{f}(x_i) = f(i)$.*

16 Minimalpolynom

Sei $f \in \mathrm{End}_K(V)$

▪ *$\mathcal{I}_f = \{p(t) \in K[t] : p(f) \equiv 0\} \trianglelefteq K[t]$ ist das sogenannte Verschwindungsideal.*

▪ *Das eindeutig bestimmte normierte Polynom kleinsten Grades in $\mathcal{I}_f$ heißt Minimalpolynom von f und wird mit $\mu_f(t)$ bezeichnet. Analog ist $\mu_A(t)$ definiert.*

16.1 Minimalpolynomsätze

▪ *Sei $p \in K[t]$ so, dass $f(p) \equiv 0$, dann gibt es ein $q(t) \in K[t]$, sodass $p(t) = q(t)\mu_f(t)$. Insbesondere gilt $\mu_f(t) | \chi_f(t)$.*

▪ *Die Minimalpolynome ähnlicher Matritzen stimmen überein.*

▪ *$\lambda \in K$ ist genau dann Nullstelle von $\mu_f(t)$, wenn λ Nullstelle von $\chi_f(t)$ ist.*

▪ *Zerfalle $\chi_f(t)$ in Linearfaktoren. Sei $V = V_1 \bigoplus \ldots \bigoplus V_k$ eine Zerlegung von V in f-invariante Unterräume V_i. Sei μ_i das Minimalpolynom von $f_i = f|V_i$, dann gilt $\mu_f | \prod_{i=1}^k \mu_i(t)$ und $\mu_i(t) | \mu_f(t)$ für $1 \leq i \leq k$.*
Sind daher die $\mu_i(t)$ paarweise teilerfremd, so gilt $\mu_f(t) = \prod_{i=1}^k \mu_i(t)$.

▪ *Sei $A = \mathrm{diag}\{J_1, \ldots, J_k\}$ Blockdiagonalmatrix und zerfalle $\chi_A(t)$ in Linearfaktoren, dann ist $\mu_A(t) = \prod_{i=1}^k \mu_{J_i}(t)$, falls die $\mu_{J_i}(t)$ paarweise teilerfremd sind.*

▪ *Sei $\chi_f(t) = \prod_{i=1}^k (t - \lambda_i)^{n_i}$, mit λ_i paarweise verschieden , dann ist $\mu_f(t) = \prod_{i=1}^k (t - \lambda_i)^{m_i}$, wobei m_i die kleinste natürliche Zahl s ist mit $\ker(f - \ell_{\lambda_i})^s = \ker(f - \ell_{\lambda_i})^{s+1}$. Insbesondere ist f diagonalisierbar genau dann, wenn $m_i = 1, \ \forall\ 1 \leq i \leq k$.*

17 Moduln

Sei R ein Ring mit 1 oder K-Algebra.

- *Ein R-Linksmodul ist eine abelsche Gruppe $(M,+)$, zusammen mit einer äußeren binären Operation $R \times M \to M, (a,m) \mapsto am$, sodass gilt*

  (a) $1_R m = m \ \forall\ m \in M$.

  (b) $a(bm) = (ab)m \ \forall\ a,b \in R, m \in M$.

  (c) $(a+b)m = am + bm \ \forall\ a,b \in R, m \in M$.

  (d) $a(m_1 + m_2) = am_1 + am_2 \ \forall\ a \in R,\ \forall\ m_1, m_2 \in M$.

Ein R-Rechtsmodul wird analog definiert. Ist R kommutativer Ring bzw. kommutative K-Algebra, dann ist M sowohl Links- als auch Rechtsmodul und wird einfach als Modul bezeichnet.

Seien M, N R-Moduln.

- *${}_RR$ wird regulärer Modul genannt.*

- *Eine Abbildung $f : M \to N$ heißt R-Modulhomomorphismus, falls f ein Homomorphismus der zugrundeliegenden abelschen Gruppe ist, der zusätzlich die R-Operation respektiert. Die Menge $\ker f = \{m \in M : f(m) = 0_N\}$ heißt Kern, $\operatorname{im} f = \{f(m) : m \in M\}$ heißt Bild.*

- *Eine Teilmenge $\emptyset \neq U \subseteq M$ heißt Untermodul, falls $(U,+)$ abelsche Untergruppe von $(M,+)$ ist und $r \cdot u \in U \ \forall\ r \in R, u \in U$. Wir schreiben $U \leqslant M$.*

- *Sei $S \subseteq M$. Der von S erzeugte Untermoduln $U = \langle S \rangle$ ist definiert als der kleinste Untermoduln von M, der S enthält.*

- *Sei $\emptyset \neq S \subseteq M$ mit $\langle S \rangle = M$, dann heißt S Erzeugendensystem von M und M heißt endlich erzeugt (e.e.), falls es ein endliches Erzeugendensystem gibt.*

- *Sei $S \subseteq M$ Erzeugendensystem von M, dann ist S ein minimales Erzeugendensystem, falls $\langle T \rangle \subsetneqq M$ für jede echte Teilmenge T von S.*

- *Sei $U \leqslant M$. Wir definieren eine Äquivalenzrelation $\equiv \mod U$ auf M durch $x \equiv y \mod U \Leftrightarrow x - y \in U$ für $x, y \in M$. Auf der Menge M/U der Äquivalenzklassen ist eine Addition und eine äußere Operation wohldefiniert, wodurch M/U zum R-Modul, dem Faktormodul wird.*

- *Ein Modul heißt frei, falls er isomorph zu einer direkten Summe von Kopien des regulären R-Moduls ${}_RR$ ist.*

- *Eine Teilmenge $S \subseteq M$ heißt linear unabhängig, falls es keine nichttriviale Darstellung $\sum_{s \in S} r_s \cdot s = 0, r_i \in A$ fast alle 0, gibt. Ein linear unabhängiges Erzeugendensystem von M heißt Basis von M. Es gilt dann $N = \bigoplus_{s \in S} R \cdot s$.*

- *Eine Teilmenge $S = \{y_i : i \in \mathcal{I}\} \subseteq M$ heißt unabhängig, falls aus $\sum_{\mathcal{I}} \lambda_i y_i = 0$ folgt $\lambda_i y_i = 0 \ \forall\ i \in \mathcal{I}$.*

- *Eine Folge von R-Moduln*

$$M_1 \xrightarrow{a_1} M_2 \xrightarrow{a_2} M_3 \xrightarrow{a_3} \ldots \xrightarrow{a_{i-1}} M_i \xrightarrow{a_i} \ldots$$

mit R-Modulhomomorphismen $a_i : M_i \to M_{i+1}$ heißt exakt, falls $\ker a_{i+1} = \operatorname{im} a_i$ ist. Eine exakte Folge der Form

$$(0) \to M \xrightarrow{\alpha} N \xrightarrow{\beta} E \to (0),$$

heißt kurze exakte Folge (keF).

Sei R kommutativer Ring mit 1.

- *Sei R noethersch, M ein R-Modul. Dann ist der Rang $\operatorname{rg}(M)$ definiert als Kardinalität einer Basis von M.*

- *Sei $m \in M$. Der Annulator von m in R ist $\operatorname{ann}_R(m) = \{r \in R : rm = 0\}$. Für $S \subseteq M$ ist $\operatorname{ann}_R(S) = \{r \in R : rm = 0 \ \forall\ m \in S\} = \bigcap_{m \in S} \operatorname{ann}_R(m)$.*

- *Sei $m \in M$, sodass $M = Rm$, dann heißt M zyklischer R-Modul.*

Sei R Integritätsbereich.

- *$m \in M$ heißt Torsionselement, falls $\operatorname{ann}_R(m) \neq 0$ ist. Ist 0_M das einzige, so heißt M torsionsfrei.*

- *Sei $T(M) \subseteq M$ die Menge der Torsionselemente von M, dann ist $T(M) \leqslant M$ und heißt Trosionsuntermodul von M. Ist $T(M) = M$, so heißt M Torsionsmodul.*

Sei R HIR und M e.e. R-Modul.

- *Sei $p \in R$, dann ist M_p der Untermodul*

$$M_p = \left\{ m \in M : p^k m = 0 \; \exists \; k \in \mathbb{N} \right\}.$$

Ist $0 \neq p \in R$ Primelement, so heißt M_p Primärkomponente.

- *Sei $\operatorname{ann}_R(M) = rR$, dann wird r die Ordnung von M genannt und mit $r = \mathcal{O}(M)$ bezeichnet.*

17.1 Beispiele

(a) Der 0-Modul (0) ist R-Modul mit Operation $r \cdot 0 = 0 \; \forall \; r \in R$.

(b) R wird zum R-Linksmodul ${}_R R$, wobei R auf R durch die gewöhnliche Linksmultiplikation operiert.

(c) Jedes Ideal von R ist R-Modul.

(a) Sei $R = \mathbb{Z}$, dann ist ${}_{\mathbb{Z}}\mathbb{Z}$ torsionsfrei und $\mathbb{Z}/z\mathbb{Z} (0 \neq z \in \mathbb{Z})$ Torsionsmodul, also $T(\mathbb{Z}/z\mathbb{Z}) = \mathbb{Z}/z\mathbb{Z}$.

(b) Sei $R = K[t]$, V K-Vektorraum, $f \in \operatorname{End}_K(V)$, V der $K[t]$-Modul V_f, daann ist $\mathcal{O}(V_f) = \mu_f(t)$ und es gilt $\operatorname{ann}_R(V_f) = \mu_f K[t]$ und V_f ist Torsionsmodul.

17.2 Darstellungssätze

Sei R Ring mit 1.

- *Sei M ein R-Modul, dann ist $f_r : M \to M, m \mapsto mr \in \operatorname{End}(M,+)$ und $F : R \to \operatorname{End}(M,+), r \mapsto f_r$ ein Ringhomomorphismus.*

- *Sei M abelsche Gruppe mit $+$ und $F : R \to \operatorname{End}(M,+), r \mapsto f_r$ Ringhomomorphismus, der die 1 erhält, dann wird M zum R-Modul durch $rm = (F(r))(m)$ für $r \in R$ und $m \in M$.*

17.3 Moduln über Ring mit 1

Sei R Ring mit 1, M, N R-Moduln.

- *Die R-Untermoduln von ${}_R R$ sind genau die Linksideale von R.*

- *Der Durchschnitt beliebig vieler Untermoduln von M ist Modul. Dieser ist der eindeutig bestimmte größte Untermodul von M, der in allen Untermoduln der vorgegebenen Menge enthalten ist.*

- *Die natürliche Projektion $\pi : M \to M/U, m \mapsto m + U$ ist ein Epimorphismus.*

- *Sei $f : M \to N$ R-linear, dann ist $\ker f \leqslant M$ und $\operatorname{im} f \leqslant N$.*

1. Isomorphiesatz *Sei $f : M \to N$ eine R-lineare Abbildung und $U \leqslant M$ mit $U \subseteq \ker f$, dann gibt es ein eindeutig bestimmtes $\hat{f} : M/U \to N$ mit $\operatorname{im} \hat{f} = \operatorname{im} f$ und $\ker \hat{f} = U/\ker f \leqslant M/\ker f$, sodass $\hat{f} \circ \pi = f$. Ist außerdem $\ker f = U$, so ist $\hat{f}$ ein R-Modulisomorphismus, es gilt also $M/\ker f \cong \operatorname{im} f$.*

$$\begin{tikzcd} M \arrow[rr, "f"] \arrow[dr, "\pi"'] & & N \\ & M/U \arrow[ur, "\exists ! \hat{f}"'] & \end{tikzcd}$$

2. Isomorphiesatz *Seien $U, V \leqslant M$, dann ist $(U+V)/V \cong U/(U \cap V)$.*

3. Isomorphiesatz *Seien $U, V \leqslant M$ und $V \leqslant$, dann ist U $(M/V)/(U/V) \cong U/M$.*

- *Ist R außerdem K-Algebra, so wird M ein K-Vektorraum durch $\lambda m = (\lambda \cdot 1_R)m$ für $\lambda \in K, m \in M$.*

- *M ist frei genau dann, wenn M eine R-Basis besitzt.*

- *Sei $\emptyset \neq \mathcal{I}$ eine beliebige Indexmenge, dann kann der freie Modul zu $\mathcal{I}$ definiert werden als $\mathcal{F}(\mathcal{I}) = \{f : \mathcal{I} \to R : f(i) = 0 \text{ für fast alle } i \in \mathcal{I}\}$. Durch $\left\{ e_i : e_i(j) = \delta_{ij}, \; \forall \; i \in \mathcal{I} \right\}$ ist eine Basis von $\mathcal{F}(\mathcal{I})$ gegeben.*

Universelle Eigenschaft des freien R-Moduls $\mathcal{F}(\mathcal{I})$ über $\mathcal{I}$ *Sei $g : \mathcal{I} \to M, i \mapsto m_i$, eine Abbildung von Mengen, dann existiert genau eine R-lineare Abbildung $\hat{g} : \mathcal{F}(\mathcal{I}) \to M$ mit $\hat{g} \circ \iota = g$, wobei $\iota : \mathcal{I} \to \mathcal{F}(\mathcal{I}), i \mapsto e_i$ ist.*

$$\begin{tikzcd}
\mathcal{I} \arrow[r, "\iota"] \arrow[dr, "g"'] & \mathcal{F}(\mathcal{I}) \arrow[d, "\exists !\hat{g}"] \\
 & M
\end{tikzcd}$$

- *Alle K-Moduln (das sind genau die K-Vektorräume) sind frei.*

- *Sei $f : M \to N$ ein R-Epimorphismus. Sei $S \subseteq M$ ein Erzeugendensystem für M, dann wird N von $f(S)$ erzeugt. So sind insbesondere epimorphe Bilder von endlich erzeugten R-Moduln endlich erzeugt.*

- *Sei $(0) \to N \xrightarrow{\alpha} M \xrightarrow{\beta} E \to (0)$ keF von R-Moduln. Sind N und E e.e., so auch M.*

- *Sei $(0) \to N \xrightarrow{\alpha} M \xrightarrow{\beta} E \to (0)$ keF von R-Moduln und sei E freier Modul, dann gibt es ein $U \leqslant M$ mit $U \cong E$, sodass $M = \operatorname{im} \alpha \bigoplus U$.*

- *Sei $(0) \to N \xrightarrow{\alpha} M \xrightarrow{\beta} E \to (0)$ keF von R-Moduln und sei $\delta : E \to U$ ein R-Homomorphismus mit $\beta \circ \delta = \mathrm{id}_E$, dann gilt $M = \operatorname{im} \alpha \bigoplus \operatorname{im} \delta$.*

- *Sei $I \trianglelefteq R$, dann gilt:*

  (a) $IM \leqslant M$

  (b) $\operatorname{ann}_R(M) \leqslant M$.

  (c) $I \subseteq \operatorname{ann}_R(M/IM)$.

  (d) *Sei $L \trianglelefteq R$ und sei $L \subseteq \operatorname{ann}_R(M)$. Dann wird M zum R/L-Modul durch $(r + L)m = rm$, für $r \in R, m \in M$.*

  (e) *M/IM ist R/I-Modul mit R-Operation gegeben durch $(r+I)(m+IM) = rm+IM$.*

- *Sei $M = \langle m_1, \ldots, m_k \rangle$ e.e., dann ist $\operatorname{ann}_R(M) = \left\{ r \in R : rm = \bigcap_{i=1}^{k} \operatorname{ann}_R(m_i) \right\}$.*

- *Sei R kommutativer, noetherscher Ring mit 1 und sei M ein freier R-Modul. Seien $\{m_\alpha : \alpha \in \mathcal{A}\}$ und $\{m_\beta : \beta \in \mathcal{B}\}$ Basen von M mit Indexmenge $\mathcal{A}$ bzw. $\mathcal{B}$, dann ist $|\mathcal{A}| = |\mathcal{B}|$.*

- *Sei R kommutativer, noetherscher Ring mit 1 und seien M, N freie R-Moduln mit $\mathrm{rg}(M) = \mathrm{rg}(N)$. Dann sind M und N isomorph. Für jede Kardinalität α gibt es daher einen bis auf Isomorphie eindeutigen freien R-Modul $\mathcal{F}_\alpha$ vom Rang α, nämlich $\mathcal{F}_\alpha = \bigoplus_{i=1}^{\alpha} {}_R R$.*

- *Sei $S \subseteq M, m \in M$, dann gilt $\operatorname{ann}_R(m), \operatorname{ann}_R(S) \trianglelefteq R$.*

- *Sei M ein zyklischer R-Modul, dann wir durch $f : {}_R R \to M, r \mapsto rm$, ein R-Modul Epimorphismus definiert.*

- *R/I ist genau dann zyklischer R-Modul, wenn $I \trianglelefteq R$.*

- *Sei $S = \{y_i : 1 \leq i \leq m\}$ Erzeugendensystem von M, dann ist S genau dann unabhängig, wenn $M = \bigoplus_{i=1}^{m} R y_i$.*

17.4 Moduln über Integritätsbereichen

Sei R Integritätsbereich, M ein R-Modul.

- *Ist M freier R-Modul, dann ist M torsionsfrei.*

- *$M/T(M)$ ist torsionsfrei.*

- *Epimorphe Bilder von Torsionsmoduln sind Torsionsmoduln.*

- *Sei $M_\alpha, \alpha \in \mathcal{A}$ eine Menge von R-Moduln. Dann ist $T\left(\bigoplus_{\alpha \in \mathcal{A}} M_\alpha\right) = \bigoplus_{\alpha \in \mathcal{A}} T(M_\alpha)$. Sind insbesondere die M_α Torsionsmoduln (torsionsfrei), so auch ihre direkte Summe.*

- *Untermoduln von Torsionsmoduln sind Torsionsmoduln und Untermoduln von torsionsfreien Moduln sind torsionsfrei.*

- *Sei $(0) \neq M = Rm$ torsionsfreier, zyklischer R-Modul, dann ist $M \cong {}_R R$ frei mit Basis $\{m\}$.*

17.5 Moduln über HIR

Sei R ein HIR und M e.e. R-Modul.

- *Sei F e.e., freier R-Modul vom Rang n über R mit R-Basis $\mathcal{B} = \{v_i : 1 \leq i \leq n\}$. Sei $M \leqslant F$, dann ist M freier R-Modul vom Rang k mit $k \leq n$.*

- *Sei M torsionsfrei mit Erzeugendensystem S, $|S| = k$, dann ist M frei vom Rang $n \leq k$.*

- *Sei M e.e., dann ist $M = T(M) \bigoplus U$, wobei $U \leqslant M$ freier R-Modul mit $\mathrm{rg}(U) < \infty$ ist und $U \cong M/T(M)$. Ist $T(M) = (0)$, so ist M frei mir $\mathrm{rg}(M) < \infty$.*

- *Sind $0 \neq p, q \in R$ mit $\mathrm{ggT}(p,q) = 1$, so ist $M_p \cap M_q = (0)$ und daher ist $M_p \bigoplus M_q$.*

- *Sei M e.e. R-Torsionsmodul, dann gilt*

  (a) *$\mathcal{O}(M)$ ist bis auf Assoziiertheit eindeutig und es gilt $(0) \neq \mathrm{ann}_R(M) = \mathcal{O}(M)R$.*

  (b) *Ist $\mathcal{O}(M) = r$ und $r = \prod_{i=1}^n p_i^{k_i}$ die Primfaktorzerlegung von r in nicht paarweise assoziierte Primelemente $p_i \in R$, $k_i \in \mathbb{N}$, so zerlegt sich M in die direkte Summe $M = \bigoplus_{i=1}^n M_{p_i}$ seiner eindeutig bestimmten Primärkomponenten $M_{p_i}, i = 1, \ldots, n$.*

  (c) *Sei $\mathcal{O}(M) = r = \prod_{i=1}^n p_i^{k_i}$ Primfaktorzerlegung, dann ist $\mathcal{O}(M_{p_i}) = p_i^{k_i}$.*

- *M ist zyklischer R-Modul genau dann, wenn M epimorphes Bild des ${}_RR$ ist.*

- *Sei $M = Rm$ zyklischer R-Torsionsmodul mit $\mathcal{O}(m) = r$, dann ist $M \cong R/rR$ als R-Modul und $\mathcal{O}(M) = r$.*

- *Sei $S = \{y_i : 1 \leq i \leq m\}$ unabhängiges Erzeugendensystem von M und $s_i = \mathcal{O}(y_i)$, dann ist $M = \bigoplus_{i=1}^m Ry_i \cong \bigoplus_{i=1}^m R/Rs_i$.*

- *Sei M e.e. Torsionsmodul mit $\mathcal{O}(M) = p^k$ für $p \in R$ Primelement. Sei $m \in M$ mit $\mathcal{O}(m) = \mathcal{O}(M) = p^k$.*

  (a) *Sei $\overline{M} = M/Rm$, dann gibt es in jeder Nebenklasse $\overline{x} = x + Rm \in \overline{M}$ einen Vektor $y = x + Rm$ mit $\mathcal{O}(\overline{x}) = \mathcal{O}(y)$.*

  (b) *Seien $y_1, \ldots, y_n \in M$ so, dass die $\overline{y_i}$ unabhängig sind und seien die Nebenklassenvertreter so gewählt, dass $\mathcal{O}(\overline{y_i}) = \mathcal{O}(y_i)\ \forall\ i$, dann ist auch $\{m, y_1, \ldots, y_n\}$ unabhängig.*

- *Sei $M = mR$ zyklischer R-Modul, $\mathcal{O}(M) = p^k$ für ein Primelement $p \in R$, für $0 \leq \nu \leq k$ sei $M_\nu = p^\nu M = Rp^\nu \cdot m$, dann gilt*

  (a) *$M_\nu \leqslant M$ und $\{M_\nu : \nu = 0, \ldots, k\}$ ist genau die Menge der Untermoduln von M.*

  (b) *$(0) = M_k \subsetneqq M_{k-1} \subsetneqq \ldots \subsetneqq M_1 \subsetneqq M_0 = M$.*

  (c) *M_ν ist zyklisch mit Erzeuger $p^\nu m$ und der Ordnung $\mathcal{O}(M_\nu) = p^{k-\nu}$.*

  (d) *Sei $x \in M$, dann ist $M = Rx$ genau dann wenn $x \notin M_1$ ist.*

  (e) *Jedes Erzeugendensystem von M enthält ein $x \notin M_1$. $M = Rx$.*

  (f) *Sei $S \subseteq M$ minimales Erzeugendensystem von M, dann ist $S = \{x\}$ mit $x \in M$ aber $x \notin pM$.*

- *M ein e.e. R-Torsionsmodul der Ordnung p^k für ein Primelement $p \in R$. Sei $s = \{m_i : 1 \leq i \leq n\} \subseteq M$ ein endliches minimales Erzeugendensystem von M. Dann enthält jedes minimale Erzeugendensystem exakt n Elemente und es gibt einedeutig bestimmte natürliche Zahlen $k = e_1 \geq e_2 \geq \ldots \geq e_n$, sodass mit $q_i = p^{e_i}$ gilt*

$$M \cong \bigoplus_{i=1}^n R/Rq_i$$

Prototypen *Seien $\{p_i \in R : 1 \leq i \leq k\}$ paarweise nicht assoziierte Primelemente, $\left\{e_\nu^{(i)} \in \mathbb{N} : e_\nu^{(i)} \geq e_{\nu+1}^{(i)}, 1 \leq \nu \leq n_i\right\}$ und $I_\nu^{(i)} = Rp^{e_\nu^{(i)}}$.*
Sei $\underline{e}_i = \left(e_1^{(i)}, \ldots, e_{n_i}^{(i)}\right)$ und

$$E\left(p_i, \underline{e}_i\right) = \bigoplus_{\nu=1}^{n_i} R/I_\nu^{(i)}.$$

Für $\alpha \in \mathbb{N}_0$ sei $M(p_1, \underline{e}_1, \ldots, p_k, \underline{e}_k, \alpha) = \left(\bigoplus_{i=1}^k E(p_i, \underline{e}_i)\right) \bigoplus \left(\bigoplus_{j=1}^\alpha R\right)$, dann ist

$$\{M\left(p_1, \underline{e}_1, \ldots, p_k, \underline{e}_k, \alpha\right) : k, \alpha \in \mathbb{N}_0, p_i \in R \text{ Primelement}\},$$

eine vollständige Liste von paarweise nicht isomorphen, endlich erzeugten R-Moduln.

- *Sei $r \in R$ und $r = s \cdot t$ mit $s, t \notin U(R)$ und $\mathrm{ggT}(s,t) = 1$, dann ist $M = R/Rr$ ein zyklischer R-Modul isomorph zu $R/Rs \bigoplus R/Rt$.*
- *Sei $q \in R$ und $q = \prod_{i=1}^{k} p_i^{e_i}$ eine Primfaktorzerlegung, dann ist*

$$R/Rq \cong \bigoplus_{i=1}^{k} R/Rp_i^{e_i}.$$