Kurzskript zur Vorlesung „Lineare Algebra II“

von H.-G. Rück

Sommersemester 2001

In diesem Kurzskript werden lediglich die wichtigsten Definitionen und Sätze zusammengefaßt. Es ersetzt keinesfalls den Besuch der Vorlesung, da alle Kommentare, Beispiele und Beweise fehlen.

1 Bilinearformen, adjungierte Abbildungen, Orthogonalisierung

Seien K ein Körper und V ein Vektorraum über K.

Definition 1.1. Eine lineare Abbildung $\lambda : V \to K$ heißt *Linearform auf* V. Den Vektorraum $V^* = \{\lambda : V \to K \mid \lambda \text{ Linearform}\}$ bezeichnet man als den *dualen Vektorraum zu* V.

Bemerkung. Es ist $V^* = \mathrm{Hom}_K(V, K)$ und deshalb ein Vektorraum mit „punktweiser“ Addition und Skalarmultiplikation.

Lemma 1.1. Es sei V ein endlich-dimensionaler K-Vektorraum, dann gilt: $\dim_K V = \dim_K V^*$.

Definition 1.2. Sei $(v_1, \ldots, v_n)$ eine Basis von V, dann heißt die Basis $(\lambda_1, \ldots, \lambda_n)$ von V^* mit $\lambda_i(v_j) = \left\{ \begin{array}{ll} 1, & i = j \\ 0, & i \neq j \end{array} \right\}$ die zugehörige *Dualbasis*.

In Matrizenschreibweise:
Sei $\mathcal{B} = (v_1, \ldots, v_n)$ eine Basis von V mit zugehöriger Dualbasis $(\lambda_1, \ldots, \lambda_n)$, dann ist $M^{\mathcal{B}}_{(1)}(\lambda_i) = (0 \ldots 0\, 1\, 0 \ldots 0)$ (die „1“ steht an der $i-$ten Stelle) und
$M^{\mathcal{B}}_{(1)}(\sum_{i=1}^{n} k_i\lambda_i) = (k_1\, k_2 \ldots k_n)$.

Sei nun $F : V \to V$ ein Endomorphismus und sei weiterhin $\lambda \in V^*$ eine Linearform, so kann man die Hintereinanderausführung betrachten:

$$V \xrightarrow{F} V \xrightarrow{\lambda} K,$$

sie ist wieder eine Linearform. Man betrachtet somit die Abbildung

$$\begin{array}{rccl} F^* : & V^* & \longrightarrow & V^* \\ & \lambda & \longmapsto & F^*(\lambda) := \lambda \circ F \end{array}$$

Lemma 1.2. F^* ist ein Endomorphismus von V^* (und heißt *duale Abbildung* zu F).

In Matrizenschreibweise:
Sei $\mathcal{B} = (v_1, \ldots, v_n)$ eine Basis von V und sei $\mathcal{B}^*$ die zugehörige Dualbasis von V^*.

Lemma 1.3. Für $F \in \mathrm{End}_K(V)$ gilt:

$$M^{\mathcal{B}^*}_{\mathcal{B}^*}(F^*) = \left(M^{\mathcal{B}}_{\mathcal{B}}(F)\right)^T.$$

Definition 1.3. Sei V ein K-Vektorraum, eine Abbildung $\phi : V \times V \to K$ heißt *Bilinearform,* falls gilt:

i) $\phi(v_1 + v_2, w) = \phi(v_1, w) + \phi(v_2, w)$ für alle $v_1, v_2, w \in V$,
ii) $\phi(k\,v, w) = k\,\phi(v, w)$ für alle $v, w \in V$, $k \in K$,
iii) $\phi(v, w_1 + w_2) = \phi(v, w_1) + \phi(v, w_2)$ für alle $v, w_1, w_2 \in V$,
iv) $\phi(v, k\,w) = k\,\phi(v, w)$ für alle $v, w \in V$, $k \in K$.

ϕ heißt *symmetrisch* , falls $\phi(v, w) = \phi(w, v)$ für alle $v, w \in V$; ein symmetrisches ϕ heißt *nicht-ausgeartet* , falls folgendes gilt: wenn $\phi(v, w) = 0$ für alle $v \in V$, dann ist $w = 0$.

Beispiel. Sei $A \in M_{n\times n}(K)$, betrachte $\phi : K^n \times K^n \to K$ mit $\phi(x, y) = x^T \cdot A \cdot y$.

Lemma 1.4. Sei V ein K-Vektorraum mit Basis $\mathcal{B} = (v_1, \ldots, v_n)$ und sei ϕ eine Bilinearform auf V, $\phi_{\mathcal{B}} : K^n \to V$ sei die Koordinatenabbildung. Man betrachte die Matrix $M^{\mathcal{B}}(\phi) = \big(\phi(v_i, v_j)\big)_{i,j}$, dann gilt für alle $v, w \in V$

$$\phi(v, w) = \big(\phi_{\mathcal{B}}^{-1}(v)\big)^T \cdot M^{\mathcal{B}}(\phi) \cdot \phi_{\mathcal{B}}^{-1}(w).$$

Spezialfall. $V = K^n$, $\mathcal{B} = (e_1, \ldots, e_n)$ die Standardbasis und $A \in M_{n\times n}(K)$, dann gilt für $\phi : K^n \times K^n \to K$ mit $\phi(x, y) = x^T \cdot A \cdot y$ die Gleichheit $M^{\mathcal{B}}(\phi) = A$.

Lemma 1.5. ϕ ist genau dann symmetrisch, wenn $M^{\mathcal{B}}(\phi) = M^{\mathcal{B}}(\phi)^T$. ϕ ist genau dann nicht-ausgeartet, wenn $\det M^{\mathcal{B}}(\phi) \neq 0$ und $M^{\mathcal{B}}(\phi) = M^{\mathcal{B}}(\phi)^T$.

Lemma 1.6. Seien $\mathcal{B}, \widetilde{\mathcal{B}}$ Basen von V, dann gilt für die Matrizen zu einer Bilinearform ϕ:

$$M_{\widetilde{\mathcal{B}}}^{\mathcal{B}}(id_V)^T \cdot M^{\widetilde{\mathcal{B}}}(\phi) \cdot M_{\widetilde{\mathcal{B}}}^{\mathcal{B}}(id_V) = M^{\mathcal{B}}(\phi).$$

Sei ϕ eine Bilinearform auf V sei $v \in V$, dann ist $\phi(v, \cdot) : V \to K$ mit $w \mapsto \phi(v, w)$ eine Linearform. Man erhält somit eine Abbildung $\delta_\phi : V \to V^*$ mit $v \mapsto \phi(v, \cdot)$.

Satz 1.1. Sei $\phi : V \times V \to K$ eine nicht-ausgeartete, symmetrische Bilinearform, dann ist δ_ϕ ein K-Vektorraum-Isomorphismus von V nach V^*.

Definition 1.4. Sei ϕ eine nicht-ausgeartete, symmetrische Bilinearform. Sei $F \in \mathrm{End}_K(V)$, ein Endomorphismus $\widetilde{F} \in \mathrm{End}_K(V)$ mit $\phi\big(\widetilde{F}(v), w\big) = \phi\big(v, F(w)\big)$ für alle $v, w \in V$ heißt *zu F adjungierte Abbildung* .

Satz 1.2. Sei ϕ wie oben. Dann gibt es zu jedem $F \in \mathrm{End}_K(V)$ genau eine adjungierte Abbildung $\widetilde{F}$.

Definition 1.5. F heißt selbstadjungiert, falls $\widetilde{F} = F$.

In Matrizenschreibweise:
Sei $\mathcal{B}$ eine Basis von V, dann gilt:

$$M_{\mathcal{B}}^{\mathcal{B}}(\widetilde{F}) = M^{\mathcal{B}}(\phi)^{-1} \cdot M_{\mathcal{B}}^{\mathcal{B}}(F)^T \cdot M^{\mathcal{B}}(\phi).$$

Falls $M^{\mathcal{B}}(\phi) = E_n$, gilt somit $M_{\mathcal{B}}^{\mathcal{B}}(\widetilde{F}) = M_{\mathcal{B}}^{\mathcal{B}}(F)^T$.

Definition 1.6. Sei ϕ eine nicht-ausgeartete, symmetrische Bilinearform auf einem K-Vektorraum V. Eine Basis $\mathcal{B} = (v_1, \ldots, v_n)$ von V heißt *Orthogonalbasis* bzgl. ϕ, wenn $\phi(v_i, v_j) = 0$ für alle $i \neq j$.

Satz 1.3. Sei ϕ wie oben, dann gibt es eine Orthogonalbasis von V bzgl. ϕ. (Wir setzen ab jetzt voraus, daß char $K \neq 2$, d. h. $1 + 1 \neq 0$ in K.)

Definition 1.7. Sei ϕ wie oben, eine Basis $(v_1, \ldots, v_n)$ von V heißt *Orthonormalbasis* , falls

$$\phi(v_i, v_j) = \begin{cases} 0, & \text{für } i \neq j \\ 1, & \text{für } i = j. \end{cases}$$

Korollar zu Satz 1.3. Sei ϕ wie oben (nicht-ausgeartet, symmetrisch); ϕ hat genau dann eine Orthonormalbasis, wenn es eine Orthogonalbasis $(v_1, \ldots, v_n)$ gibt, so daß $\phi(v_i, v_i)$ ein Quadrat in K^* ist für alle $i = 1, \ldots, n$.

Lemma 1.7. Sei ϕ wie oben und sei $\mathcal{B} = (v_1, \ldots, v_n)$ eine Orthonormalbasis. Sei $\widetilde{\mathcal{B}} = (\widetilde{v}_1, \ldots, \widetilde{v}_n)$ eine weitere Basis von V mit Übergangsmatrix $M_{\mathcal{B}}^{\widetilde{\mathcal{B}}}(id_V) = (a_{ij})$, d. h.

$$\widetilde{v}_i = \sum_{j=1}^{n} a_{ji}\, v_j,$$

so ist $(\widetilde{v}_1, \ldots \widetilde{v}_n)$ genau dann ebenfalls eine Orthonormalbasis, wenn $M_{\mathcal{B}}^{\widetilde{\mathcal{B}}}(id_V)^T \cdot M_{\mathcal{B}}^{\widetilde{\mathcal{B}}}(id_V) = E_n$ ist.

Definition 1.8. Matrizen $M \in M_{n\times n}(K)$ mit $M^T \cdot M = E_n$ heißen *orthogonale Matrizen* .

Sei nun speziell $K = \mathbb{R}$. Ein $x \in \mathbb{R} \setminus \{0\}$ ist genau dann ein Quadrat, wenn $x > 0$. Wann hat eine nicht-ausgeartete, symmetrische Bilinearform über $\mathbb{R}$ eine Orthonormalbasis?

Definition 1.9. Eine nicht-ausgeartete, symmetrische Bilinearform ϕ über einem $\mathbb{R}$-Vektorraum V heißt *positiv-definit,* wenn $\phi(v, v) > 0$ für alle $v \in V$ mit $v \neq 0$.

Satz 1.4. Eine nicht-ausgeartete, symmetrische Bilinearform über $\mathbb{R}$ hat genau dann eine Orthonormalbasis, wenn sie positiv definit ist.

Erhard Schmidtsches Orthonormalisierungsverfahren:

Sei ϕ positiv-definit und sei $(v_1, \ldots, v_n)$ eine Basis von V.
1) Wähle $\widetilde{v}_1 = v_1$ und normiere $w_1 = \widetilde{v}_1/\sqrt{\phi(\widetilde{v}_1, \widetilde{v}_1)}$, dann gilt $\phi(w_1, w_1) = 1$.
2) Wähle $\widetilde{v}_2 = \lambda_1 w_1 + v_2$, so daß $\phi(\widetilde{v}_2, w_1) = 0$. Das bedeutet $\lambda_1 = -\phi(v_2, w_1)$. Normiere $w_2 = \widetilde{v}_2/\sqrt{\phi(\widetilde{v}_2, \widetilde{v}_2)}$.
3) Wähle $\widetilde{v}_3 = \lambda_1 w_1 + \lambda_2 w_2 + v_3$, so daß $\phi(\widetilde{v}_3, w_1) = 0$ und $\phi(\widetilde{v}_3, w_2) = 0$. Das bedeutet $\lambda_1 = -\phi(v_3, w_1)$ und $\lambda_2 = -\phi(v_3, w_2)$. Normiere $w_3 = \widetilde{v}_3/\sqrt{\phi(\widetilde{v}_3, \widetilde{v}_3)}$.
...
Allgemein wähle $\widetilde{v}_{k+1} = v_{k+1} - \phi(v_{k+1,} w_1)w_1 - \cdots - \phi(v_{k+1}, w_k)w_k$ und normiere

$w_{k+1} = \widetilde{v}_{k+1}/\sqrt{\phi(\widetilde{v}_{k+1}, \widetilde{v}_{k+1})}$.
Als Ergebnis erhält man eine Orthonormalbasis $(w_1, \ldots, w_n)$ bzgl. ϕ.

Beispiel. $V = \mathbb{R}^n, < x, y >:= \sum_{i=1}^n x_i y_i$. $<,>$ ist nicht-ausgeartete, symmetrische, positiv-definite Bilinearform, und die Standardbasis $(e_1, \ldots, e_n)$ ist Orthonormalbasis.

Definition 1.10. Seien V n-dimensionaler $\mathbb{R}$-Vektorraum und ϕ eine Bilinearform auf V. (V, ϕ) heißt *isomorph* zu $(\mathbb{R}^n, <,>)$, wenn es einen Vektorraumisomorphismus $F : V \to \mathbb{R}^n$ gibt mit $\phi(v, w) =< F(v), F(w) >$. (V, ϕ) heißt dann *Euklidischer Raum* der Dimension n.

Satz 1.5. (V, ϕ) ist genau dann Euklidischer Raum, wenn ϕ nicht-ausgeartet, symmetrisch und positiv definit ist.

Sei (V, ϕ) ein Euklidischer Raum, dann kann man *Längen* messen:

$$||v|| := \sqrt{\phi(v, v)} \quad \text{für} \quad v \in V.$$

Es gilt:
i) $||v|| = 0$ genau dann, wenn $v = 0$,
ii) $||\lambda\, v|| = |\lambda| \cdot ||v||$ für alle $v \in V$ und $\lambda \in \mathbb{R}$,
iii) $||v + w|| \leq ||v|| + ||w||$ für alle $v, w \in V$.

Man kann auch *Winkel* messen:

$$\cos \alpha(v, w) := \frac{\phi(v, w)}{||v|| \cdot ||w||} \quad \text{für} \quad v, w \in V.$$

Insbesondere „steht v genau dann senkrecht auf w“, wenn $\phi(v, w) = 0$.

Wichtig für diese Eigenschaften der Länge und des Winkels ist:

Satz 1.6. (Cauchy-Schwarzsche Ungleichung) Sei ϕ nicht-ausgeartet, symmetrisch, positiv definit, dann gilt

$$|\phi(v, w)| \leq ||v|| \cdot ||w|| \quad \text{für alle} \quad v, w \in V.$$

Definition 1.11. Sei (V, ϕ) Euklidscher Raum. Ein Endomorphismus $F \in \mathrm{End}_{\mathbb{R}}(V)$ heißt *orthogonal* , falls $\phi\big(F(v), F(w)\big) = \phi(v, w)$ für alle $v, w \in V$.

Bemerkung. Orthogonale Abbildungen sind längen- und winkelerhaltend. Es gilt aber auch umgekehrt: Jeder längenerhaltende Endomorphismus ist orthogonal, d. h. wenn $||F(v)|| = ||v||$ für alle $v \in V$, dann gilt auch $\phi\big(F(v), F(w)\big) = \phi(v, w)$ für alle $v, w \in V$.

Lemma 1.8. $F \in \mathrm{End}_{\mathbb{R}}(V)$ ist genau dann orthogonal, wenn F invertierbar ist mit $\widetilde{F} = F^{-1}$.

Bemerkung. Wenn $\mathcal{B}$ eine Orthonormalbasis für ϕ und wenn F orthogonal ist, dann gilt $M_{\mathcal{B}}^{\mathcal{B}}(F)^T \cdot M_{\mathcal{B}}^{\mathcal{B}}(F) = E_n$, d. h. $M_{\mathcal{B}}^{\mathcal{B}}(F)$ ist orthogonale Matrix.

2 Sesquilinearformen, Hermitesche Formen

Definition 2.1. Sei V ein $\mathbb{C}$-Vektorraum, $\phi : V \times V \to \mathbb{C}$ heißt *Sesquilinearform,* wenn folgendes gilt:
a) $\phi(v_1 + v_2, w) = \phi(v_1, w) + \phi(v_2, w)$ für alle $v_1, v_2, w \in V$,
b) $\phi(k\,v, w) = k \cdot \phi(v, w)$ für alle $v, w \in V$, $k \in \mathbb{C}$,
c) $\phi(v, w_1 + w_2) = \phi(v, w_1) + \phi(v, w_2)$ für alle $v, w_1, w_2 \in V$,
d) $\phi(v, k\,w) = \overline{k} \cdot \phi(v, w)$ für alle $v, w \in V$, $k \in \mathbb{C}$.

ϕ heißt *Hermitesche Form* , falls zusätzlich $\phi(v, w) = \overline{\phi(w, v)}$ für alle $v, w \in V$. Eine Hermitesche Form heißt *nicht-ausgeartet* , falls folgendes gilt: aus $\phi(v, w) = 0$ für alle $w \in V$ folgt $v = 0$.
Bei einer Hermiteschen Form gilt $\phi(v, v) = \overline{\phi(v, v)}$; also $\phi(v, v) \in \mathbb{R}$. Deshalb ist folgende Definition sinnvoll: Eine Hermitesche Form heißt *positiv-definit* , falls $\phi(v, v) > 0$ für alle $v \in V$ mit $v \neq 0$. Wenn ϕ positiv-definite Hermitesche Form ist, dann heißt (V, ϕ) *unitärer Raum* (vgl. Definition von Euklidischem Raum).

Satz 2.1. Sei ϕ eine positiv-definite Hermitesche Form auf V, dann hat V eine Orthonormalbasis $(v_1, \ldots, v_n)$ bzgl. ϕ, d. h. es gilt

$$\phi(v_i, v_j) = \begin{cases} 1, \text{falls } i = j \\ 0, \text{falls } i \neq j \ . \end{cases}$$

Spezialfall. $V = \mathbb{C}^n$, $< z, u >:= \sum_{i=1}^{n} z_i \overline{u}_i$. $< , >$ ist positiv-definite Hermitesche Form und $(e_1, \ldots, e_n)$ ist Orthonormalbasis.

Analog zu Satz 1.5. gilt:
Korollar. Sei ϕ positiv definite Hermitesche Form, dann ist (V, ϕ) isomorph zu $(\mathbb{C}^n, < , >)$, d. h. es gibt einen $\mathbb{C}$-linearen Isomorphismus $\psi : V \to \mathbb{C}^n$ mit $\phi(v, w) = < \psi(v), \psi(w) >$ für alle $v, w \in V$. Natürlich gilt auch umgekehrt: Wenn es einen solchen Isomorphismus ψ gibt, dann ist ϕ positiv-definit und Hermitesch.

Definition 2.2. Sei ϕ nicht-ausgeartete Hermitesche Form auf V. Sei $F \in \mathrm{End}_{\mathbb{C}}(V)$, ein Endomorphismus $\widetilde{F} \in \mathrm{End}_{\mathbb{C}}(V)$ mit $\phi\big(\widetilde{F}(v), w\big) = \phi\big(v, F(w)\big)$ für alle $v, w \in V$ heißt zu F *adjungierte Abbildung* .

Satz 2.2. Sei ϕ wie oben. Dann gibt es zu jedem $F \in \mathrm{End}_{\mathbb{C}}(V)$ genau eine adjungierte Abbildung $\widetilde{F}$.

Lemma 2.1. Sei ϕ eine Sesquilinearform auf V, $\mathcal{B} = (v_1, \ldots, v_n)$ eine Basis von V und $M^{\mathcal{B}}(\phi) := \big(\phi(v_i, v_j)\big)_{i,j}$, so gilt:

$$\phi(v, w) = \big(\phi_{\mathcal{B}}^{-1}(v)^T\big) \cdot M^{\mathcal{B}}(\phi) \cdot \overline{\phi_{\mathcal{B}}^{-1}(w)}.$$

In Matrizenschreibweise:
Sei ϕ eine positiv-definite Hermitesche Form, $F, \widetilde{F} \in \mathrm{End}_{\mathbb{C}}(V)$ wie oben, $\mathcal{B}$ eine

Basis von V. Dann gilt:

$$M_{\mathcal{B}}^{\mathcal{B}}(\widetilde{F}) = \overline{M^{\mathcal{B}}(\phi)}^{-1} \cdot \overline{M_{\mathcal{B}}^{\mathcal{B}}(F)}^{T} \cdot \overline{M^{\mathcal{B}}(\phi)}.$$

Falls $\mathcal{B}$ eine Orthonormalbasis für ϕ ist, d. h. falls $M^{\mathcal{B}}(\phi) = E_n$, dann gilt:

$$M_{\mathcal{B}}^{\mathcal{B}}(\widetilde{F}) = \overline{M_{\mathcal{B}}^{\mathcal{B}}(F)}^{T} .$$

Definition 2.3. Sei $\phi : V \times V \to \mathbb{C}$ eine positiv-definite Hermitesche Form. $F \in \mathrm{End}_{\mathbb{C}}(V)$ heißt *normal* (bzgl. ϕ), falls $\widetilde{F} \circ F = F \circ \widetilde{F}$.

Bemerkung. Falls F selbstadjungiert ist, d. h. falls $F = \widetilde{F}$, dann ist F normal.

Satz 2.3. (Hauptsatz) Sei ϕ positiv-definite Hermitesche Form auf V, sei $F \in \mathrm{End}_{\mathbb{C}}(V)$. Dann gilt: F ist genau dann normal, wenn es eine Orthonormalbasis für V bzgl. ϕ gibt, die aus Eigenvektoren von F besteht.

Zum Beweis benötigt man folgende Hilfssätze:

Lemma 2.2. Sei U Unterraum von V, betrachte

$$U^{\perp} := \{v \in V \mid \phi(u, v) = 0 \text{ für alle } u \in U\}.$$

Dann gilt: $U \oplus U^{\perp} = V$.

Lemma 2.3. Sei $F \in \mathrm{End}_{\mathbb{C}}(V)$ normal, dann gilt: $\mathrm{Ker}\ F = \mathrm{Ker}\ \widetilde{F}$.

Lemma 2.4. Sei F normal. Wenn v ein Eigenvektor zu F mit Eigenwert λ ist, dann ist v ein Eigenvektor zu $\widetilde{F}$ mit Eigenwert $\overline{\lambda}$.

Lemma 2.5. Sei F normal und sei v Eigenvektor von F, dann gilt:

$$F\Big(\mathrm{Lin}(v)^{\perp}\Big) \subset \mathrm{Lin}(v)^{\perp} .$$

Korollar zu Satz 2.3. Falls F selbstadjungiert ist, dann ist F diagonalisierbar und alle Eigenwerte sind reell.

Für Matrizen:
Sei ϕ positiv-definite Hermitesche Form mit Orthonormalbasis $\mathcal{B}$ (also $M^{\mathcal{B}}(\phi) = E_n$). Sei F normal, d. h. $M_{\mathcal{B}}^{\mathcal{B}}(F) \cdot \overline{M_{\mathcal{B}}^{\mathcal{B}}(F)}^{T} = \overline{M_{\mathcal{B}}^{\mathcal{B}}(F)}^{T} \cdot M_{\mathcal{B}}^{\mathcal{B}}(F)$. Dann gibt es eine Basis $\widetilde{\mathcal{B}}$, so daß $M^{\widetilde{\mathcal{B}}}(\phi) = E_n$ und

$$M_{\widetilde{\mathcal{B}}}^{\widetilde{\mathcal{B}}}(F) = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} .$$

Die Übergangsmatrix $S = M_{\widetilde{\mathcal{B}}}^{\mathcal{B}}(id_V)$ erfüllt:

$$M_{\widetilde{\mathcal{B}}}^{\mathcal{B}}(id_V) \cdot \overline{M_{\widetilde{\mathcal{B}}}^{\mathcal{B}}(id_V)} = M^{\mathcal{B}}(\phi) = E_n .$$

Definition 2.3. Eine Matrix S mit $S^T = \overline{S^{-1}}$ heißt *unitär* .

Definition 2.4. (vgl. orthogonale Abb.) Sei ϕ positiv-definite Hermitesche Form auf V. $F \in \mathrm{End}_{\mathbb{C}}(V)$ heißt *unitär* , falls $\phi(F(v), F(w)) = \phi(v, w)$ für alle $v, w \in V$.

Bemerkung. Unitäre Abbildungen sind längenerhaltend, es gilt auch umgekehrt, d. h. wenn $\phi(F(v), F(v)) = \phi(v, v)$ für alle $v \in V$, dann ist F unitär.

Lemma 2.6. $F \in \mathrm{End}_{\mathbb{C}}(V)$ ist genau dann unitär, wenn F invertierbar ist mit $F^{-1} = \widetilde{F}$.

Bemerkung. Sei $\mathcal{B}$ ein Orthonormalbasis für ϕ, dann gilt für unitäres F die Gleichung $M_{\mathcal{B}}^{\mathcal{B}}(F)^T \cdot \overline{M_{\mathcal{B}}^{\mathcal{B}}(F)} = E_n$; es ist also die Matrix $M_{\mathcal{B}}^{\mathcal{B}}(F)$ unitär.

Satz 2.4. Sei ϕ wie oben, und sei $F \in \mathrm{End}_{\mathbb{C}}(V)$ unitär, dann gibt es eine Orthonormalbasis von V bzgl. ϕ, die aus Eigenvektoren von F besteht, so daß für die Eigenwerte λ_i gilt $|\lambda_i| = 1$.

3 Hauptachsentransformation

Wir wollen die Ergebnisse für Hermitesche Formen auf reelle Vektorräume anwenden, deshalb müssen wir den Übergang von $\mathbb{R}$ nach $\mathbb{C}$ studieren.

Komplexifizierung eines reellen Vektorraums:

Betrachte die Einbettung $\mathbb{R} \hookrightarrow \mathbb{C} = \{x + i \cdot y \mid x, y \in \mathbb{R}\}$ mit $x \mapsto x + i \cdot 0$ und analog die Einbettung $\mathbb{R}^n \hookrightarrow \mathbb{C}^n$.

Wir verallgemeinern dies: Sei V ein reeller n-dimensionaler Vektorraum, wir definieren dazu den zugehörigen komplexen Vektorraum $(V_{\mathbb{C}}, +, \cdot)$ folgendermaßen:
i) die Menge: $V_{\mathbb{C}} := V \times V$,
ii) die Addition: wir nehmen die komponentenweise Addition auf $V \times V$,
iii) die Skalarmultiplikation: für $x \in \mathbb{R}$ und $(v_1, v_2) \in V_{\mathbb{C}}$ definiere $x \cdot (v_1, v_2) = (x\, v_1, x\, v_2)$, für $y \in \mathbb{R}$ und $(v_1, v_2) \in V_{\mathbb{C}}$ definiere $i \cdot y \cdot (v_1, v_2) = (-y\, v_2, y\, v_1)$, und setze dies additiv fort.

Es ist dann $V_{\mathbb{C}}$ ein Vektorraum über den komplexen Zahlen $\mathbb{C}$. Als $\mathbb{R}$-Vektorräume gelten die Einbettung $V \hookrightarrow V_{\mathbb{C}}$ mit $v \mapsto (v, 0)$ und die Zerlegung $V_{\mathbb{C}} = V \oplus i \cdot V$.

Satz 3.1. Sei $(v_1, \ldots, v_n)$ eine Basis von V über $\mathbb{R}$, dann ist auch $(v_1, \ldots, v_n)$ eine Basis von $V_{\mathbb{C}}$ über $\mathbb{C}$. Insbesondere gilt: $\dim_{\mathbb{R}} V = \dim_{\mathbb{C}} V_{\mathbb{C}}$.

Komplexifizierung einer positiv-definiten symmetrischen Bilinearform:

Sei ϕ eine positiv-definite symmetrische Bilinearform auf V, setze sie auf $V_{\mathbb{C}}$ so fort: $\phi_{\mathbb{C}}(v_1 + iv_2, w_1 + iw_2) = \phi(v_1, w_1) + \phi(v_2, w_2) + i\big(\phi(v_2, w_1) - \phi(v_1, w_2)\big)$.

$\phi_{\mathbb{C}}$ ist eine Hermitesche Form und positiv definit, da $\phi_{\mathbb{C}}(v+iw, v+iw) = \phi(v,v) + \phi(w,w)$. Falls $(v_1, \ldots, v_n)$ eine Orthonormalbasis von V bzgl. ϕ, dann ist $(v_1, \ldots, v_n)$ auch eine Orthonormalbasis von $V_{\mathbb{C}}$ bzgl. $\phi_{\mathbb{C}}$.

Komplexifizierung eines Endomorphismus:

Sei $F \in \mathrm{End}_{\mathbb{R}}(V)$, dann gibt es genau eine $\mathbb{C}$-lineare Abbildung $F_{\mathbb{C}} \in \mathrm{End}_{\mathbb{C}}(V_{\mathbb{C}})$ mit $F_{\mathbb{C}}|_V = F$. Sei $F \in \mathrm{End}_{\mathbb{R}}(V)$ mit adjungierter Abbildung $\widetilde{F}$, dann gilt $\widetilde{F}_{\mathbb{C}} = (\widetilde{F})_{\mathbb{C}}$.

Satz 3.2. (Hauptsatz) Sei V ein $\mathbb{R}$-Vektorraum, und ϕ sei eine positiv-definite symmetrische Bilinearform auf V. Sei $F \in \mathrm{End}_{\mathbb{R}}(V)$ selbstadjungiert (d. h. $\widetilde{F} = F$), dann gibt es eine Orthonormalbasis von V bzgl. ϕ, die aus Eigenvektoren von F besteht.

Definition 3.1. Die Orthonormalbasisvektoren von Satz 3.2. heißen *Hauptachsen* von F bzgl. ϕ.

Korollar zu Satz 3.2. Sei $A \in M_{n\times n}(\mathbb{R})$ mit $A = A^T$, dann gibt es $S \in GL_n(\mathbb{R})$ mit $S \cdot S^T = E_n$, so daß $S^{-1} \cdot A \cdot S = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$.

Hyperflächen 2.Ordnung:

Definition 3.2. Sei $A \in M_{n\times n}(\mathbb{R})$, $b \in \mathbb{R}^n$, $c \in \mathbb{R}$, dann heißt die Teilmenge $H = \{x \in \mathbb{R}^n \mid x^T \cdot A \cdot x + b^T \cdot x + c = 0\}$ *Hyperfläche 2. Ordnung in* $\mathbb{R}^n$.

Wir wollen den „Typ“ von H bestimmen.

1. Schritt: Symmetrisiere die Matrix $A = (a_{ij})$, d. h. suche $A' \in M_{n\times n}(\mathbb{R})$, die symmetrisch ist und die $x^T \cdot A \cdot x = x^T \cdot A' \cdot x$ erfüllt. Dazu nimmt man $A' = (a'_{ij})$ mit $a'_{ij} = \frac{1}{2}(a_{ij} + a_{ji})$.

2. Schritt (Hauptachsen): Sei jetzt A symmetrisch. Nach dem Hauptsatz (Satz 3.2) gibt es eine Matrix S mit $S \cdot S^T = E_n$, so daß $S^{-1} \cdot A \cdot S = S^T \cdot A \cdot S = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$. S ist die Übergangsmatrix von der Standardbasis zur Basis aus Satz 3.2. Setzt man $x = S\widetilde{x}$, so erhält man die Gleichung

$$\widetilde{x}^T \cdot \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \cdot \widetilde{x} + b^T \cdot S \cdot \widetilde{x} + c = 0\,,$$

eine Gleichung ohne „gemischte Glieder“. Ordnet man die Variablen noch um, so daß $\lambda_1, \ldots, \lambda_r \neq 0$ und $\lambda_{r+1} = \lambda_{r+2} = \cdots = \lambda_n = 0$, so ergibt sich $\sum_{i=1}^{r} \lambda_i \widetilde{x}_i^2 + \sum_{i=1}^{n} \widetilde{b}_i \widetilde{x}_i + c = 0$.

3. Schritt (Nullpunktwahl): Verschiebe $\widetilde{x}_i = \widetilde{\widetilde{x}}_i - \widetilde{b}_i/(2\lambda_i)$ für $i = 1, \ldots, r$, dann gilt $\sum_{i=1}^{r} \lambda_i \widetilde{\widetilde{x}}_i^2 + \sum_{i=r+1}^{n} \widetilde{b}_i \widetilde{\widetilde{x}}_i + \widetilde{\widetilde{c}} = 0$. Durch Multiplizieren mit $\widetilde{\widetilde{c}}^{-1}$ erreicht man, daß $\widetilde{\widetilde{c}} = 0$ oder -1. Ersetze man schließlich $\lambda_i = 1/a_i^2$, falls $\lambda_i > 0$ und $\lambda_i = -1/a_i^2$, falls $\lambda_i < 0$, so erhält man die

Metrische Normalform:

$$H = \left\{ x \in \mathbb{R}^n \mid \sum_{i=1}^{t} \frac{x_i^2}{a_i^2} - \sum_{i=t+1}^{r} \frac{x_i^2}{a_i^2} + \sum_{i=r+1}^{n} b_i x_i = \left\{ \begin{array}{c} 0 \\ 1 \end{array} \right\} \right.$$

Speziell im 2-dimensionalen Raum:

$n = 2$, also $r = 1$, $r = 2$ oder $r = 0$ (linearer Teilraum)

$r = 2$	$t = 2$		$\frac{x_1^2}{a_1^2} + \frac{x_2^2}{a_2^2} = 1$	Ellipse
			$\cdots = 0$	Punkt
	$t = 1$		$\frac{x_1^2}{a_1^2} - \frac{x_1^2}{a_2^2} = 1$	Hyperbel
			$\cdots = 0$	2 Geraden, die sich in $(0, 0)$ schneiden
	$t = 0$	$-$	$\frac{x_1^2}{a_1^2} - \frac{x_2^2}{a_2^2} = 1$	$\varnothing$
			$\cdots = 0$	Punkt
$r = 1$	$t = 1$		$\frac{x_1^2}{a_1^2} + b_2 x_2 = c$	Parallelen zur x_2-Achse, falls $b_2 = 0$
			$\cdots$	Parabel, falls $b_2 \neq 0$
	$t = 0$	$-$	$\frac{x_1^2}{a_1^2} + b_2 x_2 = c$	x_2-Achse, falls $b_2 = 0$ und $c = 0$
			$\cdots$	$\varnothing$, falls $b_2 = 0$ und $c = 1$
			$\cdots$	Parabel, falls $b_2 \neq 0$.

4 Moduln

Bisher betrachteten wir Vektorräume, d. h. abelsche Gruppen mit Skalarmultiplikatoren aus einem Körper. Jetzt ersetzen wir Körper durch Ring. Dabei gehen wichtige Eigenschaften verloren!

Definition 4.1. Ein kommutativer Ring R mit Einselement heißt *Integritätsbereich,* wenn aus $x, y \in R, x \neq 0, y \neq 0$ immer $x \cdot y \neq 0$ folgt.

Wir wollen hier immer Integritätsbereiche betrachten. Später werden wir uns ausschließlich auf Euklidische Ringe beschränken.

Definition 4.2. Sei R ein Integritätsbereich. Ein *Modul* über R ist eine abelsche Gruppe $(M,+)$ mit einer Verknüpfung $\cdot : R\times M \to M$ mit folgenden Eigenschaften:
i) $r\cdot(m_1+m_2) = r\cdot m_1 + r\cdot m_2$,
ii) $(r_1+r_2)\cdot m = r_1\cdot m + r_2\cdot m$,
iii) $(r_1\cdot r_2)\cdot m = r_1\cdot(r_2\cdot m)$,
iv) $1\cdot m = m$,
für alle $r, r_1, r_2 \in R$ und $m, m_1, m_2 \in M$.

Ein *Untermodul* N von M ist eine nichtleere Untermenge N von M, so daß
i) $n_1+n_2 \in N$ für alle $n_1, n_2 \in N$,
ii) $r\cdot n \in N$ für alle $n\in N$ und $r\in R$.

$(N,+,\cdot)$ ist dann ein Modul über R. R ist auch selbst ein R-Modul. Ein R-Untermodul $\mathfrak{A}$ dieses Moduls R heißt *Ideal* in R, d. h. es gilt $\mathfrak{A}\neq\varnothing$, $a_1+a_2\in\mathfrak{A}$ für alle $a_1,a_2\in\mathfrak{A}$ und $r\cdot a\in\mathfrak{A}$ für alle $r\in R, a\in\mathfrak{A}$.

Seien $M, \widetilde{M}$ beides R-Moduln, dann heißt eine Abbildung $f: M\to\widetilde{M}$ *R-Modul-Homomorphismus,* falls
i) $f(m_1+m_2) = f(m_1)+f(m_2)$,
ii) $f(r\cdot m) = r\cdot f(m)$,
für alle $m_1, m_2, m\in M$ und $r\in R$.

Ist f zusätzlich bijektiv, so heißt f *R-Modul-Isomorphismus.*
Wenn R ein Körper ist, dann ist ein R-Modul ein Vektorraum.

Definition 4.3. und Bemerkungen.
i) Seien N_1, N_2 Untermoduln eines R-Moduls M, dann ist auch
$N_1+N_2 = \{n_1+n_2 \mid n_1\in N_1,\ n_2\in N_2\}$ ein Untermodul von M und heißt *Summe* von N_1 und N_2.
ii) M heißt *direkte Summe* zweier Untermoduln N_1 und N_2, wenn $M = N_1+N_2$ und $N_1\cap N_2 = \{0\}$.
iii) Seien M_1, M_2 zwei R-Moduln, dann ist
$M_1\times M_2 = \{(m_1,m_2) \mid m_1\in M_1,\ m_2\in M_2\}$ auch ein R-Modul und heißt *direktes Produkt* von M_1 und M_2.
iv) Seien N_1, N_2 Untermoduln von M, dann ist die Abbildung $N_1\times N_2\to M$ mit $(n_1,n_2)\mapsto n_1+n_2$ genau dann ein R-Modul-Isomorphismus, wenn M direkte Summe von N_1 und N_2 ist.
v) Sei M ein R-Modul und N ein Untermodul, dann definiert man den *Quotientenmodul* M/N folgendermaßen: Zu der Äquivalenzrelation $\underset{N}{\sim}$ auf M mit $a\underset{N}{\sim} b$ genau dann, wenn $a-b\in N$ sei M/N die Menge aller Äquivalenzklassen $\{\overline{m} \mid m\in M\}$. Auf M/N erklärt man die Addition $\overline{m}_1+\overline{m}_2 = \overline{m_1+m_2}$ und

die Skalarmultiplikation $r \cdot \overline{m} = \overline{r \cdot m}$ jeweils mittels Repräsentanten. Somit wird M/N zu einem R-Modul und die Abbildung $\pi : M \to M/N$ mit $\pi(m) = \overline{m}$ zu einem surjektiven R-Modul-Homomorphismus.

Satz 4.1. Sei $f : M \to N$ ein R-Modul-Homomorphismus, Dann ist $\operatorname{Ker} f = \{m \in M \mid f(m) = 0\}$ ein R-Untermodul von M und $\operatorname{Bild} f = \{f(m) \mid m \in M\}$ ein R-Untermodul von N. Sie heißen *Kern* und *Bild* von f.
Außerdem gibt es zu jedem f einen eindeutig bestimmten R-Modul-Isomorphismus $\overline{f} : M/\operatorname{Ker} f \to \operatorname{Bild} f$ mit $f = \overline{f} \circ \pi$.

Definition 4.4. Sei M ein R-Modul, M heißt *endlich erzeugt,* falls es endliche viele Elemente $m_1, \ldots, m_n \in M$ gibt mit $M = \operatorname{Lin}(m_1, \ldots, m_n) = \{\sum_{i=1}^{n} \lambda_i m_i \mid \lambda_1, \ldots, \lambda_n \in R\}$. Ist M speziell von einem Element m erzeugt, dann heißt M *zyklischer R-Modul.*

Sei $M = \operatorname{Lin}(m) = R \cdot m$ ein zyklischer R-Modul, dann betrachte man die Abbildung $\varphi : R \to M$ mit $\varphi(r) = r \cdot m$. φ ist surjektiver R-Modul-Homomorphismus, und sein Kern $\mathfrak{A} = \operatorname{Ker} \varphi$ ist ein Ideal in R. Somit gilt nach Satz 4.1, daß M zu $R/\mathfrak{A}$ isomorph ist, d. h. jeder zyklische Modul ist isomorph zum Quotientenmodul des Rings nach einem Ideal.

Definition 4.5. Sei M ein R-Modul, ein $m \in M$ heißt *Torsionselement,* falls es ein $r \in R, r \neq 0$ gibt mit $r \cdot m = 0$.

Lemma 4.1. Sei M ein R-Modul, dann bilden die Menge aller Torsionselemente von M einen Untermodul M_t von M.

Definition 4.6. M heißt *Torsionsmodul,* wenn $M_t = M$.

Definition 4.7. M heißt *freier R-Modul,* falls es $m_1, \ldots, m_n \in M$ gibt mit der Eigenschaft: Jedes $m \in M$ hat eine eindeutige Schreibweise $m = r_1 m_1 + \ldots + r_n m_n$ mit $r_1, \ldots, r_n \in R$.

Lemma 4.2. M ist genau dann frei, wenn es einen R-Modul-Isomorphismus $R^n = R \times \ldots \times R \to M$ gibt.

Analog zu Vektorräumen definiert man den Begriff *linear unabhängig.* Dann ist die Definition eines freien Moduls äquivalent zur Existenz eines linear unabhängigen Erzeugendensystems, welches man *Basis* nennt.

Satz 4.2. Sei R ein Integritätsbereich und sei M ein freier R-Modul mit Basis $(m_1, \ldots, m_n)$. Seien $(s_1, \ldots, s_k)$ linear unabhängige Elemente aus M, dann gilt $k \leq n$. Insbesondere ist die Elementanzahl einer Basis wohlbestimmt, sie heißt *Rang von M.*

5 Moduln über Euklidischen Ringen

Definition 5.1. Ein Integritätsbereich R heißt *Euklidischer Ring,* falls es eine Funktion $g : R \setminus \{0\} \to \mathbb{N} \cup \{0\}$ gibt mit folgenden Eigenschaften:
i) $g(r_1 \cdot r_2) \geq g(r_1)$ für alle $r_1, r_2 \in R \setminus \{0\}$,
ii) aus $g(r_1) < g(r_2)$ folgt $g(r_1 \cdot r) < g(r_2 \cdot r)$ für alle $r_1, r_2, r \in R \setminus \{0\}$,
iii) für alle $a, b \in R$, $b \neq 0$ gibt es $q, r \in R$, so daß $a = q \cdot b + r$ mit $r = 0$ oder $g(r) < g(b)$.

Beispiele. In dieser Vorlesung betrachten wir ausschließlich die beiden Beispiele
a) $R = \mathbb{Z}$ mit $g(z) = |z|$ und
b) $R = K[X]$ mit $g(f(X)) = \operatorname{grad} f(X)$.

Satz 5.1. Sei R ein Euklidischer Ring und sei $\mathfrak{A} \subset R$ ein Ideal, dann ist $\mathfrak{A}$ *Hauptideal,* d. h. $\mathfrak{A} = \{0\}$ oder $\mathfrak{A}$ ist freier R-Modul vom Rang 1. (Ringe mit dieser Eigenschaft nennt man auch *Hauptidealringe*).

Satz 5.2. Seien R ein Euklidischer Ring und M ein freier R-Modul. Sei weiterhin N ein Untermodul von M. Dann ist N ebenfalls ein freier R-Modul.

Eine Basis des Untermoduls N kann man folgendermaßen induktiv berechnen:
Sei $(m_1, \ldots, m_n)$ eine Basis von M, betrachte $N_i = N \cap \operatorname{Lin}(m_1, \ldots, m_i)$. Das Ideal $\{r \in R \mid$ es gibt $m \in N_{i+1}$ mit $m = \widetilde{m} + r \cdot m_{i+1}$ und $\widetilde{m} \in N_i\}$ werde von dem Ringelement a_{i+1} erzeugt und es sei $n_{i+1} = \widetilde{m} + a_{i+1} m_{i+1}$ mit $\widetilde{m} \in N_i$, dann gilt $N_{i+1} = N_i \oplus R \cdot n_{i+1}$.
Mit anderen Worten:
Seien R ein Euklidischer Ring, M ein freier R-Modul mit Basis $(m_1, \ldots, m_n)$ und N ein Untermodul von M. Dann gibt es eine Dreiecksmatrix

$$\begin{pmatrix} a_{11} & a_{12} & & & a_{1n} \\ 0 & a_{22} & & & a_{2n} \\ \vdots & 0 & \ddots & & \\ \vdots & \vdots & & \ddots & \\ 0 & 0 & & & a_{nn} \end{pmatrix}$$

mit Koeffizienten aus R, so daß mit
$n_1 = a_{11} m_1$, $n_2 = a_{12} m_1 + a_{22} m_2$, ... , $n_n = a_{1n} m_1 + \cdots + a_{nn} m_n$
die Elemente $(n_i \mid a_{ii} \neq 0)$ eine Basis von N bilden. Es ist außerdem der Rang von N genau dann n, wenn $a_{11} \cdot a_{22} \cdot \cdots \cdot a_{nn} \neq 0$.

Satz 5.3. Sei R ein Euklidischer Ring, M sei ein endlich-erzeugter R-Modul. Wenn $M_t = \{0\}$, d. h. wenn M „torsionsfrei“ ist, dann ist M ein freier R-Modul.

Korollar. Sei M endlich-erzeugt, dann ist M/M_t ein freier R-Modul.

Satz 5.4. Seien R ein Euklidischer Ring und M ein endlich-erzeugter R-Modul. Dann gibt es einen freien Untermodul N von M mit $M = N \oplus M_t$.

Korollar. M_t ist ebenfalls endlich erzeugt.

Bemerkung. Die Sätze 5.1. – 5.4. benötigen lediglich die Voraussetzung, daß R ein Hauptidealring ist.

Zerlegung in Euklidischen Ringen

Wir wollen Elemente aus R in einfache Bestandteile zerlegen.

Definition 5.2. Ein Element $\epsilon \in R$ heißt *Einheit*, wenn es ein $\epsilon_1 \in R$ gibt mit $\epsilon \cdot \epsilon_1 = 1$. Ein Element $q \in R$ heißt *irreduzibel*, wenn q keine Einheit ist und wenn aus $q = q_1 \cdot q_2$ immer folgt, daß q_1 oder q_2 eine Einheit ist. Ein $a \in R$ *teilt* $b \in R$, wenn es ein $c \in R$ mit $b = a \cdot c$ gibt.

Satz 5.5. Sei R ein Euklidischer Ring. Dann hat jedes $r \in R$, das keine Einheit ist, eine eindeutige Zerlegung $r = q_1 \cdot \ldots \cdot q_n$ mit irreduziblen Elementen $q_1, \ldots, q_n \in R$. Die Eindeutigkeit bedeutet dabei: wenn $q_1 \cdot \ldots \cdot q_n = \widetilde{q}_1 \cdot \ldots \cdot \widetilde{q}_m$, dann gilt $m = n$ und eventuell nach Umnumerierung $q_i = \widetilde{q}_i \cdot \epsilon_i$ mit einer Einheit ϵ_i.

Größter Gemeinsamer Teiler (ggT) und Euklidischer Algorithmus

Ein *größter gemeinsamer Teiler* (ggT) von Elementen r und s aus R ist ein gemeinsamer Teiler von r und s, der Vielfaches jedes anderen gemeinsamen Teilers von r und s ist.
Wenn $r = \epsilon \cdot q_1^{a_1} \cdot \ldots \cdot q_n^{a_n}$ und $s = \tilde{\epsilon} \cdot q_1^{b_1} \cdot \ldots \cdot q_n^{b_n}$, wobei $\epsilon, \tilde{\epsilon}$ Einheiten und q_i paarweise „verschiedene“ irreduzible Elemente sind, dann ist ein ggT von r und s gegeben durch $q_1^{\min(a_1,b_1)} \cdot \ldots \cdot q_n^{\min(a_n,b_n)}$.

Einen ggT berechnet man mit dem *Euklidischen Algorithmus:*
Seien $r, s \in R$, $r, s \neq 0$, bilde $r_1 = r$, $r_2 = s$ und danach induktiv r_i mit:

$$\begin{aligned} r_1 &= q_1 r_2 + r_3 \text{ mit } g(r_3) < g(r_2) \\ r_2 &= q_2 r_3 + r_4 \text{ mit } g(r_4) < g(r_3) \\ &\vdots \\ r_{n-1} &= q_{n-1} r_n + r_{n+1} \text{ mit } g(r_{n+1}) < g(r_n) \\ r_n &= q_n r_{n+1} + 0, \end{aligned}$$

dann ist r_{n+1} ein ggT von r und s und dieser läßt sich als Linearkombination $r_{n+1} = \lambda \cdot r + \mu \cdot s$ mit $\lambda, \mu \in R$ schreiben.

6 Endlich erzeugte Torsionsmoduln über Euklidischen Ringen

Seien R ein Euklidischer Ring und $M = \mathrm{Lin}(m_1, \ldots, m_n)$ ein endlich-erzeugter Torsionsmodul über R.

Definition 6.1. $\mathrm{Ann}(M) = \{r \in R \mid r \cdot m = 0 \text{ für alle } m \in M\}$ heißt *Annullator von M.*

Bemerkung. $\mathrm{Ann}(M)$ ist ein Ideal von R und $\mathrm{Ann}(M) \neq R, \{0\}$, falls $M \neq \{0\}$. In diesem Fall erhält man $\mathrm{Ann}(M) = R \cdot a$ mit $a = \epsilon \cdot q_1^{\lambda_1} \cdot \ldots \cdot q_s^{\lambda_s}$ mit „verschiedenen“ irreduziblen Elementen q_i aus R.

Wir wollen M in kleinere Teile zerlegen:

Definition 6.2. Sei q ein irreduzibles Element in R, dann heißt $M(q) = \{m \in M \mid \text{ es gibt } k \in \mathbb{N} \text{ mit } q^k \cdot m = 0\}$ der *q-primäre Anteil von M.*

Bemerkungen. 1) $M(q)$ ist Untermodul von M.
2) $M(q) = \{0\}$, falls q nicht den Annullator a von M teilt.

Satz 6.1. Sei R ein Euklidischer Ring, M sei ein endlich-erzeugter Torsionsmodul über R. Weiterhin sei $\mathrm{Ann}(M) = R \cdot a$ mit der Zerlegung $a = \epsilon \cdot q_1^{\lambda_1} \cdot \ldots \cdot q_s^{\lambda_s}$ wie oben. Dann gilt $M = M(q_1) \oplus \ldots \oplus M(q_s)$.

Satz 6.2. Seien R ein Euklidischer Ring und M ein endlich-erzeugter Torsionsmodul, sei q ein irreduzibles Element aus R und es gelte $M = M(q)$. Dann existieren natürliche Zahlen $k_1 \geq k_2 \geq \cdots \geq k_s \geq 1$ und Elemente $m_1, \ldots, m_s \in M$ mit $M = R \cdot m_1 \oplus R \cdot m_2 \oplus \ldots \oplus R \cdot m_s$ und $R \cdot m_i \simeq R/q^{k_i}R$ für alle $i = 1, \ldots, s$. Die Zahlen $k_1, \ldots, k_s$ sind durch M eindeutig bestimmt.

Dazu sind einige Hilfsbetrachtungen, u.a. das folgende Lemma erforderlich:

Sei $m \in M \setminus \{0\}$ mit $q^k \cdot m = 0$ und $q^{k-1} \cdot m \neq 0$, dann heißt $k = \mathrm{Per}(m)$ *die Periode von m.* Wenn $m = \lambda_1 m_1 + \ldots + \lambda_l m_l$ mit $\lambda_i \in R$, dann gilt $\mathrm{Per}(m) \leq \max_{i=1,\ldots,l}(\mathrm{Per}(m_i))$. Da M endlich-erzeugt ist, gibt es deshalb in M Elemente mit maximaler Periode.

Lemma 6.1. Sei $m_1 \in M$ mit maximaler Periode k_1, bilde $M_1 = R \cdot m_1$ und $\overline{M} = M/M_1$. Sei $0 \neq \overline{b} \in \overline{M}$ mit Periode k. Dann gibt es ein $b' \in M$ mit $\pi(b') = \overline{b}$ und $\mathrm{Per}(b') = k$.

Faßt man die Sätze 5.4, 6.1 und 6.2 zusammen, so erhält man:

Satz 6.3. (Hauptsatz über endlich-erzeugte Moduln über Euklidischen Ringen) Sei R ein Euklidischer Ring, sei M ein endlich-erzeugter R-Modul. Dann gibt es eindeutig bestimmte $d \in \mathbb{N} \cup \{0\}$, $q_1, \ldots, q_r$ „verschiedene “irreduzible Elemente in R und natürliche Zahlen $(k_{11} \geq k_{12} \geq \cdots k_{1s_1} \geq 1) \ldots (k_{r1} \geq k_{r2} \geq \cdots k_{rs_r} \geq 1)$ so, daß

$$M \simeq R^d \times \left(\prod_{j=1}^{s_1} R/q_1^{k_{1j}} R \right) \times \ldots \times \left(\prod_{j=1}^{s_r} R/q_r^{k_{rj}} R \right) .$$

Wichtiges Beispiel. Wir betrachten $R = \mathbb{Z}$. $\mathbb{Z}$-Moduln sind gerade die abelschen Gruppen. Das heißt, Satz 6.3 für $R = \mathbb{Z}$ ist der Hauptsatz für endlich erzeugte abelsche Gruppen. Endliche abelsche Gruppen sind dabei endlich-erzeugte

Torsionsmoduln über $\mathbb{Z}$. Also: Jede endliche abelsche Gruppe hat die bis auf Isomorphie eindeutige Form

$$(\mathbb{Z}/p_1^{k_{11}}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_1^{k_{1s_1}}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_r^{k_{r1}}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{k_{rs_r}}\mathbb{Z})$$

mit Primzahlen $p_1, \ldots, p_r$ und natürlichen Zahlen k_{ij} wie oben.

7 Anwendungen: Normalformen von Matrizen

Sei K ein Körper, V sei K-Vektorraum der Dimension n, und sei $F \in \mathrm{End}_K(V)$. Man kann V mittels F zu einem $K[X]$-Modul machen:

Lemma 7.1. Mit der Verknüpfung $K[X] \times V \to V$, $f(X) \cdot v = f(F)(v)$ und der Vektorraum-Addition wird V zu einem $K[X]$-Modul. Dieser ist endlich-erzeugt, ist Torsionsmodul, und es ist $\mathrm{Ann}(V) = K[X] \cdot m_F(X)$, wobei $m_F(X)$ das Minimalpolynom von F ist.

Lemma 7.2. Sei $V = V_1 \oplus \ldots \oplus V_k$ eine Zerlegung von V als $K[X]$-Modul, dann ist dies auch eine Zerlegung von V als K-Vektorraum. Außerdem gilt $f(V_i) \subset V_i$ für alle $i = 1, \ldots, k$. Sei $(v_{i1}, \ldots, v_{ik_i})$ eine Basis des K-Vektorraums V_i, dann hat F bzgl. der Basis $(v_{11}, \ldots, v_{1k_1}, \ldots, v_{k1}, \ldots, v_{kk_k})$ die Kästchenform

$$\begin{pmatrix} \boxed{A_1} & & 0 \\ & \boxed{A_2} & \\ & \ddots & \\ 0 & & \boxed{A_k} \end{pmatrix}$$

wobei jeweils A_i die Matrix von $F|V_i$ bzgl. $v_{i1}, \ldots, v_{ik_i}$ ist.

Wie sehen die Bausteine von V als $K[X]$-Modul aus? Sei $m_F(X)$ das Minimalpolynom von F, zerlege dieses $m_F(X) = p_1(X)^{\lambda_1} \cdot \ldots \cdot p_s(X)^{\lambda_s}$ in irreduzible Faktoren. Berechne die $p_i(X)$-primären Komponenten von V und zerlege diese wieder in zyklische Anteile $V_{ij} = K[X] \cdot v_{ij} \simeq K[X]/p_i(X)^{k_{ij}}K[X]$.

Lemma 7.3. Sei $W = K[X] \cdot v \simeq K[X]/p(X)^k K[X]$ eine zyklische Komponente von V, wobei $p(X) \in K[X]$ ein normiertes irreduzibles Polynom ist. Sei $p(X)^k = X^m + a_{m-1}X^{m-1} + \cdots + a_1X + a_0$, dann ist $\mathcal{B} = \big(v, F(v), \ldots, F^{m-1}(v)\big)$ eine Basis

von W als K-Vektorraum und bzgl. dieser hat $F|W$ die Matrix

$$M_{\mathcal{B}}^{\mathcal{B}}(F|W) = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & \vdots & \vdots \\ \vdots & 0 & \dots & \vdots & \vdots \\ \vdots & \vdots & \dots & \vdots & \vdots \\ \vdots & \vdots & \dots & 0 & -a_{m-2} \\ 0 & 0 & \dots & 1 & -a_{m-1} \end{pmatrix}$$

Somit folgt aus dem Hauptsatz (Satz 6.3.) sofort:

Satz 7.1. (Rationale Normalform bzw. Jordan-Hölder-Normalform)
Sei V ein K-Vektorraum der Dimension n und sei $F \in \mathrm{End}_K(V)$. Dann gibt es eine Basis $\mathcal{B}$ von V, bzgl. der F folgende Matrix hat

$$M_{\mathcal{B}}^{\mathcal{B}}(F) = \begin{pmatrix} \boxed{A_1} & & & 0 \\ & \boxed{A_2} & & \\ & & \ddots & \\ & 0 & & \boxed{A_k} \end{pmatrix}$$

wobei A_i Kästchen der Form

$$A_i = M_{\mathcal{B}_i}^{\mathcal{B}_i}(F|V_i) = \begin{pmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & \vdots & \vdots \\ \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_{m-1} \end{pmatrix}$$

sind, mit $X^m + a_{m-1}X^{m-1} + \dots + a_1X + a_0 = p(X)^k$, wobei $p(X)$ jeweils irreduzible Polynome aus $K[X]$ sind. Bis auf Vertauschen der Kästchen ist die Darstellung eindeutig.

Lemma 7.4. Sei speziell $p(X) = X - a$ mit $a \in K$ und sei wieder $W = K[X] \cdot v \simeq K[X]/(X-a)^k K[X]$. Dann ist auch $\widetilde{\mathcal{B}} = \big(v, (F-a)(v), (F-a)^2(v), \dots, (F-a)^{k-1}(v)\big)$ eine Basis von W und

$$M_{\widetilde{\mathcal{B}}}^{\widetilde{\mathcal{B}}}(F|W) = \begin{pmatrix} a & 0 & \dots & 0 & 0 \\ 1 & a & \dots & \vdots & \vdots \\ 0 & 1 & \dots & \vdots & \vdots \\ \vdots & 0 & \dots & \vdots & \vdots \\ \vdots & \vdots & \dots & \vdots & \vdots \\ \vdots & \vdots & \dots & a & 0 \\ 0 & 0 & \dots & 1 & a \end{pmatrix}.$$

Somit erhält man:

Satz 7.2. (Jordan-Form)
Sei V ein K-Vektorraum der Dimension n und sei $F \in \mathrm{End}_K(V)$. Das Minimalpolynom $m_F(X)$ von F zerfalle über K in Linearfaktoren. Dann gibt es eine Basis $\widetilde{\mathcal{B}}$ von V, bzgl. der F folgende Matrix hat:

$$M_{\widetilde{\mathcal{B}}}^{\widetilde{\mathcal{B}}}(F) = \begin{pmatrix} \boxed{A_1} & & 0 \\ & \boxed{A_2} & \\ & & \ddots \\ 0 & & \boxed{A_l} \end{pmatrix}$$

wobei $\widetilde{A}_i$ Kästchen der Form

$$\widetilde{A}_i = M_{\widetilde{\mathcal{B}}_i}^{\widetilde{\mathcal{B}}_i}(F|V_i) = \begin{pmatrix} a & 0 & \dots & 0 & 0 \\ 1 & a & \dots & \vdots & \vdots \\ 0 & 1 & \dots & \vdots & \vdots \\ \vdots & \vdots & \dots & a & 0 \\ 0 & 0 & \dots & 1 & a \end{pmatrix}$$

sind. Bis auf Vertauschung der Kästchen ist die Darstellung eindeutig.

Berechnung der Normalformen

Sei $m_F(X)$ das Minimalpolynom und $\chi_F(X)$ das charakteristische Polynom von $F \in \mathrm{End}_K(V)$. Nach dem Satz von Cayley-Hamilton gilt: $m_F(X)$ teilt $\chi_F(X)$. Wir erhalten sogar noch mehr:

Lemma 7.5. Das Minimalpolynom und das charakteristische Polynom haben genau dieselben irreduziblen Faktoren.

Sei $p(X)$ ein irreduzibler Faktor von $m_F(X)$, d. h. von $\chi_F(X)$, dann gilt für die $p(X)$-primäre Komponente $V\big(p(X)\big) \simeq K[X]/p(X)^{k_1}K[X] \times \ldots \times K[X]/p(X)^{k_s}K[X]$ mit $k_1 \geq \ldots \geq k_s \geq 1$. $p(X)^{k_1}$ ist die genaue $p(X)$-Potenz in $m_F(X)$.

Wie berechnet man die Zahlen $\mathbf{k_1} \geq \cdots \geq \mathbf{k_s}$?

Sei $r \in \mathbb{N}$, dann gilt: $\mathrm{Ker}\, p(F)^r|V = \mathrm{Ker}\, p(F)^r|V\big(p(X)\big)$ und
$\dim_K \mathrm{Ker}\, p(F)^r = \mathrm{grad}\, p(X) \cdot (i_r \cdot r + k_{i_r+1} + \ldots + k_s)$ mit $i_r = \max\{i \mid k_i > r\}$.

Definiert man $l_r := \dim_K \mathrm{Ker}\, p(F)^r - \dim_K \mathrm{Ker}\, p(F)^{r-1}$, dann gilt $l_r = \mathrm{grad}\, p(X) \cdot \#\{i \mid k_i \geq r\}$ und die wichtige Formel $l_r - l_{r+1} = \#\{i \mid k_i = r\} \cdot \mathrm{grad}\, p(X)$.
Es ist klar, daß man die l_r und somit mit der Formel alle k_i aus F berechnen kann. Sinnvoll ist folgende Anordnung der Basen für die einzelnen Kerne mit Basisergänzung:

$$\overbrace{\underbrace{\operatorname{Ker} p(F) \underset{\neq}{\subset} \operatorname{Ker} p^2(F) \underset{\neq}{\subset} \cdots \underset{\neq}{\subset} \operatorname{Ker} p^{k_1}(F) = \operatorname{Ker} p^{k_1+1}(F)}_{u_1^{(1)}, \ldots, u_{l_1}^{(1)} \; u_1^{(2)}, \ldots, u_{l_2}^{(2)} \qquad\qquad u_1^{(k_1)}, \ldots, u_{l_{k_1}}^{(k_1)}}}$$

Man erhält dann eine Basis zur Normalform:

1) Suche v_1 mit maximaler Periode k_1:
Setze $v_1 = u_1^{(k_1)}$ und bilde
$V_1 = \operatorname{Lin}\big(v_1, F(v_1), \ldots, F^{k_1 \cdot \operatorname{grad} p(X)-1}(v_1)\big)$,
2) Ergänze V_1 zur Basis von V auf folgende Weise:
Nimm $v_2 \in \operatorname{Lin}\Big(V_1, \operatorname{Ker} p(F)^{k_2}\Big) \setminus \operatorname{Lin}\Big(V_1, \operatorname{Ker} p(F)^{k_2-1}\Big)$ und bilde
$V_2 = V_1 \oplus \operatorname{Lin}(v_2, F(v_2), \ldots, F^{k_2 \cdot \operatorname{grad} p(X)-1}(v_2))$,
$\vdots$
r+1) Sei jetzt V_r gebildet, dann wähle wie bei 2) durch Basisergänzung:
$v_{r+1} \in \operatorname{Lin}\big(V_r, \operatorname{Ker} p(F)^{k_{r+1}}\big) \setminus \operatorname{Lin}\big(V_r, \operatorname{Ker} p(F)^{k_{r+1}-1}\big)$.

Es gilt $V_r \cap K[X] \cdot v_{r+1} = \{0\}$, deshalb kann man $V_{r+1} = V_r \oplus K[X] \cdot v_{r+1}$ bilden. Schließlich erhält man $V_s = V$.

Bemerkung. Die Jordan-Form spielt eine wichtige Rolle beim Lösen von linearen Differentialgleichungssystemen.