Lineare Algebra SS2018

Dozent: Prof. Dr. Arno Fehm

3. August 2018

Inhaltsverzeichnis

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 $\forall x, y \in X$: $(x, y) \notin R \Rightarrow (y, x) \in R$

■ **Beispiel 1.2 (Äquivalenzrelation)**
Eine Äquivalenzrelation ist eine reflexive, transitive und symmetrische Relation. Wir haben schon verschiedene Äquivalenzrelationen kennengelernt: Isomorphie von K-Vektorräumen und Ähnlichkeit von Matrizen.

Definition 1.3 (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 $x \leq y \wedge x \neq y$.

■ **Beispiel 1.4**

1. Die natürliche Ordnung $\leq$ auf $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ und $\mathbb{N}$ ist eine Z Totalordnung.
2. Teilbarkeit $|$ ist eine Halbordnung auf $\mathbb{N}$, aber Teilbarkeit ist keine Halbordnung auf $\mathbb{Z}$, da $1|-1$ und $-1|1$, aber $1 \neq -1$!
3. $\mathcal{P}(X)$ ist die Potenzmenge. "$\subseteq$" ist eine Halbordnung auf $\mathcal{P}$, aber für $|X| > 1$ ist "$\subseteq$" keine Totalordnung.
4. Sei $(X, \leq)$ eine Halbordnung, sei $Y \subseteq X$, so ist $(Y, \subseteq |_Y)$ eine Halbordnung.

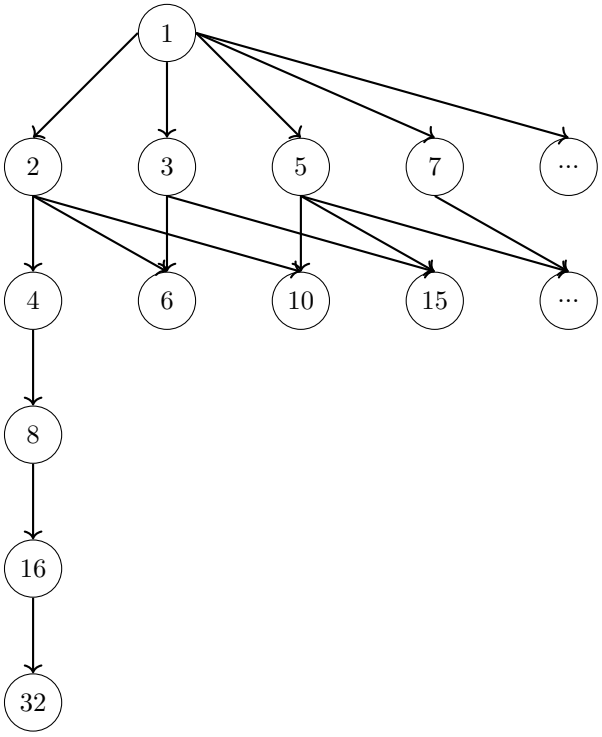
Definition 1.5 (Kette)
Sei $(X, \leq)$ eine Halbordnung, $Y \subseteq X$. Y heißt Kette , wenn $(Y, \leq |_Y)$ total ist.

$x \in Y$ 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 .



$Y = \{2^n \mid n \in \mathbb{N}\}$ ist eine Kette

▶ **Bemerkung 1.6**

- Hat Y ein kleinstes Element, so ist dies eindeutig bestimmt. Ein kleinstes Element ist minimal.
- Jede endliche Halbordnung hat minimale Elemente. Jede endliche Totalordnung hat ein kleinstes Element. Analog für maximale Elemente und größtes Element.

■ **Beispiel 1.7**
$(\mathbb{N}, \leq)$ hat als kleinstes Element die 1, aber kein größtes Element oder maximale Elemente.

■ **Beispiel 1.8**
$V = \mathbb{R}^3$, $\mathfrak{X}$ die Menge der Untervektorräume des $\mathbb{R}^3$. $(\mathfrak{X}, \leq)$ ist eine Halbordnung auf $Y \subseteq X$ mit $Y = \{U \in \mathfrak{X} \mid \dim_{\mathbb{R}}(U) \leq 2\}$.

- Y hat ein kleinstes Element: $\{0\}$.
- Es gibt unendlich viele maximale Elemente in Y, nämlich die Untervektorräume von V, die die Dimension 2 haben. Es gibt also kein größtes Element.
- V ist die obere Schranke von Y.

Theorem 1.9 (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 1.10 (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 1.11 (Basisergänzungssatz)
Sei V ein K-Vektorraum. Jede linear unabhängige Teilmenge $X_0 \subseteq V$ ist in einer Basis von V enthalten.

Beweis. Sei $\mathfrak{X} = \{X \subseteq V \mid X \text{ linear unabhängig}, X_0 \subseteq X\}$ 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.

■ **Beispiel 2.2**
Ist $V = K^n = \mathrm{Mat}_{n\times 1}(K)$, so wird $V^* = \mathrm{Hom}_K(V, K)$ durch $\mathrm{Mat}_{1\times n}(K) \cong K^n$. Wir können also die Elemente von V als Spaltenvektoren und die Linearformen auf V als Zeilenvektoren auffassen.

Lemma 2.3
Ist $B(x_1)_{i\in I}$ eine Basis von V, so gibt es zu jedem $i \in I$ genau $x_i^* \in V^*$ mit

$$x_i^*(x_j) = \delta_{ij} \quad \forall j \in I$$

Beweis. Siehe LAAG1 III.5.1, angewandt auf die Familie $(y_j)_{j\in I}$, $y_j\delta_{i.j}$ in $W = K$. □

Satz 2.4
Ist $B = (x_1)_{i\in I}$ eine Basis von V, so ist $B^* = (x_i^*)_{i\in I}$ linear unabhängig. Ist I endlich, so ist B^* eine Basis von V^*.

Beweis. Ist $\varphi = \sum_{i\in I} \lambda_i x_i^*$, $\lambda_i \in K$, fast alle gleich 0, so ist $\varphi(x_j) = \sum_{i\in I} \lambda_j x_i^*(x_j) = \lambda_j$ für jedes $j \in I$. Ist also $\varphi = 0$, so ist $\lambda_j = \varphi(x_j) = 0 \quad \forall j \in I$, B^* ist somit linear unabhängig.
Ist zudem I endlich und $\psi \in V^*$, so ist $\psi = \psi' = \sum_{i\in I} \psi(x_i)x_i^*$, denn $\psi'(x_j) = \sum_{i\in I} \psi(x_i)x_i^*(x_j) = \psi(x_i) \quad \forall j \in I$, und somit ist B^* ein Erzeugendensystem von V^*. □

Definition 2.5 (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 .

Folgerung 2.6
Zu jeder Basis B von V gibt es einen eindeutig bestimmtem Monomorphismus

$$f_V \to V^* \text{ mit } f(B) = B^*$$

Ist $\dim_K(V) < \infty$, so ist dieser ein Isomorphismus.

Folgerung 2.7
Zu jedem $= 0 \neq x \in V$ gibt es eine Linearform $\varphi \in V$ mit $\varphi(x) = 1$.

Beweis. Ergänze $x_1 = x$ zu einer Basis $(x_i)_{i\in I}$ von V (Folgerung 1.11) und $\varphi = x_1^*$. □

■ **Beispiel 2.8**
Ist $V = K^n$ mit Standardbasis $\mathcal{E} = (e_1, ..., e_n)$, so können wir V^* mit dem Vektorraum der Zeilenvektoren identifizieren, und dann ist

$$e_i^* = e_i^t$$

Definition 2.9 (Bidualraum)
Der Bidualraum zu V ist der K-Vektorraum

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

Satz 2.10
Die kanonische Abbildung

$$\iota : \begin{cases} V \to V^{**} \\ x \to \iota_x \end{cases} \quad \text{wobei } \iota_x(\varphi) = \varphi(x)$$

ist ein Monomorphismus. Ist $\dim_K(V) < \infty$, so ist ι ein Isomorphismus.

Beweis.
- $\iota_x \in V^{**}$:
  - $\iota_x(\varphi + \psi) = (\varphi + \psi)(x) = \varphi(x) + \psi(x) = \iota_x(\varphi) + \iota_x(\psi)$
  - $\iota_x(\lambda\varphi) = (\lambda\varphi)(x) = \lambda\varphi(x) = \lambda\iota_x(\varphi)$
- ι linear:
  - $\iota_{x+y}(\varphi) = \varphi(x+y) = \varphi(x) + \varphi(y) = \iota_x(\varphi) + \iota_y(\varphi) = (\iota_x + \iota_y)(\varphi)$
  - $\iota_{\lambda x}(\varphi) = \varphi(\lambda x) = \lambda\iota_x(\iota) = (\lambda\iota_x)(\varphi)$
- ι injektiv: Sei $0 \neq x \in V$. Nach Folgerung 2.7 existiert $\varphi \in V^*$ mit $\iota_x(\varphi) = \varphi(x) = 1 \neq 0$. Somit ist $\iota_x \neq 0$.
- Ist $\dim_K(V) < \infty$, so ist $V \overset{2.6}{\cong} V^* \overset{2.6}{\cong} V^{**}$, insbesondere $\dim_K(V) = \dim_K(V^{**})$. Der Monomorphismus ι ist somit ein Isomorphismus. □

▶ **Bemerkung 2.11**
Sei $\dim_K(V) < \infty$. Im Gegensatz zu den Isomorphismen $V \to V^*$, die von der Wahl der Basis B abhängen, ist der Isomorphismus $\iota : V \to V^{**}$ kanonisch (von der Wahl der Basis B unabhängig).

Die Voraussetzung, dass $\dim_K(V) < \infty$ ist hier essentiell: Für $\dim_K(V) = \infty$ ist ι nicht surjektiv.

Definition 2.12 (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.

Lemma 2.13
U^0 ist ein Untervektorraum von V^*.

Beweis. Klar. □

Satz 2.14
Ist $\dim_K(V) < \infty$ und $U \subseteq V$ ein Untervektorraum, so ist

$$\dim_K(V) = \dim_K(U) + \dim_K(U^0)$$

Beweis. Ergänze eine Basis $(x_1, ..., x_r)$ von U zu einer Basis $B = (x_1, ..., x_n)$ von V. Dann ist $B^*(x_1^*, ..., x_n^*)$ eine Basis von V^*. Sei $C = (x_{r+1}^*, ..., x_n^*)$. Dann ist C eine Basis von U^0:

- B^* ist Basis $\Rightarrow$ C ist linear unabhängig.

- $C \subseteq U^0$: Für $1 \leq j \leq r < i \leq n$ ist $x_i^*(x_j) = \delta_{ij} = 0$.
- $U^0 \subseteq \operatorname{span}_K(C)$: Ist $\varphi = \sum_{i=1}^n \lambda_i x_i^* \in U^0$, so $0 = \varphi(x_j) = \lambda_j$ für alle $j \leq r$, also $\varphi \in \operatorname{span}_K(x_{r+1}^*, ..., x_n^*)$. □

Folgerung 2.15
Ist $\dim_K(V) < \infty$ und $U \subset V$ ein Untervektorraum, so ist

$$\iota(U) = U^{00}$$

Beweis. Es ist klar, dass $\iota(U) \leq U^{00}$.
Für $\varphi \in U^0$ und $x \in U$ ist $\iota_x(\varphi) = \varphi(x) = 0$. Mit Satz 2.14 ist

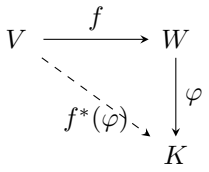
$$\begin{aligned} \dim_K(U^{00}) &= \dim_K(V^*) - \dim_K(U^0) \\ &= \dim_K(V^*) - (\dim_K(V) - \dim_K(U)) \\ &\overset{2.6}{=} \dim_K(U) \end{aligned}$$

und da ι injektiv ist, folgt $\iota(U) = U^{00}$. □

3. Die duale Abbildung

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

▶ **Bemerkung 3.1**
Ist $\varphi \in W^* = \operatorname{Hom}_K(W, K)$ eine Linearform auf W, so ist $\varphi \circ f \in \operatorname{Hom}_K(V, K) = V^*$ eine Linearform auf V.



Definition 3.2 (duale Abbildung)
Die zu f duale Abbildung ist

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

Lemma 3.3
Es ist $f^* \in \operatorname{Hom}_K(W^*, V^*)$.

Beweis. Sind $\varphi, \psi \in W^*$ und $\lambda \in K$ ist

$$\begin{aligned} f^*(\varphi+\psi) &= (\varphi+\psi)\circ f \\ &= \varphi\circ f + \psi \circ f \\ &= f^*(\varphi) + f^*(\psi) \\ f^*(\lambda\varphi) &= (\lambda\varphi)\circ f \\ &= \lambda\cdot(\varphi\circ f) \\ &= \lambda\cdot f^*(\varphi) \end{aligned}$$

□

Satz 3.4
Sind $B = (x_1, ..., x_n)$ und $C = (y_1, ..., y_m)$ Basen von V bzw. W, so ist

$$M_{B^*}^{C^*}(f^*) = \left(M_C^B(f)\right)^t$$

Beweis. Sei $A = M_C^B(f) = (a_{ij})_{i,j}$ und $B = M_{B^*}^{C^*}(f^*) = (b_{ji})_{j,i}$. Dann ist $f(x_j) = \sum_{i=1}^m a_{ij}y_i$, also $a_{ji} = y_i^*(f(x_j)) = f^*(y_i^*)(x_j)$ und $f^*(y_i^*) = \sum_{j=1}^n b_{ji}x_j^*$, also $b_{ji} = f^*(y_i^*)(x_j) = a_{ij}$. □

Folgerung 3.5
Sind V und W endlichdimensional, und identifizieren wir $V = V^{**}$ und $W = W^{**}$, so ist $f = f^{**}$, das heißt $\iota \circ f = f^{**} \circ \iota$.

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ {\scriptstyle \iota_V \cong}\downarrow & & \downarrow{\scriptstyle \iota_W \cong} \\ V^{**} & \xrightarrow[f^{**}]{} & W^{**} \end{array}$$

Beweis. Seien B und C Basen von V bzw. W. Unter der Identifizierung ist $B^{**} = B$ und $C = C^{**}$, das heißt $\iota(x_i) = x_i^{**}$ bzw. $\iota(y_j) = y_j^{**}$, denn $\iota(x_i)(x_j^*) = x_j^*(x_i) = \delta_{ij} = x_i^{**}(x_j^*) \quad \forall i,j$ und somit

$$M_C^B(f^{**}) \overset{3.4}{=} \left(M_{B^*}^{C^*}(f^*)\right)^t \overset{3.4}{=} \left(M_C^B(f)\right)^{tt} = M_C^B(f)$$

Also $f^{**} = f$. □

Folgerung 3.6
Sind V, W endlichdimensional, so liefert die Abbildung $f \mapsto f^*$ einen Isomorphismus von K-Vektorräumen.

$$\mathrm{Hom}_K(V,W) \to \mathrm{Hom}_K(W^*, V^*)$$

Beweis. Sind $f, g \in \mathrm{Hom}_K(V,W)$ und $\lambda \in K$, $\varphi \in W^*$, so ist

$$\begin{aligned} (f+g)^*(\varphi) &= \varphi\circ(f+g) = \varphi\circ f + \varphi\circ g = f^*(\varphi) + g^*(\varphi) = (f^*+g^*)(\varphi) \\ (\lambda f)^*(\varphi) &= \varphi\circ(\lambda f) = \lambda\cdot(\varphi\circ f) = \lambda\circ f^*(\varphi) = (\lambda f^*)(\varphi) \end{aligned}$$

Die Abbildung ist somit linear. Nach Folgerung 3.5 ist sie injektiv. Da

$$\begin{aligned}\dim_K(V,W) &= \dim_K(V)\cdot\dim_K(W)\\ &= \dim_K(V^*)\cdot\dim_K(W^*)\\ &= \dim_K(\mathrm{Hom}_K(W^*,V^*))\end{aligned}$$

ist sie auch ein Isomorphismus. □

Satz 3.7
Sind V, W endlichdimensional so ist

$$\mathrm{Im}(f^*) = \mathrm{Ker}(f)^0$$
$$\mathrm{Ker}(f^*) = \mathrm{Im}(f)^0$$

Beweis.

- $\mathrm{Im}(f^*) \subseteq \mathrm{Ker}(f)^0$: Ist $\varphi \in W^*$, $x \in \mathrm{Ker}(f)$, so ist

$$f^*(\varphi)(x) = (\varphi \circ f)(x) = \varphi(0) = 0$$

- $\mathrm{Ker}(f)^0 \subseteq \mathrm{Im}(f^*)$: Sei $\varphi \in \mathrm{Ker}(f)^0$. Setze eine Basis $(x_1, ..., x_r)$ von $\mathrm{Ker}(f)$ zu einer Basis $(x_1, ..., x_n)$ von V fort. Dann sind $f(x_{r+1}), ..., f(x_n)$ linear unabhängig nach der Kern-Bild-Formel (LAAG 1 III.7.13), es gibt also $\psi \in W^*$ mit

$$\psi(f(x_i)) = \varphi(x_i) \quad \forall i$$

  Es folgt

$$f^*(\psi)(x_i) = \psi(f(x_i)) = \varphi(x_i) \quad \forall i$$

  also $\varphi = f^*(\psi)$.

- Mit der Identifizierung $V = V^{**}$ ist

$$\mathrm{Im}(f)^0 \overset{3.5}{=} \mathrm{Im}(f^{**})^0 = \mathrm{Ker}(f^*)^{00} \overset{2.15}{=} \mathrm{Ker}(f^*)$$ □

Folgerung 3.8
Sind V, W endlichdimensional, so ist

$$\mathrm{rk}(f) = \mathrm{rk}(f^*)$$

Beweis.

$$\begin{aligned}\mathrm{rk}(f) &= \dim_K(\mathrm{Im}(f))\\ &\overset{2.14}{=} \dim_K(W) - \dim_K(\mathrm{Im}(f)^0)\\ &\overset{LAAG1.III.7.13}{=} \dim_K(W^*) - \dim_K(\mathrm{Ker}(f^*))\\ &= \mathrm{rk}(f^*)\end{aligned}$$ □

Folgerung 3.9
Ist $\dim_K(V) < \infty$ und $U \subseteq V$ ein Untervektorraum, so lässt sich jede Linearform auf U zu einer

Linearform auf V fortsetzen.

Beweis. Ist $f : U \to V$ die Inklusionsabbildung, so ist $f^* : V^* \to U^*$, $\varphi \mapsto \varphi|_U$ und

$$\mathrm{rk}(f^*) = \mathrm{rk}(f) = \dim_K(U) = \dim_K(U^*)$$

f^* ist somit surjektiv. □

▶ **Bemerkung 3.10**

Folgerung 3.9 gilt auch ohne die Voraussetzung $\dim_K(V) < \infty$, siehe Übung.

▶ **Bemerkung 3.11**

Ein homogenes lineares Gleichungssystem $Ax = 0$ hat als Lösungsraum $L(A, 0) \subseteq K^n$ ein Untervektorraum des K^n. Unter der Identifizierung $K^n = (K^n)^{**}$ ist $L(A, 0)$ der Annulator der Linearformen beschrieben durch die Zeilen $a_1, ..., a_m \in (K^n)^*$ von A. Wir wollen umgekehrt zu einem Untervektorraum $W \subseteq K^n$ ein $A = (a_1, ..., a_m) \in \mathrm{Mat}_{n\times m}(K)$ mit $W = L(A, 0)$ finden. Ist $W = \mathrm{span}_K(b_1, ..., b_r)$, so ist $W = \mathrm{Im}(f_B)$ mit $B = (b_1, ..., b_r) \in \mathrm{Mat}_{n\times r}(K)$.
$\Rightarrow W \overset{3.7}{=} \mathrm{Ker}(f_B^*)^0$ und $M_{\mathcal{E}^t}(f_B^*) = B^t$. Wenn man also eine Basis $(a_1, ..., a_s)$ von $L(B^t, 0)$ bestimmt und daraus eine Matrix $A = (a_1^t, ..., a_s^t) \in \mathrm{Mat}_{s\times n}(K)$ bildet, so ist $W = L(A, 0)$.

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

Lemma 4.2

$\overline{V}$ ist ein K-Vektorraum und $\mathrm{End}_K(V) = \mathrm{End}_K(\overline{V})$.

Beweis. Mit LAAG1 VI.1.7 nachprüfen, zum Beispiel:

- $\lambda * (x + y) = \overline{\lambda} \cdot (x + y) = \overline{\lambda}x + \overline{\lambda}y = \lambda * x + \lambda * y$
- $\lambda * (\mu * x) = \overline{\lambda}(\overline{\mu} \cdot x) = \overline{\lambda\mu}x = (\lambda\mu) * x$ □

Weiterhin sei: $f \in \mathrm{End}_K(V)$, $x \in V$, $\lambda \in K$
$\Rightarrow f(\lambda * x) = f(\overline{\lambda}x) = \lambda * f(x)$
$\Rightarrow f \in \mathrm{End}_K(\overline{V})$.
Umgekehrt sei $g \in \mathrm{End}_K(\overline{V})$, $x \in V$, $\lambda \in K$
$\Rightarrow g(\lambda \cdot x) = g(\overline{\lambda} * x) = \lambda \cdot g(x)$
$\Rightarrow g \in \mathrm{End}_K(V)$.

Lemma 4.3
Für $y \in V$ ist

$$\Phi_y : \begin{cases} V \to K \\ x \mapsto \langle x, y \rangle \end{cases}$$

eine Linearform auf V.

Die Abbildung $y \mapsto \Phi_y$ liefert einen Isomorphismus $\Phi : \overline{V} \to V^*$.

Beweis.
- $\Phi_y \in V^*$: Linearität in ersten Argument.
- $\Phi \in \mathrm{Hom}_K(\overline{V}, V^*)$: Für $y, y' \in V$, $\lambda \in K$, $x \in V$ ist
  - $\Phi_{y+y'}(x) = \langle x, y + y' \rangle = \langle x, y \rangle + \langle x, y' \rangle = \Phi_y(x) + \Phi_{y'}(x)$
  - $\Phi_{\lambda * y}(x) = \langle x, \lambda * x \rangle = \left\langle x, \overline{\lambda} y \right\rangle = \lambda \langle x, y \rangle = \lambda \Phi_y(x)$
- Φ injektiv: Skalarprodukt ist nicht ausgeartet.
- Da $\dim_K(\overline{V}) = \dim_K(V) = \dim_K(V^*)$ ist Φ somit ein Isomorphismus. □

Satz 4.4
Zu $f \in \mathrm{End}_K(V)$ gibt es ein eindeutig bestimmtes $f^{adj} \in \mathrm{End}_K(V)$ mit

$$\langle f(x), y \rangle = \left\langle x, f^{adj}(y) \right\rangle \quad \forall x, y \in V$$

Beweis. Existenz und Eindeutigkeit sind zu zeigen.

- Existenz:

$$\begin{array}{ccc} \overline{V} & \xrightarrow[f^{adj}]{f} & \overline{V} \\ \Phi \downarrow & & \downarrow \Phi \\ V^* & \xleftarrow{f^*} & V^* \end{array}$$

  Für $f^{adj} = \Phi{-}1 \circ f^* \circ \Phi \in \mathrm{End}_K(\overline{V}) = \mathrm{End}_K(V)$ ist

$$\Phi_y \circ = (f^* \circ \Phi)(y) = (\Phi \circ f^{adj\cdot})(y) = \Phi_{f^{adj}(y)}$$

  also

$$\langle f(x), y \rangle = (\Phi_y \circ f)(x) = \Phi_{f^{adj}(y)}(x) = \left\langle x, f^{adj}(y) \right\rangle \quad \forall x, y \in V$$

- Eindeutigkeit: Erfüllen f_1, f_2 für Gleichung

$$\langle f(x), y \rangle = \left\langle x, f^{adj}(y) \right\rangle \quad \forall x, y \in V$$

  so ist

$$0 = \langle x, f_1(y) \rangle - \langle x, f_2(y) \rangle = \langle x, f_1(y), f_2(y) \rangle \quad \forall x, y \in V$$

  da $\langle \cdot, \cdot \rangle$ nicht ausgeartet ist, folgt daraus, dass $f_1 = f_2$. □

Definition 4.5 (adjungierter Endomorphismus)
Die Abbildung f^{adj} heißt der zu f adjungierte Endomorphismus .

■ **Beispiel 4.6**

- Ist f selbstadjungiert, so ist $f^{adj} = f$.
- Ist f unitär, so ist $f \in \mathrm{Aut}_K(V)$ und

$$\langle f(x), y\rangle = \left\langle x, f^{-1}(y)\right\rangle \quad \forall x, y \in V$$

also $f^{adj} = f^{-1}$.

Lemma 4.7
Ist B eine Orthonormalbasis vin V, so ist

$$M_B(f^{adj}) = M_B(f^*)$$

Beweis. Ist $A = M_B(f)$ und $B = M_B(f^{adj})$, $v = \Phi_B(x)$, $w = \Phi_B(y)$, so ist

$$\begin{aligned}(Ax)^t\overline{y} = \langle f(v), w\rangle &= \left\langle v, f^{adj}(w)\right\rangle\\ x^tA^t\overline{y} &= x^t\overline{B}\overline{y}\\ \Rightarrow B = \overline{A^t} &= A^*\end{aligned}$$

□

Lemma 4.8
Für $f, g \in \mathrm{End}_K(V)$ und $\lambda, \mu \in K$ ist

$$\begin{aligned}(\lambda f + \mu g)^{adj} &= \overline{\lambda} f^{adj} + \overline{\mu} g^{adj}\\ (f^{adj})^{adj} &= f\end{aligned}$$

Beweis. Für $x, y \in V$ ist

$$\begin{aligned}\langle(\lambda f + \mu g)(x), y\rangle &= \lambda\langle f(x), y\rangle + \mu\langle g(x), y\rangle\\ &= \lambda\left\langle x, f^{adj}(y)\right\rangle + \mu\left\langle x, g^{adj}\right\rangle\\ &= \left\langle x, (\overline{\lambda} f^{adj} + \overline{\mu} g^{adj})(y)\right\rangle\end{aligned}$$

und

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

□

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

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

Mathematica/WolframAlpha-Befehle (normale Matrix)
Ob eine Matrix A normal ist, beantwortet folgende Funktion für Mathematica bzw. WolframAlpha:

```
NormalMatrixQ[A]
```

■ **Beispiel 5.2**

- Ist f selbstadjungiert, so ist $f^{adj} = f$, insbesondere ist f normal.
- Ist f unitär, so ist $f^{adj} = f^{-1}$, insbesondere ist f normal.

Lemma 5.3
Genau dann ist $f \in \mathrm{End}_K(V)$ normal, wenn

$$\langle f(x), f(y)\rangle = \left\langle f^{adj}(x), f^{adj}(y)\right\rangle \quad \forall x, y \in V$$

Beweis.

- Hinrichtung: Ist f normal, so ist

$$\begin{aligned}\langle f(x), f(y)\rangle &= \left\langle x, (f^{adj} \circ f)(y)\right\rangle \\ &= \left\langle x, (f \circ f^{adj})(y)\right\rangle \\ &= \left\langle f^{adj}(x), f^{adj}(y)\right\rangle \quad \forall x, y \in V\end{aligned}$$

- Rückrichtung: Ist umgekehrt $\left\langle f^{adj}(x), f^{adj}(y)\right\rangle$, so ist

$$\begin{aligned}\left\langle x, (f^{adj} \circ f)(y)\right\rangle &= \left\langle x, (f \circ f^{adj})(y)\right\rangle \\ 0 &= \left\langle x, (f^{adj} \circ f - f \circ f^{adj})(y)\right\rangle \\ f^{adj} \circ f &= f \circ f^{adj}\end{aligned}$$

□

Lemma 5.4
Ist f normal, ist ist

$$\mathrm{Ker}(f) = \mathrm{Ker}(f^{adj})$$

Beweis. Nach Lemma 5.3 ist

$$\|f(x)\| = \|f^{adj}(x)\| \quad \forall x \in V$$

Insbesondere gilt

$$f(x) = 0 \iff f^{adj}(x) = 0$$ □

Lemma 5.5
Ist f normal, so ist

$$\mathrm{Eig}(f, \lambda) = \mathrm{Eig}(f^{adj}, \overline{\lambda}) \quad \forall \lambda \in K$$

Beweis. Da $(\lambda \cdot \mathrm{id} - f)^{adj} \overset{4.8}{=} \overline{\lambda} \cdot \mathrm{id} - f^{adj}$ ist auch $\lambda \cdot \mathrm{id} - f$ normal. Somit ist

$$\begin{aligned}\mathrm{Eig}(f, \lambda) &= \mathrm{Ker}(\lambda\,\mathrm{id} - f) \\ &\overset{5.4}{=} \mathrm{Ker}((\lambda\,\mathrm{id} - f)^{adj}) \\ &= \mathrm{Ker}(\overline{\lambda}\,\mathrm{id} - f^{adj}) \\ &= \mathrm{Eig}(f^{adj}, \overline{\lambda})\end{aligned}$$ □

Theorem 5.6 (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 $M_B(f^{adj}) \overset{4.7}{=} A^*$ 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 Lemma 5.5 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. □

Folgerung 5.7
Sei $A \in \mathrm{Mat}_n(\mathbb{C})$. Genau dann gibt es $S \in \mathrm{U}_n$ mit $S^*AS = D$ eine Diagonalmatrix, wenn A normal ist.

▶ **Bemerkung 5.8**
Theorem 5.6 ist eine gemeinsame Verallgemeinerung von ?? und ??

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

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

■ **Beispiel 6.2**
Seien $V = W = K[t]_{\leq d}$, $U = K[t]_{\leq 2d}$. Die Abbildung

$$\xi : \begin{cases} V \times W \to U \\ (f.g) \mapsto fg \end{cases} \qquad \text{ist bilinear}$$

Wir sehen, dass $\mathrm{Im}(\xi)$ im Allgemeinen kein Untervektorraum von U ist. Ist zum Beispiel $K = \mathbb{Q}$, $d = 1$, so liegen $t^2 = \xi(t, t)$ und $-2 = \xi(-2, 1)$ im $\mathrm{Im}(\xi)$ nicht jedoch $t^2 - 2$, denn wäre $t^2 - 2 = fg$ mit $f, g \in \mathbb{Q}[t]$ linear, so hätte $t^2 - 2$ eine Nullstelle in $\mathbb{Q}$, aber $\sqrt{2} \notin \mathbb{Q}$.

Lemma 6.3
$\mathrm{Bil}_K(V, W, U)$ bildet einen Untervektorraum des K-Vektorraum $\mathrm{Abb}(V \times W, U)$.

Beweis. klar, zum Beispiel

$$(\xi + \xi')(\lambda v, w) = \xi(\lambda v, w) + \xi'(\lambda v, w) = \lambda\xi(v, w) + \lambda\xi(v, w) = \lambda(\xi + \xi')(v, w)$$ □

Lemma 6.4
Ist $\xi \in \mathrm{Bil}_K(V, W, U)$ und $f \in \mathrm{Hom}_K(U, U')$ für einen K-Vektorraum, so ist

$$f \circ \xi \in \mathrm{Bil}_K(V, W, U')$$

Beweis. klar, zum Beispiel

$$(f \circ \xi)(\lambda v, w) = f(\xi(\lambda v, w)) = f(\lambda \xi(v, w)) = \lambda \cdot (f \circ \xi)(v, w) \qquad \square$$

Lemma 6.5
Sei $(v_i)_{i \in I}$ eine Basis von V und $(w_j)_{j \in J}$ eine Basis von W. Zu jeder Familie $(u_{ij})_{(i,j) \in I \times J}$ in U gibt es genau ein $\xi \in \mathrm{Bil}_K(V, W, U)$ mit

$$\xi(v_i, w_i) = u_{ij} \quad \forall i \in I, j \in J$$

Beweis.

- Eindeutigkeit: Ist ξ bilinear, $v = \sum_{i \in I} \lambda_i v_i$, $w = \sum_{j \in J} \mu_j w_j$ so ist

$$\begin{aligned} \xi(v, w) &= \xi\left(\sum_{i \in I} \lambda_i v_i, \sum_{j \in J} \mu_j w_j\right) \\ &= \sum_{i \in I} \lambda_i \xi\left(v_i, \sum_{j \in J} \mu_j w_j\right) \\ &= \sum_{i,j} \lambda_i \mu_j u_{ij} \end{aligned} \tag{1}$$

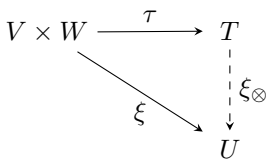
  durch die Familie $(u_{ij})_{i,j}$ bestimmt.

- Existenz: Wird ξ durch (1) definiert, so ist ξ bilinear: Für festes $w = \sum_{j \in J} \mu_j w_j$ ist

$$\begin{cases} V & \to U \\ v = \sum_{i \in I} \lambda_i v_i & \mapsto \xi(v, w) = \sum_{i \in I} \lambda_i \left(\sum_{j \in J} \mu_j u_{ij}\right) \end{cases}$$

  linear (LAAG1 III.5.1), analog für festes v. $\square$

Definition 6.6 (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 $\xi = \xi_\otimes \circ \tau$.*



Anmerkung
Sind V und W zwei Vektorräume und K ein gemeinsamer Körper, so kann man das Tensorprodukt $V \otimes W$, was auch ein Vektorraum ist, wie folgt konstruieren: Wenn $B = (b_1, ..., b_n)$ eine Basis von V und $C = (c_1, ..., c_m)$ eine Basis von W ist, dass ist $V \otimes W$ ein Vektorraum, genannt *Tensorproduktraum*, in dem es eine Basis gibt, die auf eindeutige Weise mit den geordneten Paaren des kartesischen Produkts

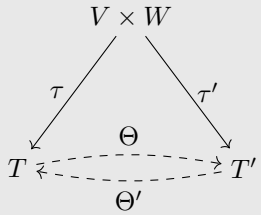
$$B \times C = \{(b_i, c_j)\}$$

der Basen der Ausgangsräume identifiziert werden kann. Die Dimension von $V \otimes W$ ist dann das Produkt der Dimensionen von V und W. Ein Element der Basis von $V \otimes W$, das dem Paar (b_i, c_j) entspricht, wird als $b_i \otimes c_j$ notiert, das $\otimes$ hat also keine tiefere Bedeutung. Ein Element des Tensorproduktes $V \otimes W$ hat dann die Gestalt:

$$\sum_{i,j} \lambda_{ij} \cdot (b_i \otimes c_j)$$

mit $\lambda_{ij} \in K$.

Lemma 6.7
Sind (T, τ) und (T', τ') Tensorprodukte von V und W, so gibt es einen eindeutig bestimmten Isomorphismus $\Theta : T \to T'$ mit $\tau' = \Theta \circ \tau$.



Beweis. Da (T, τ) die universelle Eigenschaft erfüllt, gibt es ein eindeutig bestimmtes $\Theta = (\tau')_{\otimes} \in \mathrm{Hom}_K(T, T')$ mit $\tau' = \Theta \circ \tau$. Analog gibt es $\Theta' \in \mathrm{Hom}_K(T', T)$ mit $\tau = \Theta' \circ \tau'$. Es folgt, dass $\tau = \Theta' \circ \tau' = \Theta' \circ \Theta \circ \tau$. Da auch $\tau = \mathrm{id}_T \circ \tau$ liefert die Eindeutigkeitsaussage in der universellen Eigenschaft von (T, τ), für $U = T$, $\xi = \tau$, dass $\Theta \circ \Theta' = \mathrm{id}_T$. Analog sieht man, dass $\Theta \circ \Theta' = \mathrm{id}_{T'}$. Somit ist Θ ein Isomorphismus. □

Definition 6.8 (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 $\delta_x(y) = \delta_{x,y} = \begin{cases} 1 & x = y \\ 0 & x \neq y \end{cases}$

Lemma 6.9
Sei X eine Menge und V der K-Vektorraum mit Basis X. Dann ist V ein K-Vektorraum und $(\delta_x)_{x \in X}$ ist eine Basis von V.

Beweis. Zu zeigen ist nur, dass $(\delta_x)_{x \in X}$ linear unabhängig ist. Ist $f = \sum_{x \in X} \lambda_x \delta_x$, $\lambda_x \in K$, fast alle gleich 0, und $f = 0$, so ist $\lambda_x = f(x) = 0$ für jedes $x \in X$. □

Lemma 6.10
Sei $(v_i)_{i\in I}$ eine Basis von V und $(w_j)_{j\in J}$ eine Basis von W. Sei T der K-Vektorraum mit der Basis $I \times J$ (im Sinne von Definition 6.8) und $\tau : V \times W \to T$ die bilineare Abbildung gegeben durch $(v_i, w_j) \mapsto \delta_{i,j}$, vergleiche Lemma 6.5. Dann ist (T, τ) ein Tensorprodukt von V und W.

Beweis. Wir schreiben $v_i \otimes w_j$ für $\delta_{i,j}$. Sei U ein weiterer K-Vektorraum und $\xi \in \mathrm{Bil}_K(V, W, U)$. Da $(v_i \otimes w_j)_{(ij)\in I\times J}$ eine Basis von T ist, gibt es genau ein $\xi_\otimes \in \mathrm{Hom}_K(T, U)$ mit $\xi_\otimes(v_i \otimes w_j) = \xi(v_i, w_j)$ für alle i, j, also mit $\xi_\otimes \circ \tau = \xi$ nach Lemma 6.5. Die universelle Eigenschaft ist somit erfüllt. □

Satz 6.11
Es gibt ein bis auf Isomorphie (im Sinne von Lemma 6.7) eindeutig bestimmtes Tensorprodukt

$$(V \otimes_K W, \otimes)$$

von V und W. Sind V und W endlichdimensional, so ist

$$\dim_K(V \otimes_K W) = \dim_K(V) \cdot \dim_K(W)$$

Beweis. Lemma 6.10 und Lemma 6.7 □

■ **Beispiel 6.12**
Durch die Wahl der Standardbasis erhält man einen kanonischen Isomorphismus $K^m \otimes_K K^n \cong \mathrm{Mat}_{m\times n}(K)$.

■ **Beispiel 6.13**
Ist V ein $\mathbb{R}$-Vektorraum mit Basis $(x_1, ..., x_n)$, so ist $\mathbb{C} \otimes_\mathbb{R} V$ ein $\mathbb{R}$-Vektorraum der Dimension $2n$ mit Basis $(1 \otimes x_1 ..., 1 \otimes x_n, i \otimes x_1, ..., i \otimes x_n)$. Durch $\lambda \cdot z \otimes x = (\lambda z) \otimes x$ für $\lambda, z \in \mathbb{C}$, $x \in V$ wird $\mathbb{C} \otimes_\mathbb{R} V$ zu einem $\mathbb{C}$-Vektorraum der Dimension $1 \otimes x_1, ..., 1 \otimes x_n$, $V_\mathbb{C}$, genannt die Komplexifizierung von V.

Satz 6.14
Sei $V \otimes_K W$ ein Tensorprodukt von V und W. Für jeden weiteren K-Vektorraum U liefert die Abbildung $\xi \to \xi_\otimes$ ein Isomorphismus

$$\mathrm{Bil}_K(V, W, U) \xrightarrow{\cong} \mathrm{Hom}_K(V \otimes_K W, U)$$

Beweis. Diese Abbildung heiße Λ.

- Λ ist linear: klar aus Eindeutigkeitsaussage, z.B.

$$(\xi_\otimes + \xi'_\otimes) \circ \otimes = \xi_\otimes \circ \otimes + \xi'_\otimes \circ \otimes = \xi + \xi' = (\xi + \xi')_\otimes \circ \otimes$$

  und somit $\xi_\otimes + \xi'_\otimes = (\xi + \xi')_\otimes$.
- Λ ist injektiv: Ist $\xi \neq 0$, so wegen $\xi = \xi_\otimes \circ \otimes$ auch $\xi_\otimes \neq 0$.
- Λ ist surjektiv: Ist $f \in \mathrm{Hom}_K(V \otimes_K W, U)$, so ist $\xi = f \circ \otimes$ bilinear, die universelle Eigenschaft liefert somit $f = \xi_\otimes \in \mathrm{Im}(\Lambda)$. □

Folgerung 6.15
Sind V und W endlichdimensional, so ist

$$V \otimes_K W \cong \mathrm{Bil}_K(V, W, K)^*$$

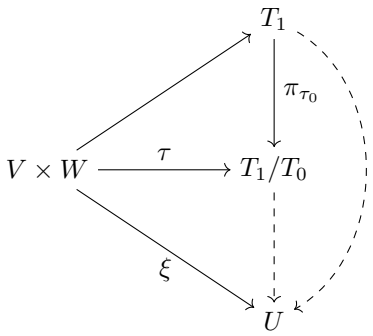
Beweis. Es ist $\dim_K(V \otimes_K W) < \infty$ und deshalb

$$V \otimes_K W \cong (V \otimes_K W)^{**} \overset{6.14}{\cong} \mathrm{Bil}_K(V, W, K) \qquad \square$$

▶ **Bemerkung 6.16**
Während obige Konstruktion des Tensorprodukts von der Wahl (und Existenz) von Basen abhängt, ist die folgende Konstruktion "basisfrei":
Sei T_1 der K-Vektorraum mit Basis $V \times W$ und T_0 der Untervektorraum von T_1 erzeugt von Elementen der Form:

$$\begin{aligned} \delta_{v+v',w} - \delta_{v,w} - \delta_{v',w} \\ \delta_{v,w+w'} - \delta_{v,w} - \delta_{v,w'} \\ \delta_{\lambda v,w} - \lambda \cdot \delta_{v,w} \\ \delta_{v,\lambda w} - \lambda \cdot \delta_{v,w} \end{aligned}$$

mit $v, v' \in V$, $w, w' \in W$ und $\lambda \in K$. Sei weiter $T = T_1/T_0$ und $\tau : V \times W \to T$ gegeben durch $(v, w) \mapsto \delta_{v,w} + T_0$. Dann ist (T, τ) ein Tensorprodukt von V und W.



▶ **Bemerkung 6.17**
Analog kann man für $k \geq 2$ und die K-Vektorräume $V_1, ..., V_k$ k-lineare Abbildungen $V_1 \times ... \times V_k \to U$ definieren und erhält dann Tensorprodukte $V_1 \otimes_K ... \otimes_K V_k$.

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

▶ **Bemerkung 1.3**
Sei M ein R-Modul. Wie für Vektorräume (LAAG 1 II.1.5) überzeugt man sich leicht, dass $0x = 0$, $a0 = 0$, $(-a)x = a(-x) = -ax$ für alle $a \in R$, $x \in M$.

Im Gegensatz zu Vektorräumen folgt aber aus $ax = 0$ nicht, dass $a = 0$ oder $x = 0$, siehe zum

Beispiel das $\mathbb{Z}$-Modul $M = \mathbb{Z}/n\mathbb{Z}$. Es ist

$$n \cdot \overline{1} = \overline{n} = \overline{0} \in \mathbb{Z}/n\mathbb{Z}$$

aber $0 \neq n \in \mathbb{Z}$.

Definition 1.4 (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.

■ **Beispiel 1.5**

- Ist $R = K$, so sind die R-Homomorphismen genau die lineare Abbildungen.
- Ist $R = \mathbb{Z}$, so sind die R-Homomorphismen genau die Gruppenhomomorphismen.

■ **Beispiel 1.6**
Für jedes $a \in R$ ist die Abbildung

$$\begin{cases} M \to M \\ x \mapsto ax \end{cases}$$

einen Endomorphismus von M.

Definition 1.7 (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.

▶ **Bemerkung 1.8**
Wieder ist der Kern eines R-Homomorphismus $f : M \to M'$ ein Untermodul von M. Leicht sieht man auch hier, dass $\sum_{i \in I} Rx_i$ ein Untermodul von M ist, und zwar der kleinste, der alle x_i enthält.

■ **Beispiel 1.9**

- Ist $R = K$ ein Körper, so sind die Untermoduln von M genau die Untervektorräume.
- Ist $R = \mathbb{Z}$, so sind die Untermoduln von M genau die Untergruppen und der von einer Familie erzeugte Untermodul ist genau gleich der davon erzeugten Untergruppe.
  Ist zum Beispiel $M = \mathbb{Z}$, so sind alle $n\mathbb{Z}$ Untermoduln von M.

Definition 1.10 (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 .

Satz 1.11
Seien M, M' R-Moduln, $(x_i)_{i\in I}$ eine Basis von M und $(y_i)_{i\in I}$ eine Familie in M'. Dann gibt es genau eine R-lineare Abbildung $f : M \to M'$ mit $f(x_i) = y_i$ für alle i.

Beweis. klar, siehe LAAG 1 III.5.1 □

■ **Beispiel 1.12**

- Für $n \in \mathbb{N}$ ist $M = R^n$ mit komponentenweiser Addition und Skalarmultiplikation ein endlich erzeugter freier R-Modul mit der üblichen Standardbasis.
- Allerdings ist zum Beispiel der $\mathbb{Z}$-Modul $\mathbb{Z}/n\mathbb{Z}$ zwar endlich erzeugt aber nicht frei. Für $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ ist $n\overline{a} = \overline{0}$, also $\overline{a}$ linear abhängig.

Definition 1.13 (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.

▶ **Bemerkung 1.14**
Wie auch für Vektorräume ist eine externe direkte Summe eine direkte Summe der entsprechenden Untermoduln und ist $M = \bigoplus_{i\in I} N_i$, so ist M isomorph zur externen direkten Summe der N_i.

Definition 1.15 (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.

Satz 1.16
Für $a \in R$ ist $M[a]$ ein Untermodul von M. Ist R nullteilerfrei, so ist auch M_{tor} ein Untermodul von M.

Beweis. $M[a]$ ist der Kern des Endomorphismus $x \mapsto ax$ (Beispiel 1.6), somit ein Untermodul (Bemerkung 1.8). Seien $a, b \in R\backslash\{0\}$ und $x \in M[a]$, $y \in M[b]$. Ist R nullteilerfrei so ist $ab \neq 0$ und

$$(ab) \cdot (x + y) = b \cdot \underbrace{ax}_{=0} + a \cdot \underbrace{by}_{=0} = 0$$

also $x + y \in M[ab] \subseteq M_{tor}$. Somit ist M_{tor} in diesem Fall einer Untermodul von M. □

■ **Beispiel 1.17**
Sei $R = \mathbb{Z}$ und $M = \mathbb{Z}/n\mathbb{Z}$, dann ist $M_{tor} = M = M[n]$.

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 $b = ax$.

Mathematica/WolframAlpha-Befehle (Teiler)
Möchte man mit Mathematica bzw. WolframAlpha überprüfen, ob n von m geteilt wird, also $m \mid n$ (!), kann man folge Funktion aufrufen:

```
Divisible[n,m]
```

Eine Liste der Teiler einer Zahl x erhält man mit

```
Divisors[x]
```

Lemma 2.2
Für $a, b, c, d \in R$ gelten

1. $a \mid a$
2. $a \mid b$ und $b \mid c \Rightarrow a \mid c$
3. $a \mid b$ und $a \mid c \Rightarrow a \mid (b + c)$
4. $a \mid b$ und $c \mid d \Rightarrow (ac) \mid (bd)$

Beweis. klar □

Lemma 2.3
Für $a, b, c, d \in R$ gelten

1. $a \sim a$
2. $a \sim b$ und $b \sim c \Rightarrow a \sim c$
3. $a \sim b \Rightarrow b \sim a$
4. $a \sim b$ und $c \sim d \Rightarrow (ac) \sim (bd)$

Beweis. klar, da $(R^\times, \cdot)$ eine Gruppe ist. □

▶ **Bemerkung 2.4**
Teilbarkeit auf R ist insbesondere eine Präordnung , das heißt reflexiv und transitiv, und Assoziiertheit ist eine Äquivalenzrelation.

Lemma 2.5
Sei R nullteilerfrei und seien $a, b \in R$. Genau dann ist $a \sim b$, wenn $a \mid b$ und $b \mid a$.

Beweis.
- Hinrichtung: $b = ax$ mit $x \in R^\times \Rightarrow a = bx^{-1}$.
- Rückrichtung: $b = ax$, $a = by$ mit $x, y \in R^\times$

$$a = by = axy$$
$$a(1 - xy) = 0$$

Also $a = 0$ und damit $b = 0$ oder $xy = 1$, also $x, y \in R^\times$. In beiden Fällen folgt $a \sim b$. □

■ **Beispiel**
Offenbar $2 \mid -2$ und $-2 \mid 2$. Es gilt $2 \sim -2$ und $-2 \sim 2$.

Satz 2.6
Sie R nullteilerfrei. Mit $[a] := \{a' \in R \mid a \sim a'\}$ wird durch $[a][b] \iff a \mid b$ eine wohldefinierte Halbordnung auf $R/\sim := \{[a] \mid a \in R\}$ gegeben.

Beweis.

- wohldefiniert: $a \mid b$, $a \sim a'$, $b \sim b' \Rightarrow a' \mid b'$: $ax = b$, $au = a'$, $bv = b$ mit $x \in R$ und $u, v \in R^\times$

$$b' = bv = axv = a' \underbrace{u^{-1}vx}_{\in R}$$

  also $a' \mid b'$.
- reflexiv: klar
- transitiv: aus Transitivität von $\mid$
- antisymmetrisch: Lemma 2.5 □

Definition 2.7 (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 $c = \mathrm{ggT}(a, b)$, 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 $c = \mathrm{kgV}(a, b)$, wenn gilt: $a \mid c$ und $b \mid c$ und ist $d \in R$ mit $a \mid d$ und $b \mid d$, so ist $c \mid d$.

Mathematica/WolframAlpha-Befehle (ggT und kgV)
Die Funktionen für den größten gemeinsamen Teiler und das kleinste gemeinsame Vielfache in Mathematica bzw. WolframAlpha sind

```
GCD[6,12,4,32]
LCM[6,12,4,32]
```

▶ **Bemerkung 2.8**
Wenn ggT und kgV in einem nullteilerfreien Ring R existieren, sind sie eindeutig bestimmt, aber nur bis auf Assoziiertheit (Lemma 2.5).

Definition 2.9 (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 $x = ab \Rightarrow a \in R^\times \vee b \in R^\times$.

▶ **Bemerkung 2.10**
Leicht sieht man: Ist $p \in R$ prim und $a_1, ..., a_n \in R$ mit $p \mid (a_1 \dots a_n)$, so gilt $p \mid a_i$ für ein i.

■ **Beispiel 2.11**

- In $R = \mathbb{Z}$ gilt: p prim $\iff$ p irreduzibel
- Sei $f \in R = \mathbb{Q}[t]$.
  - $\deg(f) = 1 \Rightarrow f \sim (t - a)$ ist irreduzibel und prim (denn $(t - a) \mid g \iff g(a) = 0$)
  - $\deg(f) = 2$: $f = t^2 - 1$ ist nicht irreduzibel, $t^2 - 2$ ist irreduzibel

Satz 2.12
Sei R nullteilerfrei und $0 \neq p \in R \backslash R^\times$. Ist p prim, so ist es auch irreduzibel.

Beweis. Sei $p = ab$ mit $a, b \in R$. Da insbesondere $p \mid ab$ und p prim ist, folgt $p \mid a$ oder $p \mid b$. Sei ohne Einschränkung $p \mid a$, das heißt $a = pa'$ mit $a' \in R$.

$$\begin{aligned} &\Rightarrow p = ab = pa'b \\ &\Rightarrow p(1 - ab) = 0 \\ &\Rightarrow a'b = 1, \text{ insbesondere } b \in R^\times \end{aligned}$$

Somit ist p irreduzibel. □

▶ **Bemerkung 2.13**
Erinnerung: Ein Ideal von R ist eine Untergruppe $I \subseteq (R, +)$ mit

$$a \in I, r \in R \Rightarrow ra \in I$$

also genau ein Untermodul des R-Moduls R.

Definition 2.14 (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 .

▶ **Bemerkung 2.15**
Das von A erzeugte Ideal $\langle A \rangle$ ist gleich dem von A erzeugten Untermodul des R-Moduls R, und ist das kleinste Ideal von R, das A enthält.

▶ **Bemerkung 2.16**
Für $a \in R$ ist $(a) = Ra$ und für $a, b \in R$ sind äquivalent:

1. $a \mid b$
2. $b \in (a)$
3. $(b) \subseteq (a)$

Für R nullteilerfrei sind zudem äquivalent:

1. $a \sim b$
2. $(a) = (b)$

■ **Beispiel 2.17**
Jeder Ring hat die Ideale $(0) = \{0\}$ und $(1) = R$. Für jedes $a \in R^\times$ ist $(a) = (1)$, ist R also ein Körper, so hat R keine weiteren Ideale.

■ **Beispiel 2.18**
In $R = \mathbb{Z}$: Für $n \in \mathbb{Z}$ ist $(n) = \mathbb{Z} \cdot n = n\mathbb{Z}$.

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.

■ **Beispiel 3.4**

1. Auf $R = \mathbb{Z}$ ist der Absolutbetrag
$$\delta(x) = |x|$$
eine euklidische Gradfunktion. (LAAG 1 I.4.6)
2. Auf $R = K[t]$, K ein Körper, ist der Grad
$$\delta(f) = \deg(f)$$
eine euklidische Gradfunktion. (LAAG 1 I.6.5)
3. $R = K$ ein Körper ist
$$\delta(x) = 0$$
eine euklidische Gradfunktion, da man in einem Körper jedes Element durch jedes Element (Ausnahme: 0) teilen kann.

Lemma 3.5
Sei $\delta : R\backslash\{0\} \to \mathbb{N}_0$ eine euklidische Gradfunktion und $(0) \neq \trianglelefteq R$ ein Ideal. Ist $0 \neq a \in I$ mit $\delta(a) = \min\{\delta(b) \mid 0 \neq b \in I\}$, so ist $I = (a)$.

Beweis.
- "$\supseteq$": $a \in I \Rightarrow (a) \subset I$
- "$\subseteq$": Sei $0 \neq b \in I$. Schreibe $b = qa + r$ mit $q, r \in R$ und $r = 0$ oder $\delta(r) < \delta(a)$. Da $r = \underbrace{b}_{\in I} - q\underbrace{a}_{\in I} \in I$ folgt wegen der Minimalität von $\delta(a)$, dass $r = 0$, also $b \in (a)$. □

Satz 3.6
Ist R euklidisch, so ist R ein Hauptidealring.

Beweis. Sei $I \trianglelefteq R$ ein Ideal. Ist $I = (0)$, so ist I ein Hauptideal. Andernfalls existiert ein $0 \neq a \in I$ mit $\delta(a)$

minimal. Nach Lemma 3.5 ist $I = (a)$ ein Hauptideal. □

Folgerung 3.7
Die Ringe $\mathbb{Z}$ und $K[t]$, K ein Körper, sind Hauptidealringe.

Lemma 3.8 (Lemma von Bézout)
Sei R ein Hauptidealring und $a, b \in R$. Es existiert ein $c \in R$ mit $c = \text{ggT}(a, b)$ und $(c) = (a, b)$. Insbesondere gibt es $x, y \in R$ mit $c = ax + by$ und $\text{ggT}(x, y) = 1$.

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

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

Satz 3.9
Sei R ein Hauptidealring, $p \in R$. Ist p irreduzibel, so auch prim.

Beweis. Seien $a, b \in R$ mit $p \mid (ab)$. Angenommen $p \nmid a$. DA p irreduzibel ist, ist $\text{ggT}(p, a) = 1$, also $1 = px + ay$ mit $x, y \in R$ nach Lemma 3.8. Also $p \mid (pbx + aby) = b$. □

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.

Lemma 4.2
Sei R faktoriell und $x \in R$. Ist x irreduzibel, so auch prim.

Beweis. Sei x irreduzibel, insbesondere $0 \neq x \in R \backslash R^\times$. Da R faktoriell, ist $x = p_1, ..., p_n$ mit $p_1, ..., p_n \in R$ prim. Da x irreduzibel ist und $p_i \notin R^\times$ ist $n = 1$ und somit $x = p_1$ prim. □

Lemma 4.3
Sei R ein Hauptidealring und

$$I_1 \subseteq I_2 \subseteq ...$$

eine Kette von Idealen in R. Dann existiert ein $n \in \mathbb{N}$ mit $I_n = I_m$ für alle $m \geq n$.

Beweis. Behauptung: $I = \bigcup_{n=1}^{\infty} I_n$ ist wieder ein Ideal von R.
Beweis: schon in den Übungen zum Teil behandelt, aber hier noch mal kurz bewiesen

- $i \in I$, $r \in R \Rightarrow x \in I_n$ für ein $n \overset{I_n \trianglelefteq}{\Rightarrow} rx \in I_n \subseteq I$
- $x, y \in I \Rightarrow x \in I_n, y \in I_m$ mit $n, m \in \mathbb{N} \overset{\text{Kette}}{\Rightarrow} x + y \in I_k \subseteq$ mit $k = \max\{n, m\}$

Da R Hauptidealring ist, ist somit $I = (x)$ für ein $x \in R$. Mit $I = \bigcup_{n\in\mathbb{N}} I_n$ folgt $x \in I_n$ für ein n, und somit $(x) \subseteq I_n \subseteq I_m \subseteq I = (x)$, für $m \geq n$, also $I_n = I_m$. □

Satz 4.4
Ist R ein Hauptidealring, so ist R faktoriell.

Beweis. Sei $X := \{a \in R \mid a \text{ ist Produkt von Primelementen}\} \cup \{0\} \cup R^\times$. Zu zeigen ist $X = R$. Angenommen, es gebe $a \in R\backslash X$. Da nicht prim ist, insbesondere nicht irreduzibel (Satz 3.9), ist $a = a_1 \cdot a_1'$ mit $a_1, a_1' \in R\backslash R^\times$. Wären a_1 und a_1' in X, so auch a, also ohne Einschränkung $a_1 \notin X$. Fährt man nun mit a_1 so fort, erhält man eine Folge $a_1, a_2, ...$ von Elementen von $R\backslash X$ mit $a_{i+1} \mid a_i$ und $a_{i+1} \not\sim a_i$ für alle i. Die entsprechenden Hauptideale bilden eine Kette

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq ...$$

im Widerspruch zu Lemma 4.3. Somit ist $X = R$, also R faktoriell. □

Anmerkung
Es gilt also euklidisch ⇒ Hauptidealring ⇒ faktoriell.

Lemma 4.5
Sind $p_1, ..., p_r \in R$ prim, $q_1, ..., q_s \in R$ irreduzibel mit

$$\prod_{i=1}^{r} p_i = \prod_{j=1}^{s} q_j$$

ist $r = s$ und nach Umnummerierung ist

$$p_i \sim q_i \quad \forall i$$

Beweis. Wir zeigen die Behauptung unter der schwächeren Annahme

$$\prod_{i=1}^{r} p_i \sim \prod_{j=1}^{s} q_j$$

durch Induktion nach r.
$\underline{r = 0}$: $1 \sim \prod_{j=1}^{s} q_j \Rightarrow q_j \in R^\times \ \forall j \overset{q_j \text{ irred.}}{\Rightarrow} s = 0$
$\underline{r - 1 \to r}$: $p_1 \mid \prod_{i=1}^{r} p_i \sim \prod_{j=1}^{s} q_j \overset{p_1 \text{ prim}}{\Rightarrow} p_1 \mid q_j$ für ein j. Nach Umnummerierung ist $j = 1$. Da q_1 irreduzibel und $p_1 \notin R^\times$ ist $p_1 \sim q_1$, also $q_1 = p_1 \cdot u$ mit $u \in R^\times$. Es folgt

$$p_1 \cdot \left(\prod_{i=2}^{r} p_i - u \cdot \prod_{j=2}^{s} q_j \right) = 0$$

$$\prod_{i=2}^{r} p_i = u \cdot \prod_{j=2}^{s} q_j \sim \prod_{j=2}^{s} q_j$$

Nach Induktionshypothese ist $r - 1 = s - 1$, und nach Umnummerierung ist $p_i \sim q_i$ für $i = 2, ..., r$. □

Satz 4.6
Ist R faktoriell, so lässt sich jedes $0 \neq x \in R \backslash R^\times$ auf eindeutige Weise (bis auf Reihenfolge und Assoziiertheit) als Produkt von Primelementen schreiben.

Beweis. Sei $x = \prod_{i=1}^{r} p_i = \prod_{j=1}^{s} q_j$ mit p_i, q_j prim. Da die q_j nach Satz 2.12 irreduzibel sind, folgt $r = s$ und $p_i \sim q_i$ für alle i aus Lemma 4.5. □

Folgerung 4.7
Sei R faktoriell und enthalte $\mathcal{P} \subseteq R$ für jede Äquivalenzklasse assoziierter Primelemente genau einen Vertreter. Dann lässt sich jedes $0 \neq a \in R$ als

$$a = \varepsilon \cdot \prod_{p \in \mathcal{P}} p^{\mu(p)}$$

mit eindeutig bestimmten $\varepsilon \in R^\times$ und $\mu(p) \in \mathbb{N}_0$, fast alle gleich 0, schreiben.

Beispiel 4.8

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 $x \mapsto x + N$.

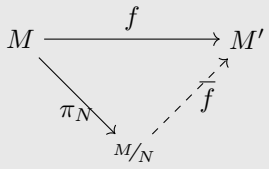
Lemma 5.2
Addition und Skalarmultiplikation sind wohldefiniert und machen M/N zu einem R-Modul. Die Abbildung $\pi_N : M \to M/N$ ist ein R-Epimorphismus mit Kern

$$\mathrm{Ker}(\pi_N) = N$$

Beweis.
- wohldefiniert: wie in LAAG 1 III.7.5
- M/N ist R-Modul: wie in LAAG 1 III.7.7 □

▶ **Bemerkung 5.3**
Durch $x \sim_N x' \iff x - x' \in N$ wird eine Äquivalenzrelation $\sim_N$ auf M definiert, und $x + N$ ist eine $\sim_N$-Äquivalenzklasse $[x]_{\sim_N} = \{y \in M \mid x \sim_N y\}$.

Satz 5.4 (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 $f = \overline{f} \circ \pi_N$.



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. □

Lemma 5.5
Durch $U \mapsto \pi_N(U)$ wird eine Bijektion gegeben zwischen

- den Untermoduln von M, die N enthalten
- den Untermoduln von ${}^{M}/_{N}$.

Beweis. Sei $\mathcal{U}$ die Menge der Untermoduln von M, die N enthalten, $\overline{\mathcal{U}}$ die Menge der Untermoduln von ${}^{M}/_{N}$.

- $U \in \mathcal{U} \Rightarrow \pi_N(U) \in \overline{\mathcal{U}}$: klar, da π_N ein Homomorphismus ist
- $\overline{U} \in \overline{\mathcal{U}} \Rightarrow \pi_N^{-1} \in \mathcal{U}$: klar, da π_N ein Homomorphismus ist und $N = \mathrm{Ker}(\pi_N) = \pi_N^{-1}(\{0\}) \subseteq \pi_N^{-1}(\overline{U})$
- $\overline{U} \in \overline{\mathcal{U}} \Rightarrow \pi_N(\pi_N^{-1}(\overline{U})) = \overline{U}$: klar, da π_N surjektiv
- $U \in \mathcal{U} \Rightarrow \pi_N^{-1}(\pi_N(U)) = U$:

$$\begin{aligned}\pi_N^{-1}(\pi_N(U)) &= \bigcup_{x \in U} \pi_N^{-1}(\pi_N(x)) \\ &= \bigcup_{x \in U} \pi_N^{-1}(x + N) \\ &= \bigcup_{x \in U} (x + N) \\ &= U + N = U\end{aligned}$$

□

▶ **Bemerkung 5.6**
Das Ideal $I \trianglelefteq R$ ist ein Untermodul des R-Moduls R, somit haben wir ein R-Modul ${}^{R}/_{I}$ definiert. Man kann ${}^{R}/_{I}$ mit einer Ringstruktur ausstatten.

Definition 5.7 (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 Quotientenring von R modulo I mit Addition und Skalarmultiplikation

$$\begin{aligned}(x + I) + (x' + I) &= (x + x') + I \quad \forall x, x' \in R \\ (x + I) \cdot (x' + I) &= (x \cdot x') + I \quad \forall x, x' \in R\end{aligned}$$

Und wieder $\pi_I : R \to {}^{R}/_{I}$ mit $x \mapsto x + I$.

Satz 5.8
Addition und Multiplikation sind wohldefiniert und machen ${}^{R}/_{I}$ zu einem kommutativen Ring mit Einselement. π_I ist ein Ringhomomorphismus mit Kern

$$\mathrm{Ker}(\pi_I) = I$$

Beweis.

- Addition wohldefiniert: Lemma 5.2
- Multiplikation wohldefiniert: Sind $x, x', y, y' \in R$ mit

$$x + I = x' + I$$
$$y + I = y' + I$$

Dann ist

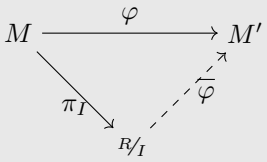
$$x - x' = a \in R \quad \Rightarrow x = x' + a$$
$$y - y' = b \in R \quad \Rightarrow y = y' + a$$

Also

$$xy = (x' + a)(y' + b) = x'y' + \underbrace{ay' + x'b + ab}_{\in I}$$
$$\Rightarrow xy + I = x'y' + I$$

- R/I ist Ring: R1 bis R3 folgen aus den entsprechenden Eigenschaften von R.
- R/I ist kommutativ: folgt auch aus den Eigenschaften von R.
- Einselement: $1 + I$
- π_I ist ein Ringhomomorphismus: folgt nach Definition
- $\mathrm{Ker}(\pi_I)$: klar □

Satz 5.9 (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 $\overline{\varphi} \circ \pi_I = \varphi$.



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. □

■ **Beispiel 5.10**

- $R = \mathbb{Z}$, $\forall n \in \mathbb{N}$ ist $n\mathbb{Z}$ ein Ideal.

$$\mathbb{Z}/(n) = \mathbb{Z}\backslash n\mathbb{Z}$$

- Sei K ein Körper und sei $a \in K$. Dann ist $K[t] \to K$, $P \mapsto P(a)$ ist ein Ringepimorphismus.

Der Kern $\mathrm{Ker}(\varphi) = (t-a)$, also alle Polynome, die in a eine Nullstelle haben. Es folgt

$$K[t]/(t-a) \cong K$$

☺ $\mathbb{Z}$ ist der Herr der Ringe ☺

■ **Beispiel 5.11**

Sei $0 \neq p \in K[t]$. $K[t]/(p)$ ist ein Ring, aber auch ein $K[t]$-Modul und damit ein K-Vektorraum.

$$\dim_K \left(K[t]/(p)\right) = n = \deg(p)$$

Ist $B = (1, \overline{t}, ..., \overline{t^{n-1}})$ eine Basis wobei $\overline{x} = \pi_{(p)}(x)\ \forall x \in K[t]$.

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

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

Lemma 6.2

Ist $ax - by \in R^\times$, so ist

$$E_{ij}(a,b,x,y) \in \mathrm{GL}_n(\mathbb{R})$$

Beweis. Folgt aus LAAG1 IV.3.4, da

$$\det(E_{ij}(a,b,x,y)) = ax - by \in R^\times$$

Oder direkt: Das Inverse ist $E_{ij}(xc^{-1}, bc^{-1}, ac^{-1}, -yc^{-1})$, zum Beispiel

$$\begin{pmatrix} a & b \\ y & x \end{pmatrix} \begin{pmatrix} xc^{-1} & -bc^{-1} \\ -yc^{-1} & ac^{-1} \end{pmatrix} = \begin{pmatrix} (ax-by)c^{-1} & 0 \\ 0 & (ax-by)c^{-1} \end{pmatrix}$$

□

▶ **Bemerkung 6.3**

Multiplikation von $E_{ij}(a,b,x,y)$ von links an A führt eine Zeilenumformung durch: Sind $a_1, ..., a_n$ die Zeilen von A, so wird a_i durch $aa_i + ba_j$ ersetzt, und gleichzeitig a_j durch $ya_i + xa_j$ ersetzt. Ist $ax - by = 1$, so sind diese Zeilenumformungen invertierbar.

Spezialfälle: elementare Zeilenumformungen von Typ II und III aus Kapitel III (LAAG 1). War-

nung: Im Gegensatz dazu sind über einem Ring R die elementaren Zeilenumformungen vom Typ I (Multiplikation mit einem Skalar) nicht immer invertierbar!

Multiplikation mit $E_{ij}(a,b,x,y)$ von rechts führt entsprechende Spaltenumformungen durch.

Theorem 6.4 (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. □

Mathematica/WolframAlpha-Befehle (Smith-Normalform)
Elementarteiler einer Matrix A lassen sich mit Mathematica mit der Funktion

```
SmithDecomposition[A]
```

die als einziges Argument eine Matrix braucht. Allerdings ist der Output unformatiert, mit folgenden Befehl sieht das deutlich besser aus:

```
MatrixForm/@ ({u,r,v} = SmithDecomposition[A])
```

Der Output sind 3 Matrizen, wobei `u` für S, `v` für T und `r` für das Ergebnis von SAT steht.

▶ **Bemerkung 6.5**
Man kann zeigen, dass die $d_1, ..., d_r$ bis auf Assoziiertheit eindeutig bestimmt sind. Man nennt sie deshalb Elementarteiler der Matrix A.

■ **Beispiel 6.6**
Sei $R = \mathbb{Z}$. Die Elementarteiler von

$$A = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 6 \end{pmatrix}$$

sind

$$\begin{pmatrix} 4 & 0 \\ 0 & 6 \end{pmatrix} \to \begin{pmatrix} 4 & 0 \\ 4 & 6 \end{pmatrix} \to \begin{pmatrix} 4 & 0 \\ -2 & 6 \end{pmatrix} \to \begin{pmatrix} 2 & -6 \\ 4 & 0 \end{pmatrix} \to \begin{pmatrix} 2 & 0 \\ 4 & 12 \end{pmatrix} \to \begin{pmatrix} 2 & 0 \\ 0 & 12 \end{pmatrix}$$

2, 2 und 12.

Anmerkung (Teil 1)
Um die Elementarteiler der Matrix A_0 zu ermitteln, muss man geschickt mit Matrizen S und T multiplizieren. Dazu starten wir links oben bei Element $a_{11} \neq 0$ und versuchen nun, auf der ersten Spalte und auf der ersten Zeile nur Nullen zu produzieren, aber $a_{11} \neq 0$ zu erhalten.

Dazu fangen wir mit der ersten Spalte an. Ziel ist es, das letzte Element dieser Spalte durch geschickte Addition der vorletzten Spalte zu 0 werden zu lassen. Wir schauen uns die letzten 2 Elemente, nennen wir sie x und y, dieser ersten Spalte an und bestimmen $\mathrm{ggT}(x, y)$. Weiterhin suchen wir u und v, sodass folgende Gleichung erfüllt ist:

$$\mathrm{ggT}(x, y) = u \cdot x + v \cdot y$$

Da wir eine Zeilenoperation durchführen wollen, brauchen wir eine Matrix S_0, die wir von links an A ranmultiplizieren. Dabei müssen wir auf die richtige Dimension von S_0 aufpassen. Dazu setzen wir S_0 auf $\mathbb{1}_m$ und fügen an der richtigen Stelle die Matrix S_0' ein:

$$S_0' = \begin{pmatrix} u & v \\ -\frac{y}{\mathrm{ggT}(x,y)} & \frac{x}{\mathrm{ggT}(x,y)} \end{pmatrix}$$

Jetzt bestimmen wir $A_1 := A_0 \cdot S_0$. Jetzt haben wir das letzte Element der ersten Spalte zu 0 verwandelt. Wir arbeiten uns jetzt in der ersten Spalte nach oben, versuchen also das vorletzte Element zu 0 zu verwandeln, aber mithilfe der vorvorletzten Zeile. Auch dazu bestimmen wir wieder Matrizen $S_1, S_2, ...$ bis die erste Spalte 0 ist, mit Ausnahme von a_{11}.

Anmerkung (Teil 2)
Jetzt wenden wir uns der ersten Zeile zu: Auch hier versuchen wir das letzte Element zu 0 zu verwandeln, aber eben mit Benutzung der vorletzten Spalte. Die Vorgehensweise ist nahezu identisch, wir bestimmen auch wieder $\mathrm{ggT}(x, y)$ und lösen

$$\mathrm{ggT}(x, y) = u \cdot x + v \cdot y$$

Damit bauen wir uns wieder T_0', die wir an der passenden Stelle in $T_0 = \mathbb{1}_n$ einsetzen

$$T_0' = \begin{pmatrix} u & -\frac{y}{\mathrm{ggT}(x,y)} \\ v & \frac{x}{\mathrm{ggT}(x,y)} \end{pmatrix}$$

Die Matrix T_0 multiplizieren wir aber diesmal von rechts an A_n. So arbeiten wir uns wieder von hinten nach vorne. Es kann passieren, dass wir uns damit leider wieder in der ersten Spalte ein paar Nullen kaputt machen, aber dann bauen wir wieder eine S_n-Matrix mit der wieder Nullen erscheinen. Falls das wieder die Spalten kaputt macht, dann multiplizieren wir wieder mit einer T_n-Matrix. Das Theorem 6.4 garantiert uns, dass wir irgendwann fertig werden.

Anmerkung (Teil 3)
Haben wir nun die erste Zeile und die erste Spalte zu 0 verwandelt, außer a_{11} natürlich, kümmern wir uns um die Untermatrix in Richtung rechts unten. Hier geht der Algorithmus von vorne los; das Schöne ist, dass er uns die erste Zeile/Spalte nicht mehr kaputt machen kann. Irgendwann sind wir rechts unten angekommen und haben nur noch Elemente auf der Hauptdiagonalen stehen. Diese sollten, wie in Theorem 6.4 behauptet eine solche Teilerkette bilden. Tun sie das nicht, kann man wieder mit Matrizen S_n und T_n nachhelfen.

$$S'_n = \begin{pmatrix} u & v \\ -\frac{y}{\mathrm{ggT}(x,y)} & \frac{x}{\mathrm{ggT}(x,y)} \end{pmatrix} \quad T'_n = \begin{pmatrix} 1 & -\frac{vy}{\mathrm{ggT}(x,y)} \\ 1 & \frac{ux}{\mathrm{ggT}(x,y)} \end{pmatrix}$$

$$\text{unter Vorbehalt! } S'_n = \begin{pmatrix} 1 & 1 \\ -\frac{vy}{\mathrm{ggT}(x,y)} & \frac{ux}{\mathrm{ggT}(x,y)} \end{pmatrix}$$

Und dann sind wir endlich fertig! Die Transformationsmatrizen S und T sind dann einfach

$$S = S_1 \cdot S_2 \cdot ...$$
$$T = T_1 \cdot T_2 \cdot ...$$

Weitere Informationen und Beispiele findet man auf http://www.igt.uni-stuttgart.de/eiserm/lehre/2010/Algebra/Matrizenringe.pdf, ab Abschnitt §7D

Lemma 6.7
Ist M ein endlich erzeugter freier R-Modul und $N \subseteq M$ ein Untermodul, so ist auch N endlich erzeugt.

Beweis. Sei $(x_1, ..., x_m)$ eine Basis von M. Induktion nach m.
$\underline{m = 1:}$ Durch $1 \mapsto x_1$ wird nach Satz 1.11 eine R-lineare Abbildung $f : R \to M$ gegeben, die ein Isomorphismus ist. Der Untermodul $N \subseteq M$ entspricht einem Ideal $I := f^{-1}(N)$ von R. Da R ein Hauptidealring ist, ist $I = (a)$ für ein $a \in R$, somit $N = f(I) = R \cdot f(a)$. Insbesondere ist N endlich erzeugt, sogar von einem Element.
$\underline{m - 1 \to m:}$ Definiere $M' = \sum_{i=1}^{m-1} Rx_i$, $M'' = Rx_m$, $N' = N \cap M'$. Sei unter $\pi : M \to M''$ die R-lineare Abbildung gegeben nach Satz 1.11 durch $\pi(x_i) = \delta_{i,m} x_m$. Nach Induktionshypothese ist N' endlich erzeugt, etwa $N' = \sum_{j=1}^{n} Ry_j$. Aus dem Fall $m = 1$ sehen wir zudem, dass $N'' = \pi(N) = R\pi(y)$ für ein $y \in N$. Sei $\tilde{N} = Ry + \sum_{j=1}^{n} Ry_j \subseteq N$. Da $\mathrm{Ker}(\pi|_N) = M'' \cap N = N' \subseteq \tilde{N}$ und $\pi|_N(\tilde{N}) \supseteq R\pi(y) = N'' = \pi|_N(N)$ ist $\tilde{N} = N$ nach Lemma 5.5 und Satz 5.4. Somit ist N endlich erzeugt. □

Satz 6.8 (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 $(d_1 x'_1, ..., d_r x'_r)$ eine Basis von N ist.

Beweis. Sei $B = (x_1, ..., x_m)$ eine Basis von M. Nach Lemma 6.7 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 6.4 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. □

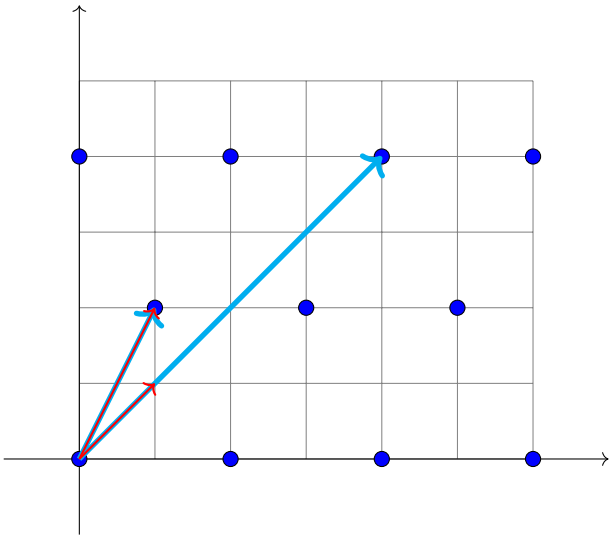
■ **Beispiel**

Sei $R = \mathbb{Z}$, $M = \mathbb{Z}^2$, $N = \mathbb{Z}\begin{pmatrix}2\\0\end{pmatrix} + \mathbb{Z}\begin{pmatrix}1\\2\end{pmatrix}$

$$\begin{pmatrix}2&1\\0&2\end{pmatrix} \to \begin{pmatrix}1&2\\2&0\end{pmatrix} \to \begin{pmatrix}1&0\\2&-4\end{pmatrix} \to \begin{pmatrix}1&0\\0&4\end{pmatrix}$$

$$\Rightarrow B = \left(\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\4\end{pmatrix}\right) \Rightarrow B' = \left(\begin{pmatrix}1\\2\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}\right)$$

$$\Rightarrow C = \left(1 \cdot \begin{pmatrix}1\\2\end{pmatrix}, 4 \cdot \begin{pmatrix}1\\1\end{pmatrix}\right) \text{ ist Basis von } N$$



▶ **Bemerkung 6.9**

Wieder kann man zeigen, dass $d_1, ..., d_r$ bis auf Einheiten eindeutig bestimmt sind.

Folgerung 6.10
Ist R ein Hauptidealring, so ist ein Untermodul eines endlich erzeugten freien R-Moduls wieder frei.

▶ **Bemerkung 6.11**
Folgerung 6.10 wird falsch ohne "R Hauptidealring". So ist zum Beispiel $N = (x, y) \trianglelefteq \mathbb{Q}[x, y] = (\mathbb{Q}[x])[y] = R = M$ kein Hauptideal und somit ein nicht freier Untermodul des freien R-Moduls R: Je zwei Elemente von R sind linear abhängig, für $a, b \in R$ ist

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

Deshalb kann N keine Basis mit mehr als einem Element besitzen.

Die Voraussetzung "endlich erzeugt" ist hingegen nicht notwendig, aber der Beweis wird dadurch einfacher.

Folgerung 6.12
Ist R ein Hauptidealring, so ist ein Untermodul eines endlich erzeugten R-Moduls M wieder endlich erzeugt.

Beweis. Ist $M = \sum_{j=1}^{m} Ry_j$, so betrachte die R-lineare Abbildung $f : R^m \to M$ gegeben durch $f(e_j) = y_j$ für $j = 1, ..., m$. Nach Lemma 6.7 ist $f^{-1}(N) \subseteq R^m$ endlich erzeugt, etwa $f^{-1}(N) = \sum_{i=1}^{n} Rx_i$. Somit ist $N = f(f^{-1}(N)) = \sum_{i=1}^{n} R \cdot f(x_i)$ endlich erzeugt. □

Theorem 6.13 (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 6.8 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 $(d_1x_1, ..., d_nx_n)$ eine Basis von N ist. Nach dem Homomorphiesatz ist

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

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 $y = 0$. □

▶ **Bemerkung 6.14**
Auch hier sind $d_1, ..., d_n$ (bis auf Einheiten) sowie r eindeutig bestimmt. Man nennt r den (freien) Rang von M.

■ **Beispiel 6.15**
Eine endlich erzeugte abelsche Gruppe A ist von der Form

$$A \cong \mathbb{Z}^r \oplus \bigoplus_{i=1}^{k} {}^{\mathbb{Z}}/_{d_i\mathbb{Z}}$$

mit (eindeutig bestimmten) $d_1, ..., d_k \in \mathbb{N}$, $d_1 \mid d_2 \mid ... \mid d_k$.

7. Zyklische Vektorräume

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

▶ **Bemerkung 7.1**
Wir betrachten V als $K[t]$-Modul mit $P(t) \cdot x = P(f)(x)$, vergleiche .
Erinnerung: V heißt f-zyklisch $\iff \exists x \in V$ mit $V = \mathrm{span}_K(x, f(x), f^2(x), ...)$. Ist k minimal mit $f^k(x) \in \mathrm{span}_K(x, f(x), f^2(x), ..., f^{k-1}(x))$, so ist $\underbrace{(x, ..., f^{k-1}(x))}_{B}$ eine Basis von V und $M_B(f) = M_{\chi_f}$.

Satz 7.2
Es gibt einen $K[t]$-Modul-Isomorphismus

$$V \cong \bigoplus_{i=1}^{m} {}^{K[t]}/_{(P_i)}$$

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

Beweis. Nach Theorem 6.13 ($K[t]$ Hauptidealring) ist

$$V \cong K[t]^r \oplus \bigoplus_{i=1}^{m} {}^{K[t]}/_{K[t] \cdot P_i}$$

mit $P_i \in K[t]\backslash K$, $P_i \mid P_{i+1}$ $\forall i$. Da $\dim_K(K[t]) = \infty > \dim_K(V)$ ist, ist $r = 0$, und wir können ohne Einschränkung P_i normiert annehmen. □

Lemma 7.3
Für $P \in K[t]$ sei $W := {}^{K[t]}/_{(P)}$. Durch $f_t(x) = \bar{t}x$ wird $f_t \in \mathrm{End}_K(W)$ definiert, wobei $\bar{t} = t + (P) = \pi_{(P)}(t) \in {}^{K[t]}/_{(P)}$. Genau dann ist $\varphi \in \mathrm{Hom}_K(V, W)$ ein $K[t]$-Modul-Homomorphismus, wenn $\varphi(f(x)) = f_t(\varphi(x))\ \forall x \in V$.

Beweis.
- $f_t \in \mathrm{End}_K(W)$: klar
- Es gilt

$$\begin{aligned} \varphi \text{ ist } K[t]\text{-Modul-Homomorphismus} &\iff \varphi(ax) = a\varphi(x) \quad \forall a \in K[t], \forall x \in V \\ &\iff \varphi(tx) = t\varphi(x) \quad \forall x \in V \\ &\iff \varphi(f(x)) = f_t(\varphi(x)) \quad \forall x \in V \end{aligned}$$

□

Satz 7.4
Genau dann ist ${}^{K[t]}/_{(P)}$ (als $K[t]$-Modul), wenn V f-zyklisch ist. In diesem Fall ist

$$\chi_f = P_f = P$$

Beweis.
- Hinrichtung: Der K-Vektorraum $W = {}^{K[t]}/_{(P)}$ ist erzeugt von $1, \bar{t} = f_t(1), \bar{t}^2 = f_t^2(1), ...$, wobei $\bar{t} = t + (P)$ und somit ist W f_t-zyklisch mit Basis $C = (1, \bar{t}, \bar{t}^2, ..., \bar{t}^{n-1})$, wobei $n = \deg(P)$. Auch ist $M_C(f_t) = M_P$. Ist $V \cong {}^{K[t]}/_{(P)}$ so ist dann V f-zyklisch.
- Rückrichtung: Ist umgekehrt V ein K-Vektorraum mit Basis $B = (x, f(x), ..., f^{n-1}(x))$, so ist $M_B(f) = M_P$ für $P = \chi_f$. Der K-Vektorraum-Homomorphismus $\varphi : V \to W = {}^{K[t]}/_{(P)}$ gegeben durch $\varphi(f^i(x)) = t^i$ ist dann ein $K[t]$-Modul-Isomorphismus.
- Ist $V \cong W$ als $K[t]$-Modul, so ist $\chi_f = \chi_{f_t}$, $P_f = P_{f_t}$. Aus $M_C(f_t) = M_P$ folgt somit

$$\chi_f = \chi_{f_t} = P$$

Ist $0 \neq Q \in K[t]$ mit $\deg(Q) < \deg(P)$, so ist

$$Q(f_t)(1) = Q(\bar{t}) \neq 0$$

da $Q \neq 0$ und C Basis, insbesondere $Q(f_t) \neq 0 \in \mathrm{End}_K({}^{K[t]}/_{(P)})$. Da $P_{f_t} \mid \chi_{f_t}$ gilt, folgt

$$P_f = P_{f_t} = \chi_{f_t} = P$$

□

Folgerung 7.5
V ist direkte Summe f-zyklischer Untervektorräume.

Folgerung 7.6
Es gilt

$$\chi_f \mid (P_f)^n$$

Insbesondere haben χ_f und P_f die selben irreduziblen Faktoren.

Beweis. In der Situation von Satz 7.2 ist

$$\chi_f = \prod_{i=1}^{m} P_i$$
$$P_f = \mathrm{kgV}(P_1, ..., P_m) = P_m$$

Da $P_i \mid P_m$ für alle i folgt $\chi_f \mid (P_m)^m$, insbesondere $\chi_f \mid (P_m)^n$, denn $m \leq n$. □

Folgerung 7.7 (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.

► **Bemerkung 7.8**
Im Gegensatz zur JORDAN-Normalform existiert die FROBENIUS-Normalform für beliebige Körper K und beliebige Endomorphismen f. Man kann zeigen, dass die Frobenius-Normalform eines Endomorphismus f eindeutig bestimmt ist.

Anhang

Anhang A: Listen

A.1. Liste der Theoreme

A.2. Liste der benannten Sätze, Lemmata und Folgerungen

A.3. Liste der Mathematica/WolframAlpha-Befehle

☺ für faule Mathematiker ☺