Protokoll zur Vorlesung Lineare Algebra II

Prof. W. Bley

7. Juli 2021

1 Linear- und Bilinearformen

1.1 Linearformen

Definition 1.1.1 Sei V ein Vektorraum über dem Körper K. Unter einer Linearform versteht man eine lineare Abbildung $f : V \longrightarrow K$. Der Vektorraum $V^* := \mathrm{Hom}(V, K)$ heißt der Dualraum zu V.

Falls $\dim(V) = n < \infty$, so ist auch V^* von der Dimension n. Sei $v_1, \ldots, v_n$ eine Basis von V. Wenn wir K als eindimensionalen K-Vektorraum betrachten, so wählen wir stets den Vektor $1 \in K$ als Basis. Dann ist die Koordinatenmatrix einer Linearform $f : V \longrightarrow K$ bezüglich dieser gewählten Basen ein Zeilenvektor, der explizit durch

$$a = (f(v_1), \ldots, f(v_n))$$

gegeben ist. Sei $v = x_1v_1 + \ldots + x_nv_n, x_i \in K$, ein beliebiger Vektor in V. Dann ist $f(v) = a \cdot x$, wobei $x = (x_1, \ldots, x_n)^t$ der Spaltenvektor der Koordinaten von v bezüglich der Basis $v_1, \ldots, v_n$ ist.
Zu einer gegebenen Basis $v_1, \ldots, v_n$ definieren wir nun Linearformen $v_i^* : V \longrightarrow K$, $i = 1, \ldots, n$, durch

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

Proposition 1.1.2 *Sei V eine K-Vektor der Dimension $n < \infty$ und $v_1, \ldots, v_n$ eine Basis von V. Dann bilden die eben defininierten Linearformen $v_1^*, \ldots, v_n^*$ eine Basis von V^*.*

Definition 1.1.3 $v_1^*, \ldots, v_n^*$ heißt die zu $v_1, \ldots, v_n$ duale Basis.

Definition 1.1.4 Sei $h : V \longrightarrow W$ eine lineare Abbildung zwischen K-Vektorräumen V und W. Dann heißt die Abbildung

$$h^* : W^* \longrightarrow V^*, \quad f \mapsto f \circ h$$

die zu h transponierte Abbildung.

Bemerkungen 1.1.5 1) h^* ist eine lineare Abbildung.
2) Sei U ein weiterer K-Vektorraum und seien $h_1 : V \longrightarrow W, h_2 : W \longrightarrow U$ zwei lienare Abbildungen. Dann gilt $(h_2 \circ h_1)^* = h_1^* \circ h_2^*$.

Eine rein formale Konsequenz aus der zweiten Bemerkung ist die

Proposition 1.1.6 *Sei $h : V \longrightarrow W$ ein Isomorphismus. Dann ist auch $h^* : W^* \longrightarrow V^*$ ein Isomorphismus und es gilt:*

$$(h^{-1})^* = (h^*)^{-1}.$$

Der folgende Satz liefert eine begriffliche Interpretation der Transponierten einer Matrix.

Satz 1.1.7 *Sei $h : V \longrightarrow W$ eine lineare Abbildung zwischen endlich dimensionalen Vektorräumen. Seien $v_1, \ldots, v_n$ und $w_1, \ldots, w_m$ Basen von V und W. Sei A die Koordinatenmatrix von h bezüglich dieser Basen. Dann hat die lineare Abbildung $h^* : W^* \longrightarrow V^*$ bezüglich der dualen Basen $w_1^*, \ldots, w_m^*$ und $v_1^*, \ldots, v_n^*$ die Koordinatenmatrix A^t.*

Wir betrachten nun die kanonische Abbildung

$$V^* \times V \longrightarrow K, \quad (f, v) \mapsto \langle f, v\rangle = f(v).$$

Manchmal schreiben wir auch $\langle\ ,\ \rangle_V$, falls der zugrundeliegende Vektorraum nicht aus dem Kontext klar ist.
Die Abbildung $\langle\ ,\ \rangle$ ist bilinear, d.h.

$$\begin{aligned}
\langle f_1 + f_2, v\rangle &= \langle f_1, v\rangle + \langle f_2, v\rangle,\\
\langle f, v_1 + v_2\rangle &= \langle f, v_1\rangle + \langle f, v_2\rangle,\\
\langle af, v\rangle &= a\langle f, v\rangle = \langle f, av\rangle.
\end{aligned}$$

Hierbei sind $f, f_1, f_2 \in V^*$, $v, v_1, v_2 \in V$ und $a \in K$.
Ferner gilt für jede lineare Abbildung $h : V \longrightarrow W$ die Beziehung

$$\langle h^*(f), v\rangle_V = \langle f, h(v)\rangle_W$$

für alle $f \in W^*$ und $v \in V$.

Definition 1.1.8 Sei $M \subseteq V$. Dann heißt

$$M^o = \{f \in V^* \mid \langle f, v\rangle = 0, \forall v \in M\}$$

der Orthogonalraum von M.

Man zeigt sehr leicht, daß $M^o = \mathrm{Lin}(M)^o$ gilt und $M^o \subseteq V^*$ stets ein linearer Unterraum ist.
Durch Rückführung auf die Dimensionsformel für lineare Abbildung zwischen endlich dimensionalen Vektorräumen zeigt man

Proposition 1.1.9 *Sei $\dim(V) < \infty$ und $M \subseteq V$. Dann gilt:*

$$\dim(M^o) = \dim(V) - \dim(\mathrm{Lin}(M)).$$

Satz 1.1.10 *(Dualitätssatz) Die bilineare Abbildung $V^* \times V \longrightarrow K, \quad (f, v) \mapsto \langle f, v\rangle = f(v)$ ist nicht ausgeartet, d.h.*

$$\begin{aligned}
\langle f, v\rangle = 0, \forall v \in V \quad &\Longrightarrow \quad f = 0,\\
\langle f, v\rangle = 0, \forall f \in V^* \quad &\Longrightarrow \quad v = 0.
\end{aligned}$$

Falls $\dim(V) < \infty$, so ist die kanonische Abbildung

$$\begin{aligned}
V \quad &\longrightarrow \quad V^{**} = \mathrm{Hom}(\mathrm{Hom}(V, K), K),\\
v \quad &\mapsto \quad (f \mapsto \langle f, v\rangle = f(v))
\end{aligned}$$

ein Isomorphismus.

1.2 Bilinearformen

Definition 1.2.1 Seien V, W zwei K-Vektorräume. Eine Abbildung $\beta : V \times W \longrightarrow K$ heißt Bilinearform, wenn sie linear in jedem Argument ist, d.h.

$$\begin{aligned}
&\beta(v_1 + v_2, w) = \beta(v_1, w) + \beta(v_2, w), \forall v_1, v_2 \in V, w \in W \\
&\beta(v, w_1 + w_2) = \beta(v, w_1) + \beta(v, w_2), \forall v \in V, w_1, w_2 \in W \\
&\beta(av, w) = a\beta(v, w) = \beta(v, aw), \forall v \in V, w \in W, a \in K.
\end{aligned}$$

Definition 1.2.2 Sei $\beta : V \times W \longrightarrow K$ eine Bilinearform. Dann heißt β ausgeartet in der ersten Variablen, falls es ein $v \in V, v \neq 0$, gibt, so daß $\beta(v, w) = 0$ für alle $w \in W$. Analog hierzu heißt β ausgeartet in der zweiten Variablen, falls es ein $w \in W, w \neq 0$, gibt, so daß $\beta(v, w) = 0$ für alle $v \in V$.

Wie lineare Abbildungen zwischen endlich dimensionalen Vektorräumen, so lassen sich auch Bilinearformen durch eine Matrix beschreiben.

Definition 1.2.3 Sei $\dim(V) = n < \infty$ und $\dim(W) = m < \infty$. Seien $v_1, \ldots, v_n$ und $w_1, \ldots, w_m$ Basen von V und W und sei $\beta : V \times W \longrightarrow K$ eine Bilinearform. Dann heißt die $n \times m$-Matrix

$$B = (\beta(v_i, w_j))_{i=1,\ldots,n, j=1,\ldots,m}$$

die Strukturmatrix von β bezüglich der Basen $v_1, \ldots, v_n$ und $w_1, \ldots, w_m$.
Falls $V = W$ so spricht man von der Strukturbasis bezüglich der Basis $v_1, \ldots, v_n$.

Bemerkung 1.2.4 Die Strukturmatrix ist abhängig von der Wahl der Basen. Wir werden später diese Abhängigkeit genau analysieren.

Der folgende Satz zeigt, daß die Bilenearform β durch ihre Strukturmatrix vollständig bestimmt ist.

Satz 1.2.5 *Sei* $\dim(V) = n < \infty$ *und* $\dim(W) = m < \infty$. *Seien* $v_1, \ldots, v_n$ *und* $w_1, \ldots, w_m$ *Basen von* V *und* W *und sei* $\beta : V \times W \longrightarrow K$ *eine Bilinearform. Sei* B *die zugehörige Strukturmatrix. Sei*

$$\begin{aligned}
v &= x_1 v_1 + \ldots + x_n v_n, x_i \in K, \\
w &= y_1 w_1 + \ldots + y_m w_m, y_j \in K.
\end{aligned}$$

Dann gilt:

$$\beta(v, w) = (x_1, \ldots, x_n) B \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}.$$

Umgekehrt definiert jede Matrix $B \in K^{n,m}$ *auf diese Weise eine Bilinearform* $\beta : V \times W \longrightarrow K$.

Folgerung 1.2.6 *Sei* $\dim(V) = \dim(W) = n < \infty$ *und* $\beta : V \times W \longrightarrow K$ *eine Bilinearform mit Strukturmatrix* B *(bezüglich gewählter Basen). Dann sind die folgenden Aussagen äquivalent:*
a) β *ist ausgeartet im ersten Argument.*
b) β *ist ausgeartet im zweiten Argument.*
c) $\det(B) = \det(B^t) = 0$.
d) $\mathrm{rg}(B) = \mathrm{rg}(B^t) < n$.
e) $\ker(B) \neq \{0\}$.
f) $\ker(B^t) \neq \{0\}$.

Während die Aussagen a) und b) unabhängig von der Wahl von Basen sind, scheinen die restlichen Aussagen von B und damit von der Basiswahl abhängig zu sein. Der folgende Satz zeigt jedoch, daß dies nicht der Fall ist.

Satz 1.2.7 *Sei* $\dim(V) = n < \infty$ *und* $\dim(W) = m < \infty$. *Seien* $v_1, \ldots, v_n$ *und* $w_1, \ldots, w_m$ *Basen von* V *und* W *und sei* $\beta : V \times W \longrightarrow K$ *eine Bilinearform. Sei* B *die zugehörige Strukturmatrix. Seien* $v_1', \ldots, v_n'$ *und* $w_1', \ldots, w_m'$ *weitere Basen mit Übergangsmatrizen* $S \in \mathrm{Gl}_n(K)$ *und* $T \in \mathrm{Gl}_m(K)$. *Sei* B' *die Srukturmatrix bezüglich der neuen Basen. Dann gilt:*

$$B' = S^t B T.$$

Von besonderer Bedeutung ist der Spezialfall $V = W, \dim(V) = n < \infty$. Hier gilt $B' = S^t B S$, wobei $v_1, \ldots, v_n$ und $v_1', \ldots, v_n'$ Basen von V sind mit Übergangsmatrix S.

Definition 1.2.8 a) Sei $\beta : V \times W \longrightarrow K$ eine Bilinearform. Dann heißt

$$\beta^t : W \times V \longrightarrow K, \quad \beta^t(w, v) = \beta(v, w)$$

die zu β transponierte Bilinearform.
b) Eine Bilinearform $\beta : V \times V \longrightarrow K$ heißt symmetrisch, falls $\beta^t = \beta$.

Bemerkung 1.2.9 a) Falls β bezüglich gewählter Basen die Strukturmatrix B hat, so hat β^t bezüglich dieser Basen die Strukturmatrix B^t.
b) $\beta : V \times V \longrightarrow K$ ist genau dann symmetrisch, wenn die Strukturmatrix B symmetrisch ist.

Lemma 1.2.10 *Sei* $\dim(V) = \dim(W) = n < \infty$ *und* $\beta \colon V \times W \longrightarrow K$ *eine nicht ausgeartete Bilineareform. Dann ist*

$$W \longrightarrow V^*, \quad w \mapsto \beta(\_\,, w)$$

ein Isomorphismus.

Satz 1.2.11 *Sei* $\beta : V \times W \longrightarrow K$ *eine nicht ausgeartete Bilinearform und* $\dim(V) = \dim(W) < \infty$. *Sei* $h : V \longrightarrow V$ *ein Endomorphismus. Dann gibt es genau einen Endomorphismus* $\hat{h} : W \longrightarrow W$, *so daß*

$$\beta(h(v), w) = \beta(v, \hat{h}(w)), \forall v \in V, w \in W.$$

Definition 1.2.12 $\hat{h}$ heißt der bezüglich β zu h rechtsadjungierte Endomorphismus. Für $g : W \longrightarrow W$ definiert man in analoger Weise den linksadjungierten Endomorphismus $\hat{g} : V \longrightarrow V$. Es gilt dann: $\beta(\hat{g}(v), w) = \beta(v, g(w)), \forall v \in V, w \in W$.

Definition 1.2.13 Sei $\beta : V \times V \longrightarrow K$ bilinear und $s : V \longrightarrow V$ linear. Dann nennt man s eine Isometrie, falls

$$\beta(s(v), s(w)) = \beta(v, w), \forall v, w \in V.$$

Unter Isometrien sollte man sich längen- und winkeltreue Abbildungen vorstellen.

Satz 1.2.14 *Sei* V *ein endlich dimensionealer Vektorraum,* $\beta : V \times V \longrightarrow K$ *eine nicht ausgeartete Bilinearform und* $s : V \longrightarrow V$ *linear. Dann sind folgende Aussagen äquivalent:*
(i) s *ist eine Isometrie.*
(ii) $(\hat{s})s = id_V$.
(iii) $s^{-1} = \hat{s}$.
(iv) Sei $v_1, \ldots, v_n$ *eine Basis von* V, B *die zugehörige Strukturmatrix und* S *die Koordinatenmatrix von* s *(bezüglich* $v_1, \ldots, v_n$*). Dann gilt:* $B = S^t B S$.
Falls diese äquivalenten Bedingungen erfüllt sind, so gilt außerdem: $\hat{s} = \hat{s} = s^{-1}$.

Definition 1.2.15 a) Sei $\beta : V \times V \longrightarrow K$ eine symmetrische Bilinearform. Ein Vektor $v \in V$ heißt orthogonal zu $w \in V$, falls $\beta(v, w) = 0$.
b) Sei $X \subseteq V$. Dann heißt

$$X^{\perp} = \{v \in V \mid \beta(v, x) = 0, \forall x \in X\}$$

das orthogonale Komplement von X bezüglich β.

Einfache Beobachtungen:
a) $X^{\perp} = Lin(X)^{\perp}$.
b) $X^{\perp}$ ist ein linearer Unterraum von V.

Satz 1.2.16 *Sei $\beta : V \times V \longrightarrow K$ eine nicht ausgeartete symmetrische Bilinearform auf dem endlich dimensionalen Vektorraum V. Sei $X \subseteq V$ ein linearer Unterraum. Dann gilt:*

$$\dim(V) = \dim(X) + \dim(X^{\perp}).$$

Außerdem gilt: $\left(X^{\perp}\right)^{\perp} = X$.
Falls zusätzlich $\beta(v, v) \neq 0$ für alle $0 \neq v \in V$ gilt, so gilt auch: $X \oplus X^{\perp} = V$.

Definition 1.2.17 Eine Bilinearform $\beta : V \times V \longrightarrow K$ heißt schiefsymmetrisch, falls für alle $v, w \in V$ gilt: $\beta(v, w) = -\beta(w, v)$.

Lemma 1.2.18 *Sei $char(K) \neq 2$. Dann gilt:*

$$\beta \text{ ist schiefsymmetrisch } \iff \beta(x, x) = 0, \forall x \in V.$$

Lemma 1.2.19 *Sei $char(K) \neq 2$ und $\dim(V) < \infty$. Falls $\beta : V \times V \longrightarrow K$ eine nicht ausgeartete schiefsymmetrische Bilinearform auf V ist, so ist $\dim(V)$ gerade.*

Satz 1.2.20 *Sei $char(K) \neq 2$ und $\dim(V) < \infty$. Falls $\beta : V \times V \longrightarrow K$ eine nicht ausgeartete schiefsymmetrische Bilinearform auf V ist, so gibt es eine sogenannte symplektische Basis*

$$u_1, v_1, u_2, v_2, \ldots, u_m, v_m,$$

so daß die zugehörige Strukturmatrix B die Gestalt

$$\begin{pmatrix} 0 & 1 & & & & & & \\ -1 & 0 & & & & & & \\ & & 0 & 1 & & & & \\ & & -1 & 0 & & & & \\ & & & & \ddots & & & \\ & & & & & & 0 & 1 \\ & & & & & & -1 & 0 \end{pmatrix}$$

hat. Ferner gilt: Falls B eine beliebige schiefsymmetrische Matrix ist (d.h. $B^t = -B$), so ist $\det(B)$ ein Quadrat in K.

Dieser Satz löst das folgende Klassifikationsproblem. Es sei

$$\mathrm{Symp}_n(K) = \{B \in M_n(K) \mid B^t = -B\}$$

die Menge der schiefsymmetrsichen $n \times n$-Matrizen. Auf $\mathrm{Symp}_n(K)$ definieren wir die Äquivalenzrelation

$$B_1 \sim B_2 : \iff \exists T \in \mathrm{Gl}_n(K) : B_1 = T^t B_2 T.$$

Diese Äquivalenzrelation hat die folgende Interpretation: bezüglich geeigneter Basen des K^n definieren B_1 und B_2 dieselbe schiefsymmetrische Bilinearform.

Folgerung 1.2.21 *In jeder Äquivalenzklasse gibt es genau eine Matrix der Form*

$$\begin{pmatrix} 0 & & & & & \\ & \ddots & & & & \\ & & 0 & & & \\ & & & H & & \\ & & & & \ddots & \\ & & & & & H \end{pmatrix}$$

mit m Kästchen der Form $H = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ und r Nullen auf der Diagonalen. Es gilt also $n = r + 2m$.

Bemerkung 1.2.22 Schiefsymmetrische Matrizen sind also bis auf die Äquivalenz $\sim$ durch ihren Rang bestimmt.

2 Wiederholung: Faktorräume

Sei V ein Vektorraum und $U \subseteq V$ ein linearer Unterraum. Für $v_1, v_2 \in V$ definieren wir

$$v_1 \equiv v_2 (\mathrm{mod}\ U) : \iff v_1 - v_2 \in U.$$

Man zeigt leicht, dass $\equiv$ eine Äquivalenzrelation auf V ist. Es sei V/U die Menge der Äquivalenzklassen. Es gilt dann:

$$V/U = \{v + U \mid v \in V\}.$$

Häufig schreibt man auch $\bar{v} := v + U$ für die Äquivalenzklasse von v. Es gilt:

$$v_1 \equiv v_2 (\mathrm{mod}\ U) \iff v_1 - v_2 \in U \iff v_1 + U = v_2 + U \iff \bar{v}_1 = \bar{v}_2.$$

Wir wollen nun V/U auf kanonische Weise mit einer Vektorraumstruktur versehen.

Satz 2.0.1 *Durch*

$$\begin{aligned} \bar{v} + \bar{w} &:= \overline{v + w}, \quad v, w \in V, \\ \alpha \bar{v} &:= \overline{\alpha v}, \quad v \in V, \alpha \in K, \end{aligned}$$

wird auf V/U eine Vektorraumstruktur definiert.

Im wesentlichen ist dazu zu zeigen, dass die im Satz definierte Addition und skalare Multiplikation wohldefiniert ist.

Satz 2.0.2 *Seien $U \subseteq W \subseteq V$ Vektorräume. Es sei $\{v_j + W \mid j \in J\}$ eine Basis von V/W und $\{w_i + U \mid i \in I\}$ eine Basis von W/U. Dann ist $\{v_j + U, w_i + U \mid i \in I, j \in J\}$ eine Basis von V/U.*

Folgerung 2.0.3 *a) Falls* $\dim(V/U) < \infty$, *so gilt* $\dim(V/U) = \dim(V/W) + \dim(W/U)$.
b) Falls $\dim(V) < \infty$, *so gilt* $\dim(V/W) = \dim(V) - \dim(W)$.

Satz 2.0.4 *(Homomorphiesatz) Sei $f \colon V \longrightarrow W$ eine lineare Abbildung und $U \subseteq \ker(f)$ ein linearer Unterraum. Dann induziert f eine Abbildung*

$$\bar{f} \colon V/U \longrightarrow W, \quad v + U \mapsto f(v),$$

Es gilt:

$$\bar{f} \text{ ist injektiv} \iff U = \ker(f).$$

Bezeichnen wir mit $\pi : V \longrightarrow V/U$ die kanonische Abbildung $v \mapsto v + U$, so besagt dieser Satz, dass es eine lineare Abbildung $\bar{f}\colon V/U \longrightarrow W$ gibt, so dass $f = \bar{f} \circ \pi$ gilt. Da π surjektiv ist, gibt es genau eine solche Abbildung $\bar{f}$.

Satz 2.0.5 *Sei $\beta\colon V \times W \longrightarrow K$ eine Bilinearform. Sei*

$$U := \{v \in V \mid \beta(v, w) = 0, \forall w \in W\}.$$

Dann ist U ein linearer Unterraum von V und für alle Unterräume $U_1 \subseteq U$ wird durch

$$\bar{\beta}\colon V/U_1 \times W \longrightarrow K, \quad (v + U_1, w) \mapsto \beta(v, w)$$

eine Bilinearform definiert. Es gilt:

$$\bar{\beta} \text{ ist nicht ausgeartet im 1.Argument } \iff U_1 = U.$$

Natürlich kann man analoge Aussagen für das zweite Argument formulieren.

3 Euklidische Vektorräume

3.1 Skalarprodukte

Definition 3.1.1 Sei V ein $\mathbb{R}$-Vektorraum. Eine symmetrische Bilinearform

$$\beta : V \times V \longrightarrow \mathbb{R}$$

heißt positv definit, falls $\beta(x, x) > 0, \forall x \in V \setminus \{0\}$.

Unser Standardbeispiel ist $V = \mathbb{R}^n$ und $\beta = \langle , \rangle : V \times V \longrightarrow \mathbb{R}, \langle x, y\rangle = \sum_{i=1}^{n} x_i y_i$.

Definition 3.1.2 Sei V ein $\mathbb{R}$-Vektorraum. Ein Skalarprodukt auf V ist eine symmetrische, positiv definite Bilinearform $\beta = \langle , \rangle : V \times V \longrightarrow \mathbb{R}$.

Definition 3.1.3 Unter einem euklidischen Vektorraum versteht man ein Paar $(V, \langle , \rangle)$, wobei V ein $\mathbb{R}$-Vektorraum und $\langle , \rangle$ ein Skalarprodukt auf V ist.

Definition 3.1.4 Sei $(V, \langle , \rangle)$ ein euklidischer Vektorraum und $x \in V$. Dann heißt $||x|| := \sqrt{\langle x, x\rangle} \in \mathbb{R}_{\geq 0}$ die Norm von x.

Unter $||x||$ hat man sich die Länge des Vektors x vorzustellen.

Satz 3.1.5 *(Cauchy-Schwarzsche Ungleichung) Sei $(V, \langle , \rangle)$ ein euklidischer Vektorraum. Dann gilt:*

$$|\langle x, y\rangle| \leq ||x|| \cdot ||y||, \forall x, y \in V.$$

Satz 3.1.6 *Sei V ein euklidischer Vektorraum. Dann hat die Norm die folgenden Eigenschaften:*

$$\begin{aligned}
&(i) && ||x|| \geq 0, \forall x \in V, \\
&(ii) && ||x|| = 0 \iff x = 0, \\
&(iii) && ||\lambda x|| = |\lambda| ||x||, \forall x \in V, \lambda \in \mathbb{R}, \\
&(iv) && ||x + y|| \leq ||x|| + ||y||, \forall x, y \in V.
\end{aligned}$$

Einen $\mathbb{R}$-Vektorraum zusammen mit einer Abbildung $||||: V \longrightarrow \mathbb{R}$ mit den Eigenschaften (i) - (iv) nennt man normierten Raum. Jeder euklidische Raum ist also ein normierter Raum.
In einem euklidischen Raum kann man auch einen Abstandsbegriff definieren. Es sei

$$d: V \times V \longrightarrow \mathbb{R}, \quad d(x,y) = ||x-y||.$$

Die Eigenschaften (i) - (iv) übersetzen sich zu

$$\begin{aligned}
(i) \quad & d(x,y) \geq 0, \forall x,y \in V, \\
(ii) \quad & d(x,y) = 0 \iff x = y, \\
(iii) \quad & d(x,y) = d(y,x), \forall x,y \in V, \\
(iv) \quad & d(x,y) \leq d(x,z) + d(z,y), \forall x,y,z \in V.
\end{aligned}$$

Einen $\mathbb{R}$–Vektorraum zusammen mit einer Abbildung $d: V \times V \longrightarrow \mathbb{R}$ mit den Eigenschaften (i) - (iv) nennt man einen metrischen Raum. Jeder normierte Raum ist also ein metrischer Raum. Die Eigenschaft (iv) heißt aus naheliegenden Gründen Dreiecksungleichung.
Nach dem Abstand wollen wir nun den Winkel zwischen zwei Elementen eines euklidischen Raumes definieren.

Definition 3.1.7 Sei V ein euklidischer Vektorraum und $x, y \in V \setminus \{0\}$. Dann heißt die Zahl $\alpha(x,y)$ definiert durch

$$\cos(\alpha(x,y)) = \frac{\langle x,y \rangle}{||x||||y||}, 0 \leq \alpha(x,y) \leq \pi,$$

der Winkel zwischen x und y.

Man beachte, daß der Winkel nicht von der Länge der Vektoren x und y abhängt.

Definition 3.1.8 Vektoren $v_1, \ldots, v_r$ eines euklidischen Vektorraums V bilden ein Orthonormalsystem, falls

$$\begin{aligned}
&||v_i|| = 1, \quad i = 1, \ldots, r, \\
&\langle v_i, v_j \rangle = 0, \quad i = 1, \ldots, r, i \neq j.
\end{aligned}$$

Lemma 3.1.9 *Ein Orthonormalsystem ist stets linear unabhängig.*

Satz 3.1.10 *Jeder endlich dimensionale euklidische Vektorraum bestizt eine Orthonormalbasis.*

Der Beweis liefert auch gleich ein Konstruktionsverfahren zur Berechnung einer solchen Orthonormalbasis (Schmidtsches Orthogonalisierungsverfahren).

Satz 3.1.11 *Sei V ein endlich dimensionaler euklidischer Raum und $U \subseteq V$ ein Unterraum. Dann gilt:*

$$V = U \oplus U^{\perp}.$$

Hieraus folgt sofort

Folgerung 3.1.12 *Sei V ein endlich dimensionaler euklidischer Raum und $U \subseteq V$ ein Unterraum. Dann gilt:*

$$U^{\perp} = \{0\} \iff U = V.$$

Definition 3.1.13 Seien V, W euklidische Vektorräume. Eine lineare Abbildung $f: V \longrightarrow W$ heißt orthogonal, falls

$$\langle v_1, v_2 \rangle_V = \langle f(v_1), f(v_2) \rangle_W, \forall v_1, v_2 \in V.$$

Im Fall $V = W$ sind die orthogonalen Abbildungen also genau die Isometrien. Orthogonale Abbildungen sind stets injektiv. Falls $V = W$ und $\dim(V) < \infty$, so sind sie also bijektiv.

Definition 3.1.14 a) Sei V ein euklidischer Vektorraum. Dann nennt man die Gruppe $O(V)$ der orthogonalen Isomorphismen $f : V \longrightarrow V$ die orthogonale Gruppe von V.
b) Sei $V = \mathbb{R}^n$ versehen mit dem Standardskalarprodukt. Dann schreibt man $O(n) = O(\mathbb{R}^n)$ und faßt $O(n)$ als Teilmenge von $M_n(\mathbb{R})$ auf. Matrizen in $O(n)$ nennt man orthogonale Matrizen.

Im folgenden Satz werden nur unsere Resultate über Isometrien eines endlich dimensionalen euklidischen Raumes auf den Spezialfall $V = \mathbb{R}^n$ übertragen.

Satz 3.1.15 *Für $A \in M_n(\mathbb{R})$ sind die folgenden Aussagen äquivalent:*
a) $A \in O(n)$.
b) $A^tA = E$.
c) $AA^t = E$.
d) $A \in \mathrm{Gl}_n(\mathbb{R})$ und $A^{-1} = A^t$.
e) Die Spalten von A bilden eine Orthonormalbasis des $\mathbb{R}^n$.
d) Die Zeilen von A bilden eine Orthonormalbasis des $\mathbb{R}^n$.

Satz 3.1.16 *Sei V ein reeller Vektorraum der Dimension $n < \infty$. Sei $\beta : V \times V \longrightarrow \mathbb{R}$ eine symmetrische Bilinearform. Sei $v_1, \ldots, v_n$ eine Basis von V und $B \in \mathrm{Gl}_n(\mathbb{R})$ die Strukturmatrix. Dann sind folgende Aussagen äquivalent:*

(i) β ist positiv definit.
(ii) $\exists W \in \mathrm{Gl}_n(\mathbb{R}) : B = W^tW$.
(iii) $\det(B_k) > 0, k = 1, \ldots, n$.

Hierbei ist $B = (b_{ij})$ und

$$B_k = \begin{pmatrix} b_{11} & \ldots & b_{1k} \\ \vdots & & \vdots \\ b_{k1} & \ldots & b_{kk} \end{pmatrix}.$$

3.2 Die Hauptachsentransformation

Im Folgenden schreiben wir

$$\mathrm{Sym}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid A^t = A\}$$

für die Menge der symmetrischen Matrizen. $\mathrm{Sym}_n(\mathbb{R})$ ist ein Vektorraum der Dimension $n(n+1)/2$.

Definition 3.2.1 a) $S \in \mathrm{Sym}_n(\mathbb{R})$ heißt positiv definit, falls $x^tSx > 0, \forall x \in \mathbb{R}^n \setminus \{0\}$.
b) $S \in \mathrm{Sym}_n(\mathbb{R})$ heißt positiv semi-definit, falls $x^tSx \geq 0, \forall x \in \mathbb{R}^n$.

Proposition 3.2.2 *Für $S \in \mathrm{Sym}_n(\mathbb{R})$ sind folgende Aussagen äquivalent:*
a) S ist positiv semi-definit.
b) $\exists W \in M_n(\mathbb{R}) : S = W^tW$.

Folgerung 3.2.3 *Sei $S \in \mathrm{Sym}_n(\mathbb{R})$ positiv semi-definit. Dann gilt:*

$$a^tSa = 0 \iff Sa = 0.$$

Wir versehen nun den $\mathbb{R}^n$ stets mit dem Standardskalarprodukt. Für $S \in \mathrm{Sym}_n(\mathbb{R})$ definieren wir

$$\mu(S) := \inf\{x^tSx \mid x \in \mathbb{R}^n, ||x|| = 1\}.$$

Satz 3.2.4 *Für jede Matrix $S \in \mathrm{Sym}_n(\mathbb{R})$ ist $\mu(S)$ endlich und wird angenommen, d.h. es gibt $u \in \mathbb{R}^n, ||u|| = 1$, mit $u^t S u = \mu(S)$.*

Folgerung 3.2.5 *Für $S \in \mathrm{Sym}_n(\mathbb{R})$ gilt:*

$$x^t S x \geq \mu(S) \cdot ||x||, \forall x \in \mathbb{R}^n.$$

Folgerung 3.2.6 *Sei $S \in \mathrm{Sym}_n(\mathbb{R})$. Dann ist $\mu(S)$ ein Eigenwert zu S.*

Das zweite Korollar ist die wesentliche Beweiszutat für den folgenden

Satz 3.2.7 *(Hauptachsentransformation) Zu $S \in \mathrm{Sym}_n(\mathbb{R})$ gibt es $T \in O(n)$, so daß*

$$T^t S T = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}.$$

Hierbei sind $\lambda_1, \ldots, \lambda_n$ die Eigenwerte von S (mit Vielfachheiten). Die Spalten von T sind eine aus Eigenvektoren zu S bestehende Orthonormalbasis des $\mathbb{R}^n$.

3.3 Anwendungen

Bemerkung 3.3.1 $\mu(S)$ ist der kleinste Eigenwert von $S \in \mathrm{Sym}_n(\mathbb{R})$. Daher liefert die Analysis Methoden zur Berechnung von Eigenwerten symmetrischer Matrizen.

Satz 3.3.2 *Für $S \in \mathrm{Sym}_n(\mathbb{R})$ sind die folgenden Aussagen äquivalent:*
a) S ist positiv definit.
b) S erfüllt das Determinantenkriterium aus Satz (3.1.16).
c) $\exists W \in \mathrm{Gl}_n(\mathbb{R}) : S = W^t W$.
d) Alle Eigenwerte von S sind positiv.
e) $S \in \mathrm{Gl}_n(\mathbb{R})$ und S^{-1} ist positiv definit.
f) S ist positiv semi-definit und $\det(S) \neq 0$.

Eine weitere Anwendung des Satzes über die Hauptachsentransformation ist die Diskussion von Hyperflächen zweiten Grades. Wir betrachten Polynome zweiten Grades in Variablen $x_1, \ldots, x_n$. Jedes solche Polynom kann man in der allgemeinen Form

$$\sum_{i,j}^{n} \alpha_{ij} x_i x_j + 2 \sum_{k=1}^{n} \alpha_k x_k + \alpha \quad (*)$$

mit $\alpha_{ij} = \alpha_{ji}, \alpha_k, \alpha \in \mathbb{R}$ schreiben..
Sei $S = (\alpha_{ij}) \in \mathrm{Sym}_n(\mathbb{R}), a = (\alpha_1, \ldots, \alpha_n)^t \in \mathbb{R}^n$. Dann kann man $(*)$ auch in der Form

$$\kappa_{S,a,\alpha}(x) := x^t S x + 2 a^t x + \alpha$$

mit $x = (x_1, \ldots, x_n)^t$ schreiben.

Definition 3.3.3 Sei

$$\Phi_{S,a,\alpha} := \{y \in \mathbb{R}^n \mid \kappa_{S,a,\alpha}(y) = 0\}$$

die Nullstellenmenge der Funktion $\kappa_{S,a,\alpha} : \mathbb{R}^n \longrightarrow \mathbb{R}$. Falls $\Phi_{S,a,\alpha} \neq \emptyset$, so nennt man $\Phi_{S,a,\alpha}$ eine Hyperfläche zweiten Grades oder Quadrik.

Satz 3.3.4 *(Normalformensatz für Polynome zweiten Grades) Von einem allgemeinen Polynom zweiten Grades in der Form* $(*)$ *darf man*
a) nach einer Translation $x \mapsto x + c, c \in \mathbb{R}^n$*, annnehmen, daß*

$$Sa = 0 = \alpha a$$

gilt.
b) nach einer affin linearen Abbildung $x \mapsto Tx + b$*,* $T \in O(n), b \in \mathbb{R}^n$*, eine der folgenden Normalformen annehmen*

$$\begin{aligned} I) \quad & \lambda_1 x_1^2 + \ldots + \lambda_n x_n^2 + \beta, \beta \in \mathbb{R}, \\ & \textit{oder} \\ II) \quad & \lambda_1 x_1^2 + \ldots + \lambda_{n-1} x_{n-1}^2 + 2\gamma x_n, \gamma \in \mathbb{R}, \gamma > 0. \end{aligned}$$

Im Fall I) sind $\lambda_1, \ldots, \lambda_n$ *die Eigenwerte von* S*. Im Fall II) sind die Eigenwerte durch* $\lambda_1, \ldots, \lambda_{n-1}, 0$ *gegeben.*

Der Beweis hierzu ist konstruktiv und liefert einen Algorithmus zur Berechnung dieser Normalformen. Da $T \in O(n)$, ist die affin lineare Abbildung $x \mapsto Tx + b$ längen- und winkelerhaltend, d.h. das Nullstellengebilde $\Phi_{S,a,\alpha}$ "behält seine ursprügliche Gestalt".

Folgerung 3.3.5 *Im Fall* $n = 2$ *erhält man als Normalform der Kurven 2.ten Grades:*
(i) $(\alpha_1 x_1)^2 + (\alpha_2 x_2)^2 = 1$ *oder* 0 *mit* $\alpha_1 \alpha_2 \neq 0$*. Hier handelt es sich um eine Ellipse oder einen Punkt.*
(ii) $(\alpha_1 x_1)^2 - (\alpha_2 x_2)^2 = 1$ *oder* 0 *mit* $\alpha_1 \alpha_2 \neq 0$*. Hier handelt es sich um eine Hyperbel oder zwei sich schneidende Geraden.*
(iii) $x_1^2 + \omega x_2 = 0$ *mit* $\omega \neq 0$*. Dies ist eine Parabel.*
(iv) $x_1^2 = \omega$ *mit* $\omega > 0$ *oder* $\omega = 0$*. Hier handelt es sich um ein Geradenpaar oder eine Doppelgerade.*

Das letzte Korollar muss noch diskutiert werden.

4 Unitäre Vektorräume

4.1 Grundlegendes

Definition 4.1.1 Sei V ein $\mathbb{C}$-Vektorraum.
a) Eine Abbildung $\beta \colon V \times V \longrightarrow \mathbb{C}$ heißt Sequilinearform, falls

- β linear im ersten Argument ist.
- β semi-linear im zweiten Argument ist, d.h.

$$\beta(x, y + z) = \beta(x, y) + \beta(x, z), \quad \beta(x, cy) = \bar{c}\beta(x, y), \quad \forall x, y, z \in V, c \in \mathbb{C}.$$

b) Eine Sesquilienarform h heißt hermitesch, falls $h(x, y) = \overline{h(y, x)}$ gilt für alle $x, y \in V$. Insbesondere gilt dann $h(x, x) \in \mathbb{R}$ für allle $x \in V$.
c) Eine hermitesche Form h heißt positiv definit, falls $h(x, x) > 0$ für alle $v \in V \setminus \{0\}$.

Bemerkungen 4.1.2 1) Sei V ein $\mathbb{C}$-Vektorraum. Dann bezeichnen wir mit $\bar{V}$ den folgenden Vektorraum: $\bar{V} = V$ als additive Gruppe versehen mit der neuen skalaren Multiplikation $c \cdot v := \bar{c}v$. Dann entsprechen die Sesquilinearformen $\beta : V \times V \longrightarrow \mathbb{C}$ genau den Bilinearformen $\beta : V \times \bar{V} \longrightarrow \mathbb{C}$. Wir können daher viele unserer Resultate aus der allgemeinen Theorie bilinearer Formen auf einfache Weise übertragen.
2) Positiv definite hermitesche Formen nennt man oft auch Skalarprodukt.

Definition 4.1.3 Ein unitärer Vektorraum ist ein Paar (V, h) bestehend aus einem $\mathbb{C}$-Vektorraum V und einer positiv definiten hermiteschen Form h.

Viele Konzepte und Resultate aus der Theorie euklidischer Vektorräume übertragen sich fast wortwörtlich. Wir listen sie nur auf.

- Falls (V, h) ein endlich dimensionaler unitärer Vektorraum ist und $U \subseteq V$ ein linearer Unterraum, so gilt
$$V = U \oplus U^{\perp} \text{ mit } U^{\perp} := \{v \in V \mid h(v, u) = 0, \forall u \in U\}.$$
- Sei $h : V \times V \longrightarrow \mathbb{C}$ hermitesch und positiv semidefinit. Dann gilt die Cauchy-Schwartzsche Ungleichung:
$$|h(x, y)|^2 \leq h(x, x)h(y, y), \quad \forall x, y \in V.$$
- Durch $||x|| := \sqrt{h(x, x)}$ wird eine Norm auf dem unitären Raum (V, h) definiert.
- Das Schmidtsche Orthogonalisierungsverfahren liefert die Existenz von Orthonormalbasen in endlich dimensionalen unitären Vektorräumen.
- Falls $\beta \colon V \times V \longrightarrow \mathbb{C}$ eine Sesquilinearform auf dem endlich dimensionalen $\mathbb{C}$-Vektorraum V ist und $v_1, \ldots, v_n$ eine Basis von V, so nennt man $B := (\beta(v_i, v_j))$ die Strukturmatrix von β bezüglich der Basis $v_1, \ldots, v_n$.
Falls $x = \sum_{i=1}^{n} x_i v_i$ und $y = \sum_{i=1}^{n} y_i v_i$, so gilt $\beta(x, y) = x^t B \bar{y}$.
- Falls $w_1, \ldots, w_n$ eine weitere Basis von V ist mit Übergangsmatrix S, so ist die Strukturmatrix B' bezüglich $w_1, \ldots, w_n$ gegeben durch $B' = S^t B \bar{S}$.
- Sei $B \in M_n(\mathbb{C})$. Dann ist durch $(x, y) \mapsto x^t B \bar{y}$ eine Sesquilinearform $\mathbb{C}^n \times \mathbb{C}^n \longrightarrow \mathbb{C}$ gegeben. Diese hat bezüglich der Standardbasis $e_1, \ldots, e_n$ offensichtlich die Strukturmatrix B.
- Eine Sesquilinearform β ist genau dann hermitesch, wenn $B^* = B$, wobei $B^* := \bar{B}^t$. Man beachte, daß diese Aussage basisunabhängig ist.
- Eine hermitesche Matrix $A \in M_n(\mathbb{C})$ ist genau dann positiv definit, wenn es eine Matrix $W \in \mathrm{Gl}_n(\mathbb{C})$ gibt, so daß $A = W^* W$. Dazu beachte man die folgende Definition.

Definition 4.1.4 $A \in M_n(\mathbb{C})$ heißt hermitesch, wenn die zugeordnete Sesquilinearform hermitesch ist. Dies ist genau dann der Fall, wenn $A^* = A$ gilt.

Man beachte, daß eine quadratische Matrix über den komplexen Zahlen stets Eigenwerte hat. Dies ist eine Konsequenz des Fundamentalsatzes der Algebra, welcher besagt, daß $\mathbb{C}$ algebraisch abgeschlossen ist.

Satz 4.1.5 *Die Eigenwerte einer hermiteschen Matrix $A \in M_n(\mathbb{C})$ sind reell.*

Dies liefert uns einen neuen Beweis dafür, dass reelle symmetrische Matrizen stets einen Eigenwert haben. Dies hatten wir mit Methoden der Analysis bewiesen. Diese werden hier ersetzt durch die Tatsache, daß $\mathbb{C}$ algebraisch abgeschlossen ist. Für den Beweis hierzu verweisen wir auf die Algebra oder Funktionentheorie.

4.2 Die unitäre Gruppe

Definition 4.2.1 a) Sei $(V, \langle , \rangle)$ ein unitärer Vektorraum. Dann heißt

$$U(V) := \{f \in \mathrm{End}(V) \mid f \text{ ist ein Isomorphismus und eine Isometrie } \}$$

die unitäre Gruppe zu V.
b) Wir setzen $U(n) = U(n, \mathbb{C}) := U(\mathbb{C}^n)$, wobei wir $\mathbb{C}^n$ mit dem Standardskalarprodukt ($\langle x, y\rangle = \sum_i x_i \bar{y}_i$) versehen.

Satz 4.2.2 *Für $A \in M_n(\mathbb{C})$ sind die folgenden Aussagen äquivalent:*
a) $A \in U(n)$.
b) $A^*A = E$.
c) $A^t\bar{A} = E$.
d) $AA^* = E$.
e) $A \in \mathrm{Gl}_n(\mathbb{C})$ und $A^{-1} = A^*$.
f) Die Spalten von A bilden eine Orthonormalbasis des $\mathbb{C}^n$.
g) Die Zeilen von A bilden eine Orthonormalbasis des $\mathbb{C}^n$.

Sei nun $(V, \langle , \rangle)$ ein n-dimensionaler unitärer Vektorraum. Dann gibt es zu jeder linearen Abbildung $f \in \mathrm{End}(V)$ genau ein $f^* \in \mathrm{End}(V)$, so daß $\langle x, f(y)\rangle = \langle f^*(x), y\rangle$ für alle $x, y \in V$ gilt. Es gilt dann auch $\langle f(x), y\rangle = \langle x, f^*(y)\rangle$ für alle $x, y \in V$. Ist $v_1, \ldots, v_n$ eine Ortonormalbasis von V und A die Koordinatenmatrix von f bez. dieser Basis, so ist A^* die Koordinatenmatrix von f^* bez. $v_1, \ldots, v_n$.

4.3 Der Spektralsatz

Definition 4.3.1 Sei $(V, \langle , \rangle)$ ein unitärer Vektorraum und $f \in \mathrm{End}(V)$. Dann nennt man f normal, falls $ff^* = f^*f$ gilt.

Satz 4.3.2 *(Spektralsatz)*
a)Sei $(V, \langle , \rangle)$ ein endlich dimensionaler unitärer Vektorraum und $f \in \mathrm{End}(V)$ normal. Dann gibt es eine Orthonormalbasis von V, die aus Eigenvektoren von f besteht.
b) Ist $A \in M_n(\mathbb{C})$ normal (d.h. $A^*A = AA^*$), so gibt es eine unitäre Matrix $U \in U(n)$, so daß

$$U^*AU = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}.$$

Hierbei sind $\lambda_1, \ldots, \lambda_n$ die Eigenwerte von A (mit Vielfachheiten). Die Spalten von U sind eine aus Eigenvektoren zu A bestehende Orthonormalbasis des $\mathbb{C}^n$.

Zum Beweis haben wir folgendes Lemma benutzt.

Lemma 4.3.3 *Sei $(V, \langle , \rangle)$ ein unitärer Vekrotraum und $f \in \mathrm{End}(V)$.*
a) Folgende Aussagen sind äquivalent:
i) f ist normal.
ii) $\langle f^*x, f^*y\rangle = \langle fx, fy\rangle, \forall x, y \in V$.
iii) $||f^*x|| = ||fx||, \forall x \in V$.
b) Sei $U \subseteq V$ ein Unterraum. Falls $f(U) \subseteq U$, so gilt $f^*(U^\perp) \subseteq U^\perp$.
c) Falls f normal ist und $v \in V$ ein Eigenvektor zum Eigenwert $\lambda \in \mathbb{C}$ ist, so ist v Eigenvektor zu f^* zum Eigenwert $\bar{\lambda}$.

4.4 Hyperebenen und Abstände

Definition 4.4.1 Sei V ein Vektorraum, $p \in V$ und $U \subseteq V$ ein Unterraum. Dann nennt man

$$M = p + U = \{p + u \mid u \in U\}$$

einen affinen Unterraum von V. Die Dimension von M ist definiert durch $\dim(M) = \dim(U)$.

Bemerkung 4.4.2 Der Unterraum U ist durch M eindeutig bestimmt. Für den sogenannten Differenzenraum

$$\Delta M = \{x_1 - x_2 \mid x_1, x_2 \in M\}$$

gilt $U = \Delta M$.

Definition 4.4.3 Sei $\dim(V) = n < \infty$. Dann nennt man einen affinen Unterraum der Dimension $n - 1$ eine Hyperebene.

Im folgenden sei $\mathbb{K}$ entweder $\mathbb{R}$ oder $\mathbb{C}$. Im Falle $\mathbb{K} = \mathbb{R}$ verstehen wir unter einem unitären Vektorraum einen euklidischen Vektorraum, eine hermitesche Form ist eine symmetrische Form, etc.

Satz 4.4.4 *Sei $(V, \langle , \rangle)$ ein unitärer Vektorraum und $H \subseteq V$ eine Teilmenge. Dann sind die folgenden Aussagen äquivalent:*
(i) H ist eine Hyperebene.
(ii) $\exists p \in V, 0 \neq f \in V^* = \mathrm{Hom}(V, \mathbb{K})$ mit $H = p + \ker(f)$.
(iii) $\exists c \in V, ||c|| = 1, \alpha \in \mathbb{C}$ mit $H = H_{c,\alpha} := \{x \in V \mid \langle x, c\rangle = \alpha\}$.
Es gilt dann: $H = p + \ker(f) = p + (\mathbb{K}c)^{\perp}$.

Definition 4.4.5 Die Darstellung $H_{c,\alpha}$ in (iii) heißt Hessesche Normalform der Hyperebene H.

Im weiteren sei V stets ein unitärer $\mathbb{K}$-Vektorraum mit Skalarprodukt $\langle , \rangle$.

Definition 4.4.6 Zwei affine Unterräume M und N heißen parallel, falls

$$\Delta M \subseteq \Delta N \text{ oder } \Delta N \subseteq \Delta M.$$

Satz 4.4.7 *Sei $\dim(V) \geq 2$. Sei $M \subseteq V$ ein affiner Unterraum der Dimension m und $H \subseteq V$ eine Hyperebene.Dann sind folgende Aussagen äquivalent:*
i) M und H sind nicht parallel.
ii) M und H schneiden sich in einem affinen Unterraum der Dimension $m - 1$.

Im folgenden schreiben wir $G_{p,a}$ für die Gerade mit Fußpunkt p und Richtungsvektor a. Explizit:

$$G_{p,a} = p + \mathbb{R}a = \{p + \lambda a \mid \lambda \in \mathbb{R}\}.$$

Folgerung 4.4.8 *Sei $\dim(V) \geq 2$. Falls die Gerade $G_{p,a}$ und die Hyperebene $H_{c,\alpha}$ nicht parallel sind, so schneiden sie sich in genau einem Punkt. Der Schnittpunkt ist von der Form*

$$p + \frac{\alpha - \langle p, c\rangle}{\langle a, c\rangle} a.$$

Definition 4.4.9 Seien M und N zwei affine Unterräume von V. Dann heißen M und N orthogonal, falls $\Delta M \perp \Delta N$.

Definition 4.4.10 Sei $U \subseteq V$ ein Unterraum. Dann heißt die lineare Abbildung

$$\begin{aligned} \pi_U : V &\longrightarrow U, \\ v &\mapsto v_1, \text{ falls } v = v_1 + v_2 \text{ mit } v_1 \in U, v_2 \in U^\perp \end{aligned}$$

die orthogonale Projektion von V auf U.

Definition 4.4.11 Seien $M_1 = p_1 + U_1$ und $M_2 = p_2 + U_2$ zwei affine Unterräume. Dann definiert man den Abstand zwischen M_1 und M_2 durch

$$d(M_1, M_2) = \inf\{||x_1 - x_2|| \mid x_1 \in M_1, x_2 \in M_2\}.$$

Satz 4.4.12 *Seien $M_1 = p_1 + U_1$ und $M_2 = p_2 + U_2$ zwei affine Unterräume und $p := p_1 - p_2$, $U := U_1 + U_2$. Dann gilt*

$$d(M_1, M_2) = d(p, U)$$

und der Abstand wird angenommen. Es gilt:

$$d(p, U) = \sqrt{||p||^2 - ||\pi_U(p)||^2}.$$

Folgerung 4.4.13 *Für den Abstand des Punktes $p \in V$ von der Hyperebene $H = H_{c,\alpha}$ ergibt sich*

$$d(p, H) = |\langle p, c\rangle - \alpha|.$$

4.5 Das Vektorprodukt

Definition 4.5.1 Für Vektoren $a = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}$ und $b = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}$ des $\mathbb{R}^3$ definiert man

$$a \times b = \begin{pmatrix} a_2 b_3 - a_3 b_2 \\ a_3 b_1 - a_1 b_3 \\ a_1 b_2 - a_2 b_1 \end{pmatrix}.$$

$a \times b$ heißt das Vektorprodukt oder äußere Produkt von a und b.

Für das Vektorprodukt gelten folgende Regeln und Identitäten:

Proposition 4.5.2 *a) Die Abbildung $\mathbb{R}^3 \times \mathbb{R}^3 \longrightarrow \mathbb{R}^3, (a, b) \mapsto a \times b$, ist bilinear, d.h.*

$$\begin{aligned} (\alpha_1 a_1 + \alpha_2 a_2) \times b &= \alpha_1 a_1 \times b + \alpha_2 a_2 \times b, \\ a \times (\beta_1 b_1 + \beta_2 b_2) &= \beta_1 a \times b_1 + \beta_2 a \times b_2. \end{aligned}$$

für alle $a, a_1, a_2, b, b_1, b_2 \in \mathbb{R}^3, \alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{R}$.
b) Das Kreuzprodukt ist schiefsymmetrisch, d.h. $a \times b = -b \times a$. Insbesondere gilt also: $a \times a = 0$ für alle $a \in \mathbb{R}^3$.
c) Das Kreuzprodukt erfüllt die sogenannte Grassmann-Identität:

$$a \times (b \times c) = \langle a, c\rangle b - \langle a, b\rangle c, \forall a, b, c \in \mathbb{R}^3.$$

d) Das Kreuzprodukt erfüllt die sogenannte Jacobi-Identität:

$$a \times (b \times c) + b \times (c \times a) + c \times (a \times b) = 0, \forall a, b, c \in \mathbb{R}^3.$$

e) $\det(a, b, c) = \langle a \times b, c\rangle, \forall a, b, c \in \mathbb{R}^3$.
f) $\langle a \times b, c\rangle = \langle a, b \times c\rangle, \forall a, b, c \in \mathbb{R}^3$.

Im $\mathbb{R}^3$ kann man mittels dem Vektorprodukt eine exakte Version der Cauchy-Schwarzschen Ungleichung formulieren.

Satz 4.5.3 $\langle a,b\rangle^2 + ||a\times b||^2 = ||a||^2||b||^2, \quad \forall a,b\in\mathbb{R}^3.$

Die obigen Identitäten b) und f) implizieren, daß $a\times b$ auf a und b senkrecht steht. Zusammen mit dem vorherigen Satz liefert dies

Satz 4.5.4 *a) Sind $a,b\in\mathbb{R}^3$ orthogonal und normiert, so ist $a,b,a\times b$ eine Orthonormalbasis des $\mathbb{R}^3$.*
b) Ist a,b,c eine Orthonormalbasis des $\mathbb{R}^3$, so ist $c=\pm a\times b$.

Eine häufige Anwendung des Vektorprodukts ist folgendes: Sei $H = q+\mathbb{R}a+\mathbb{R}b$ eine Ebene im $\mathbb{R}^3$. Dann steht $a\times b$ senkrecht auf H.

4.6 Die orthogonale Gruppe $O(n)$

In diesem Abschnitt wollen wir einsehen, daß $O(n)$ durch die Spiegelungen erzeugt wird.

Definition 4.6.1 Sei $0\neq a\in\mathbb{R}^n$ und $H=(\mathbb{R}a)^\perp$. Dann heißt die lineare Abbildung

$$\begin{array}{rcl}\mathbb{R}^n & \longrightarrow & \mathbb{R}^n,\\ v & \mapsto & -v_1+v_2, \text{ falls } v=v_1+v_2, v_1\in\mathbb{R}a, v_2\in H,\end{array}$$

die Spiegelung an der Hyperebenen H.

Man zeigt leicht, daß die Spiegelung an der Hyperebenen $H=(\mathbb{R}a)^\perp$ bezüglich der Standardbasis die Koordinatenmatrix

$$S_a = E - \frac{2}{\langle a,a\rangle}aa^t$$

hat. Wir bezeichnen daher die Spiegelung an $H=(\mathbb{R}a)^\perp$ stets mit S_a. Man beachte jedoch, daß sowohl H als auch S_a von a nur modulo skalarer Multiplikation abhängen.

Lemma 4.6.2 *Seien $u,v\in\mathbb{R}^n$, $u\neq v, ||u||=||v||$. Sei $a=u-v$. Dann gilt $S_au=v$ und $S_av=u$.*

Satz 4.6.3 *Jede Matrix $E\neq T\in O(n)$ ist Produkt von höchstens n Spiegelungen.*

Der Zwischenwertsatz liefert

Satz 4.6.4 *Sei n eine ungerade natürliche Zahl und $T\in O(n)$. Dann besitzt T einen reellen Eigenwert. Die Abbildung T hat also mindestens eine Fixgerade.*

Orthogonale Matrizen haben Determinante ±1. Wir definieren

$$\begin{array}{rcl}O^+(n) & = & \{T\in O(n)\mid \det(T)=+1\},\\ O^-(n) & = & \{T\in O(n)\mid \det(T)=-1\}\end{array}$$

Wir betrachten nun abschließend die $O(3)$.

Proposition 4.6.5 *Es gilt*

$$\begin{array}{rcl}O(3) & = & \{(a,b,\pm a\times b)\mid ||a||=||b||=1,\langle a,b\rangle=0\},\\ O^+(3) & = & \{(a,b,a\times b)\mid ||a||=||b||=1,\langle a,b\rangle=0\},\\ O^-(3) & = & \{(a,b,-a\times b)\mid ||a||=||b||=1,\langle a,b\rangle=0\}.\end{array}$$

Wir wollen nun eine einfache Darstellung der 3-dimensionalen orthogonalen Matrizen herleiten. Wegen $O^-(3) = -O^+(3)$ genügt es $T \in O^+(3)$ zu betrachen.
Es sei

$$T_3(\omega) = \begin{pmatrix} \cos(\omega) & -\sin(\omega) & 0 \\ \sin(\omega) & \cos(\omega) & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad 0 \leq \omega < 2\pi.$$

$T_3(\omega)$ beschreibt also die Drehung um den Winkel ω um die Drehachse $\mathbb{R}e_3$.

Lemma 4.6.6 *$T \in O^+(3)$ hat den Eigenwert 1.*

Satz 4.6.7 *Sei $T \in O^+(3)$ und $q \in \mathbb{R}^3$ ein Eigenvektor zum Eigenwert 1 der Länge $||q|| = 1$. Falls $q = e_3$, so sei $S = E$. Falls $q \neq e_3$, so sei S die Spiegelung mit $Se_3 = q$. Dann gibt es genau einen Drehwinkel $\omega \in \mathbb{R}, 0 \leq \omega < 2\pi$, so daß*

$$T = ST_3(\omega)S.$$

5 Normalformen

5.1 Elementare Teilbarkeitslehre

Im weiteren sei R stets ein kommutativer Ring mit 1. Unsere wichtigsten Beispiele sind der Ring der ganzen Zahlen $\mathbb{Z}$ und der Polynomring $K[x]$ über einem Körper K.

Definition 5.1.1 Zwei Element $a, b \in R$ heißen zueinander assoziiert, falls $a \mid b$ und $b \mid a$. In Zeichen: $a \sim b$.

Lemma 5.1.2 *Falls R nullteilerfrei ist, so gilt:*

$$a \sim b \iff \exists e \in R^\times : b = ea.$$

Für $a \in R$ bezeichnen wir nun mit

$$(a) = aR = \{ra \mid r \in R\}$$

die Menge aller Vielfachen von a. In einem nullteilerfreien Ring gelten folgende Äquivalenzen:

$$\begin{aligned} &1) \quad a \mid b \iff (b) \subseteq (a), \\ &2) \quad a \sim b \iff (a) = (b), \\ &3) \quad (a) = R \iff a \in R^\times. \end{aligned}$$

Definition 5.1.3 Eine Teilmenge $J \subseteq R$ heißt Ideal, falls

$$\begin{aligned} &(i) \quad 0 \in J, \\ &(ii) \quad a, b \in J \implies a + b \in J, \\ &(iii) \quad a \in J, r \in R \implies ra \in J. \end{aligned}$$

Ideale der Form (a) heißen Hauptideale.

Definition 5.1.4 Seien I, J zwei Ideale in R. Dann heißt

$$\begin{aligned} &I + J = \{a + b \mid a \in I, b \in J\} \text{ die Summe ,} \\ &I \cap J \text{ der Durchschnitt und} \\ &IJ = \{ \sum_{i,\text{endl.}} a_i b_i \mid a_i \in I, b_i \in J\} \text{ das Produkt} \end{aligned}$$

der Ideale I und J.

Man beachte, daß Summe, Durchschnitt und Produkt wieder Ideale in R sind.

Definition 5.1.5 Ein nullteilerfreier Ring heißt Hauptidealring, falls jedes Ideal ein Hauptideal ist.

Sei $f\colon R \longrightarrow S$ ein Ringhomomorphismus. Dann ist

$$\ker(f) := \{a \in R \mid f(a) = 0\}$$

ein Ideal in R. Wir erinnern an die Äquivalenzrelation

$$a \equiv b \pmod{I} :\Longleftrightarrow a - b \in I.$$

Es sei $R/I = \{a + I \mid a \in R\}$ die Menge der Äquivalenzklassen. Dann wird R/I vermöge

$$(a + I) + (b + I) := (a + b) + I, \quad (a + I) \cdot (b + I) := (ab) + I$$

zu einem kommutativen Ring

Satz 5.1.6 *Sei $f\colon R \longrightarrow S$ ein Ringhomomorphismus und $J \subseteq R$ ein Ideal mit $J \subseteq \ker(f)$. Sei $\pi\colon R \longrightarrow R/J$ die kanonische Projektion, d.h. $\pi(a) = a + J$. Dann gibt es genau einen Ringhomomorphismus $\bar{f}\colon R/J \longrightarrow S$ mit $\bar{f} \circ \pi = f$, nämlich $\bar{f}(a + J) := f(a)$.*
Ferner gilt:

$$\begin{aligned} \mathrm{Bild}(\bar{f}) &= \mathrm{Bild}(f), \\ \ker(\bar{f}) &= \ker(f)/J. \end{aligned}$$

Insbesondere ist $\bar{f}$ genau dann injektiv, wenn $J = \ker(f)$ gilt.

Satz 5.1.7 *(Chinesischer Restsatz) Seien $I_1, \ldots, I_n$ Ideale in R mit $I_k + I_l = R$ für $k \neq l$. Seien $a_1, \ldots, a_n \in R$. Dann gibt es ein $x \in R$ mit $x \equiv a_k \pmod{I_k}$ für $k = 1, \ldots, n$. Falls $y \in R$ eine weitere Lösung dieser simultanen Kongruenzen ist, so gilt $x \equiv x \pmod{J}$, wobei $J := I_1 \cap \ldots \cap I_n$. Zwei verschiedene Lösungen sind also modulo J eindeutig bestimmt.*

In äquivalenter Weise kann man den chinesischen Restsatz wie folgt formulieren.

Satz 5.1.8 *Seien $I_1, \ldots, I_n$ Ideale in R mit $I_k + I_l = R$ für $k \neq l$. Dann ist die Abbildung*

$$\begin{aligned} \varphi\colon R/J &\longrightarrow R/I_1 \times \ldots \times R/I_n, \\ x + J &\mapsto (x + I_1, \ldots, x + I_n) \end{aligned}$$

ein Isomorphismus von Ringen.

Die Surjektivität von φ ist dabei äquivalent zur Existenzaussage im chineschen Restsatz, die Injektivität ist äquivalent zur Eindeutigkeitsaussage.
Die Ringe $\mathbb{Z}$ und $K[x]$ sind Hauptidealringe. Tatsächlich sind diese Ringe sogar Beispiele für sogenannte Euklidische Ringe. Wir werden sehen, dass euklidische Ringe stets Hauptidealringe sind.

Definition 5.1.9 Ein nullteilerfreier Ring R heißt euklidisch, falls es eine Abbildung $\nu : R\backslash\{0\} \longrightarrow \mathbb{N}_0$ gibt, so daß gilt: zu $a, b \in R, b \neq 0$, gibt es $q, r \in R$ mit

$$a = qb + r, \quad r = 0 \text{ oder } \nu(r) < \nu(b).$$

Die Abbildung ν nennt man euklidische Norm.

Satz 5.1.10 *Jeder euklidische Ring ist ein Hauptidealring.*

Definition 5.1.11 Seien $a_1, \ldots, a_n \in R$. Wir nennen $d \in R$ einen größten gemeinsamen Teiler von $a_1, \ldots, a_n$, wenn die folgenden zwei Eigenschaften erfüllt sind:
a) $d \mid a_i$ für $i = 1 \ldots, n$.
b) Falls $d_1 \mid a_i$ für $i = 1, \ldots, n$ und ein $d_1 \in R$ gilt, so gilt auch $d_1 \mid d$.

Bemerkung 5.1.12 Ein ggT (falls er existiert) ist bis auf Assoziiertheit eindeutig bestimmt. D.h., sind d_1 und d_2 zwei ggT von $a_1, \ldots, a_n$, so gibt es eine Einheit $u \in R^\times$ mit $d_1 = ud_2$.

In beliebigen kommutativen Ringen existieren ggT im Allgemeinen nicht. Jedoch gilt der folgende Satz.

Satz 5.1.13 *Sei R ein Hauptidealring und $a, b \in R$. Sei $(a) + (b) = (d)$. Dann ist d ein ggT von a und b.*

In euklidischen Ringen verfügen wir über einen Algorithmus zur expliziten Berechnung von $\mathrm{ggT}(a, b)$. Der erweiterte euklidische Algorithmus erlaubt sogar die Berechnung einer Darstellung

$$ggT(a, b) = xa + yb \text{ mit } x, y \in R.$$

Allgemeiner gilt im Hauptidealring: Sei $(a_1, \ldots, a_n) = (d)$, dann ist d ein ggT. Aufgrund der Formel

$$\mathrm{ggT}(a_1, \ldots, a_n) = \mathrm{ggT}(\mathrm{ggT}(a_1, \ldots, a_{n-1}), a_n)$$

kann man in euklidischen Ringen den ggT sowie eine Darstellung

$$\mathrm{ggT}(a_1, \ldots, a_n) = x_1 a_1 + \ldots + x_n a_n$$

algorithmisch berechnen.

Definition 5.1.14 Ein Element $0 \neq p \in R \setminus R^\times$ heißt irreduzibel, falls p keine echten Teiler hat, d.h. aus $p = ab$ folgt $a \in R^\times$ oder $b \in R^\times$.

Die irreduziblen Elemente in $\mathbb{Z}$ sind genau die Primzahlen und ihre Negativen. In beliebigen Ringen gibt es jedoch einen Unterschied zwischen den Begriffen "prim" und "irreduzibel".

Definition 5.1.15 Ein Element $0 \neq p \in R \setminus R^\times$ heißt prim oder Primelement, falls gilt:

$$p \mid ab \implies p \mid a \text{ oder } p \mid b.$$

Bemerkung 5.1.16 Falls R nullteilerfrei ist, so gilt: p prim $\implies$ p irreduzibel.

Die Umkehrung ist im Allgemeinen falsch, gilt aber in Hauptidealringen.

Satz 5.1.17 *Sei R ein Hauptidealring. Dann gilt:*

$$p \text{ ist prim} \iff p \text{ ist irreduzibel.}$$

Definition 5.1.18 Sei R nullteilerfrei. Dann ist R ein ZPE-Ring (oder faktoriell), falls gilt:
(i) Jedes Element $a \in R \setminus \{0\}, a \notin R^\times$, kann man als Produkt

$$a = c_1 \cdots c_n \text{ mit irreduziblen } c_i \in R$$

schreiben.
(ii) (Eindeutigkeit) Falls $a = c_1 \cdots c_n = d_1 \cdots d_m$ mit irreduziblen Elementen c_i und d_j, so gilt $n = m$ und (bis auf Numerierung) $c_i \sim d_i$.

Satz 5.1.19 *Jeder Hauptidealring ist ein ZPE-Ring.*

Grundlegend für den Beweis dieses Satzes ist das

Lemma 5.1.20 *Sei R ein Hauptidealring. Dann wird jede aufsteigende Kette*

$$(a_0) \subseteq (a_1) \subseteq (a_2) \subseteq \ldots$$

von Idealen in R stationär, d.h. es gibt $n \in \mathbb{N}$, so daß $(a_i) = (a_n)$ für alle $i \geq n$.

5.2 Modultheorie

Moduln sind Verallgemeinerungen von a) Vektorräumen ("Vektorräume über Ringen") b) abelschen Gruppen (diese sind Moduln über $\mathbb{Z}$).

Definition 5.2.1 Sei R ein Ring. Ein (Links)-Modul ist eine (additive) abelsche Gruppe M mit einer Funktion $R \times M \to M, (r, m) \mapsto rm$, so daß für alle $r, s \in R, a, b \in M$ gilt:

$$\begin{aligned} (i) \quad & r(a+b) = ra + rb \\ (ii) \quad & (r+s)a = ra + sa \\ (iii) \quad & r(sa) = (rs)a \\ (iv) \quad & 1_R a = a \end{aligned}$$

Bemerkung: Völlig analog definiert man Rechtsmoduln. Bei uns sind Moduln in aller Regel Linksmoduln.

Definition 5.2.2 Seien A, B R-Moduln. Eine Abbildung $f : A \to B$ heißt R-Modulhomomorphismus, falls für alle $a, b \in A$, $r \in R$ gilt:

$$f(a+b) = f(a) + f(b), \quad f(ra) = rf(a).$$

Satz 5.2.3 *Seien $N \subseteq M$ R-Moduln. Dann wird die abelsche Gruppe M/N durch die Definition $r(m+N) := rm + N$ zu eine R-Modul. Die kanonische Projektion $\pi : M \to M/N$ ist ein Modulepimorphismus mit* $\ker(\pi) = N$.

Bemerkung: Es gelten für Moduln dem Sinn nach dieselben Isomorphissätze wie für Gruppen (bzw. Ringe).

Folgendes Beispiel ist die Motivation für unser Studium von Moduln über Hauptidealringen, dass wir im nächsten Abschnitt beginnen werden. Sei V ein K-Vektorraum und $\varphi\colon V \longrightarrow V$ ein Endomorphismus. Dann wird V durch die Setzung $f(x) \cdot v := f(\varphi)(v)$ zu einem $K[x]$-Modul.
Für Matrizen $A, B \in M_n(K)$ betrachten wir die folgende Äquivalenzrelation:

$$A \approx B \iff \exists S \in \mathrm{Gl}_n(K) : B = S^{-1}AS.$$

Man sagt, A und B sind zueinander konjugiert.
Sei nun $V = K^n$. Wie üblich identifizieren wir A und B mit Endomorphismen von V. Wir schreiben $V = V_A$ wenn wir V als $K[x]$-Modul betrachten vermöge $f(x) \cdot v := f(A)v$. Analog für V_B. Dann gilt:

$$V_A \simeq V_B \text{ als } K[x] - \text{Moduln} \iff A \approx B.$$

Definition 5.2.4 Sei M ein R-Modul.
a) Für $N \subseteq M$ setzen wir

$$\langle N \rangle := \left\{ \sum_{j=1}^{k} r_j n_j \mid k \in \mathbb{N}, r_j \in R, n_j \in N \right\}.$$

$\langle N \rangle$ ist offenbar der kleinste Teilmodul von M, der N enthält.
b) Sei J eine beliebige Indexmenge und $N_j \subseteq M$ Teilmoduln von M. Dann heißt der Untermodul

$$\sum_{j \in J} N_j := \left\{ \sum_{j \in J} n_j \mid n_j \in N_j, \text{ fast alle } n_j = 0 \right\}$$

die Modulsumme der N_j.
c) Wir schreiben

$$M = \bigoplus_{j \in J} N_j$$

und nennen dies die direkte Summe der N_j, falls $M = \sum_{j \in J} N_j$ und falls aus $\sum_{j \in J} n_j = 0$ stets $n_j = 0$ für alle $j \in J$ folgt.

Bemerkung 5.2.5 Es gilt:

$$M = \bigoplus_{j \in J} N_j \iff \forall k \in J : N_k \cap \sum_{j \in J \setminus \{k\}} N_j = \{0\}.$$

Definition 5.2.6 Sei R ein kommutativer Ring und $M \subseteq R$ ein Ideal mit $M \neq R$. Dann nennen wir M maximal, falls für alle Ideal J von R mit $M \subseteq J$, $M \neq J$, folgt, dass $J = R$.

Unter Verwendung des Zornschen Lemmas haben wir folgenden Satz gezeigt:

Satz 5.2.7 *Sei R ein kommutativer Ring mit 1 und $I \subseteq R$ ein Ideal mit $I \neq R$. Dann gibt es ein maximales Ideal M in R mit $I \subseteq M$. Insbesondere hat R maximale Ideale.*

Satz 5.2.8 *Sei R ein kommutativer Ring und $M \subseteq R$ ein Ideal. Dann gilt:*

$$R/M \text{ ist ein Körper} \iff M \text{ ist maximal.}$$

Man beachte, dass die maximalen Ideale in einem Hauptidealring genau diejenigen Ideale (p) sind, die von irreduziblen Elementen erzeugt werden. Ferner sind im Hauptidealring die Begriffe "prim" und "irreduzibel" äquivalent. Spezialfälle des letzten Satzes sind also die endlichen Körper $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Definition 5.2.9 Ein R-Modul heißt frei in den Erzeugenden $f_j \quad (j \in J)$, falls $F = \oplus_{j \in J} R f_j$, wobei zusätzlich gilt:

$$\sum_{j \in J} r_j f_j = 0 \iff r_j = 0, \forall j \in J.$$

Satz 5.2.10 *Sei R ein kommutativer Ring und $F = \oplus_{j=1}^{k} R f_j$ ein endlich erzeugter freier R-Modul. Dann ist k durch F eindeutig bestimmt. Wir setzen $k = \mathrm{rg}(F)$ und nennen dies den Rang von F.*

Bemerkung 5.2.11 Sei K ein Körper und $V := \{(a_0, a_1, \ldots) \mid a_i \in K\}$ der K-Vektorraum der Folgen in K. Sei $R := \mathrm{End}_K(V)$. Dann ist R ein nicht-kommutativer Ring bez. Addition und Komposition von Endomorphismen. Wir haben gezeigt, dass es für jede natürliche Zahl n einen Isomorphismus $R^n \simeq R$ gibt. In nicht-kommutativen Ringen ist der Rang also nicht wohldefiniert.

Der erste Teil des folgenden Satzes verallgemeinert die aus der Theorie der Vektorräume bekannte Tatsache, das eine lineare Abbildung durch die Angabe der Bilder einer Basis eindeutig festgelegt ist. Der zweite Teil verallgemeinert die Kern-Bild-Zerlegung.

Satz 5.2.12 *a) Sei $F = \oplus_{j \in J} R f_j$ ein freier R-Modul. Sei M ein R-Modul und sei $m_j \in M$ für alle $j \in J$. Dann gibt es genau einen R-Modulhomomorphismus $\alpha : F \longrightarrow M$ mit $\alpha(f_j) = m_j$.*
b) Sei F wieder ein freier R-Modul. Sei weiterhin M ein R-Modul und $\alpha : M \longrightarrow F$ ein surjektiver R-Modulhomomorphismus. Dann gibt es einen Untermodul N von M mit

$$M = \ker(\alpha) \oplus N \text{ und } N \simeq F \text{ als } R - \text{Modul.}$$

Die Theorie der R-Moduln ist vor allem deshalb komplizierter als die Vektorraumtheorie, weil es Torsionselemente gibt.

Definition 5.2.13 Sei R nullteilerfrei und M ein R-Modul.
a) Ein $m \in M$ heißt Torsionselement, falls es ein $r \in R \setminus \{0\}$ gibt, so dass $rm = 0$.
b) Die Menge der Torsionselemente bezeichnen wir mit $T(M)$.
c) M heißt torsionsfrei, falls $T(M) = \{0\}$.

Lemma 5.2.14 *Sei R nullteilerfrei und M ein R-Modul.*
a) $T(M)$ ist ein Teilmodul von M.
b) $M/T(M)$ ist torsionsfrei.

Satz 5.2.15 *Sei R ein Hauptidealring.*
a) Sei A ein Teilmodul des freien R-Moduls $F = \oplus_{j=1}^{k} Rf_j$ vom Rang k. Dann ist A ein freier R-Modul vom Rang $\leq k$.
b) Ist M endlich erzeugt und torsionsfrei, so ist M frei (von endlichem Rang).
c) Ist M endlich erzeugt, so gilt

$$M = T(M) \oplus F,$$

wobei F frei ist und $F \simeq T/T(M)$ (als R-Moduln).

Auf dem nächsten Übungblatt werden wir zeigen, dass kann man in b) und c) im Allgemeinen nicht auf die endliche Erzeugtheit verzichten kann.
Um die Struktur von Torsionsmoduln zu studieren, setzen wir ab jetzt voraus, dass R ein euklidischer Ring ist. Im folgenden sei $M = \bigoplus_{i=1}^{n} Ru_i$ ein freier R-Modul vom Rang n und $N \subseteq M$ ein Teilmodul gegeben durch Erzeugende $v_1, \ldots, v_k$.

Satz 5.2.16 *(Elementarteilersatz) Es gibt Basen $u'_1, \ldots, u'_n$ von M und $v'_1, \ldots, v'_m$ von N mit $m \leq n$ und*

$$v'_i = \epsilon_i u'_i, i = 1, \ldots, m, \quad \epsilon_1 \mid \epsilon_2 \mid \ldots \mid \epsilon_m.$$

Proof Der Beweis ist algorithmisch und kann als Verallgemeinerung des Gaußschen Algorithmus aufgefasst werden. Sei zunächst eine beliebige Basis $u_1, \ldots, u_n$ von M gegeben und beliebige Erzeugende $v_1, \ldots, v_k$ von N. Schreibe

$$v_l = \sum_{i=1}^{n} \alpha_{il} u_i \text{ mit } \alpha_{il} \in R.$$

Sei $A = (\alpha_{il}) \in R^{n \times k}$. Wir werden die Matrix A durch schrittweises Abändern der Basis $u_1, \ldots, u_n$ und des Erzeugendensystems $v_1, \ldots, v_k$ in die Form

$$\left(\begin{array}{ccc|c} \epsilon_1 & & & \\ & \ddots & & 0 \\ & & \epsilon_m & \\ \hline & 0 & & 0 \end{array}\right)$$

transfromieren. Erlaubte Abänderungen sind dabei:
(1) Vertauschung zweier u oder v. Dies entspricht der Vertauschung zweier Zeilen oder Spalten.
(2) Ersetzung eines u_i durch $u_i + \lambda u_j, \lambda \in R, i \neq j$. Wegen

$$v_l = \sum_{s=1}^{n} \alpha_{sl} u_s = \sum_{s=1, s \neq i,j}^{n} \alpha_{sl} u_s + \alpha_{il}(u_i + \lambda u_j) + (\alpha_{jl} - \alpha_{il}\lambda) u_j$$

entspricht dies der Ersetzung der j-ten Zeile durch j-te Zeile minus λ mal i-te Zeile.
(3) Ersetzung eines v_i durch $v_i - \lambda v_j, \lambda \in R, i \neq j$. Dies entspricht der Ersetzung der i-ten Spalte durch i-te Spalte minus λ mal j-te Spalte.

Wir wenden nun den folgenden Algorithmus auf die Matrix A an:
Schritt 1: Durch Vertauschen von Zeilen und Spalten bringe man das Element ungleich Null von kleinster euklidischer Norm an die Stelle $(1,1)$.
Schritt 2: Durch Subtraktion geeigneter Vielfacher der ersten Zeile, kann man erreichen, dass A von der Form

$$A = \begin{pmatrix} \alpha_{11} & * & \dots & * \\ \gamma_2 & & & \\ \vdots & & * & \\ \gamma_n & & & \end{pmatrix}$$

ist, wobei jedes γ_i entweder gleich Null ist oder $\varphi(\gamma_i) < \varphi(\alpha_{11})$ gilt. Falls alle γ_i gleich Null sind, so gehe zu Schritt 3. Andernfalls gehe zu Schritt 1.
Schritt 3: Durch Subtraktion geeigneter Vielfacher der ersten Spalte, kann man sodann erreichen, dass A von der Form

$$A = \left(\begin{array}{c|ccc} \alpha_{11} & \gamma_1 & \dots & \gamma_k \\ \hline 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{array}\right)$$

ist, wobei jedes γ_i entweder gleich Null ist oder $\varphi(\gamma_i) < \varphi(\alpha_{11})$ gilt. Falls alle γ_i gleich Null sind, so gehe zu Schritt 4. Andernfalls gehe zu Schritt 1.
Schritt 4: Falls $A' = 0$ so beende den Algorithmus.
Schritt 5: Falls alle Einträge von A' durch α_{11} teilbar sind, so gehe mit A' in Schritt 1.
Schritt 6: Sei α_{ik} ein Koeffizient in A', der nicht durch α_{11} teilbar ist. Teile mit Rest,

$$\alpha_{ik} = \alpha_{11}\beta + \gamma, \gamma \neq 0, \varphi(\gamma) < \varphi(\alpha_{11}).$$

Addiere nun die erste Zeile zur i-ten Zeile und subtrahiere dann β mal 1. Spalte von der k-ten Spalte. Dann kommt an der Stelle (i,k) gerade γ zu stehen. Gehe mit A in Schritt 1.
Der Algorithmus endet nach endlich vielen Schritten, da $\varphi\colon R \setminus \{0\} \longrightarrow \mathbb{N}_0$ und in den Schritten 2,3 und 5 die minimale euklidische Norm der Elemente von A verringert wird. □

Bemerkung 5.2.17 Die Aussage des Elementarteilersatzes ist gleichbedeutend mit der folgenden Aussage: Es gibt Matrizen $B \in \mathrm{Gl}_n(R)$, $C \in \mathrm{Gl}_k(R)$, so dass

$$B^{-1}AC = \left(\begin{array}{ccc|c} \epsilon_1 & & & \\ & \ddots & & 0 \\ & & \epsilon_m & \\ \hline & 0 & & 0 \end{array}\right)$$

Wir wenden nun den Elementarteilersatz an, um die Struktur von endlich-erzeugten Moduln über euklidischen Ringen zu studieren. Sei dazu $M = \langle m_1, \dots, m_n \rangle$ ein endlich erzeugter R-Modul. Sei $F = \bigoplus_{i=1}^n Ru_i$ der freie Modul vom Rang n. Dann ist die Abbildung

$$f\colon F \longrightarrow M, \quad \sum_{i=1}^n r_i u_i \mapsto \sum_{i=1}^n r_i m_i,$$

ein surjektiver Modulhomomorphismus. Sei $N := \ker(f)$. Dann gilt nach dem Isomorphiesatz:

$$F/N \simeq M.$$

Nach dem Elementarteilersatz gibt es Basen $u_1, \dots, u_n$ von F und $v_1, \dots, v_m$ von N mit $m \leq n$ sowie $\epsilon_1, \dots, \epsilon_m$ mit

$$v_1 = \epsilon_1 u_1, \dots, v_m = \epsilon_m u_m, \quad \epsilon_1 \mid \epsilon_2 \mid \dots \mid \epsilon_m.$$

Es folgt dann:

$$\begin{aligned} F/N &\simeq \bigoplus_{i=1}^{m} Ru_i/R\epsilon_i u_i \oplus \bigoplus_{i=m+1}^{n} Ru_i \\ &\simeq \bigoplus_{i=1}^{m} R/R\epsilon_i \oplus R^{m-n}. \end{aligned} \tag{1}$$

Insbesondere gilt also wegen $R/R\epsilon = 0$ für $\epsilon \in R^\times$

$$T(M) \simeq \bigoplus_{i=1,\epsilon_i \notin R^\times}^{m} R/R\epsilon_i, \quad r = \mathrm{rk}(M) = n - m.$$

Bis auf die Eindeutigkeitsaussage haben wir damit den folgenden wichtigen Satz vollständig bewiesen.

Satz 5.2.18 *Sei R ein euklidischer Ring und M ein endlich erzeugter R-Modul. Dann gibt es $r \in \mathbb{N}_0$ und $\epsilon_1, \ldots, \epsilon_s \in R \setminus R^\times$ mit $\epsilon_1 \mid \epsilon_2 \mid \ldots \mid \epsilon_s$, so dass*

$$M \simeq \bigoplus_{i=1}^{s} R/R\epsilon_i \oplus R^k.$$

Der Rang r ist eindeutig durch den Isomorphietyp von M bestimmt. Ebenso sind die $\epsilon_1, \ldots, \epsilon_s$ bis auf Assoziiertheit durch den Isomorphietyp von M eindeutig bestimmt.

Definition 5.2.19 Die durch M eindeutig bis auf Assoziiertheit bestimmten Elemente $\epsilon_1, \ldots, \epsilon_s$ aus Satz 5.2.18 nennt man die Elementarteiler von M. Falls $R = \mathbb{Z}$, so normieren wir die Elementarteiler durch dir Forderung $\epsilon_i > 0$. Falls $R = \mathbb{K}[x]$, so normieren wir die Elementarteiler durch die Forderung, dass der führende Koeffizient von ϵ_i gleich 1 ist. Damit werden die Elementarteiler in diesen Fällen eindeutig (und nicht nur eindeutig bis auf Assoziiertheit).

Bemerkung 5.2.20 Seien M, M' zwei endlich erzeugte R-Moduln mit Rang r und r' sowie Elementarteilern $\epsilon_1, \ldots, \epsilon_s$ und $\epsilon'_1, \ldots, \epsilon'_{s'}$. Dann sind M und M' genau dann isomorph, wenn $r = r'$ gilt und die Reihen der Elementarteiler übereinstimmen.

Definition 5.2.21 Sei R ein Hauptidealring und M ein R-Modul. Sei π ein irreduzibles Element von R. Dann nennt man

$$T_\pi(M) = \{m \in M \mid \pi^e m = 0 \text{ für ein geeignetes } e \in \mathbb{N}_0\}$$

den π-Torsionsmodul von M.

Man zeigt leicht, dass $T_\pi(M)$ ein Teilmodul von $T(M) \subseteq M$ ist.

Definition 5.2.22 Die Elemente

$$\pi_1^{e_{1,1}}, \ldots, \pi_1^{e_{s,1}}, \pi_2^{e_{1,2}}, \ldots, \pi_2^{e_{s,2}}, \ldots, \pi_t^{e_{1,t}}, \ldots, \pi_t^{e_{s,t}}$$

mit

$$\begin{aligned} &e_{1,1} \geq e_{2,1} \geq \ldots \geq e_{s,1} \geq 0, \\ &e_{1,2} \geq e_{2,2} \geq \ldots \geq e_{s,2} \geq 0, \\ &\ldots \\ &e_{1,t} \geq e_{2,t} \geq \ldots \geq e_{s,t} \geq 0 \end{aligned}$$

nennt man die Invariantenteiler von M.

Lemma 5.2.23 *Sei M ein endlich erzeugter R-Torsionsmodul. Dann entsprechen sich Elementarteiler und Invariantenteiler eineindeutig.*

Es genügt also zu zeigen, dass die Reihe der Invariantenteiler eindeutig durch den Isomorphietyp von M bestimmt ist.
Für den noch ausstehenden Eindeutigkeitsbeweis können wir uns oE auf die Betrachtung von endlich erzeugten R-Torsionsmoduln M beschränken. Für jedes irreduzible Element π ist $T_\pi(M)$ bis auf Isomorphie eindeutig durch den Isomorphietyp von M bestimmt. Es reicht also zu zeigen, dass die Invariantenteiler

$$\pi_j^{e_{1,j}}, \ldots, \pi_j^{e_{s,j}} \text{ mit } e_{1,j} \geq e_{2,j} \geq \ldots \geq e_{s,j}$$

eindeutig durch $T_{\pi_j}(M)$ bestimmt sind. Dazu setzen wir $\pi := \pi_j$ und entsprechend $T := T_{\pi_j}(M)$. Sei $k := R/(\pi)$ der Restklassenkörper. Dann ist $T/\pi T$ ein k-Vektorraum und es gilt

$$\dim_k(T/\pi T) = \text{ Anzahl der } e_{i,j} > 0.$$

Sodann betrachten wir den k-Vektorraum $\pi T/\pi^2 T$ und zeigen

$$\dim_k(\pi T/\pi^2 T) = \text{ Anzahl der } e_{i,j} > 1.$$

Also ist die Anzahl der $e_{i,j}$ mit $e_{i,j} = 1$ gegeben durch

$$\dim_k(T/\pi T) - \dim_k(\pi T/\pi^2 T),$$

was nur vom Isomorphietyp von T abhängt. Sukzessive zeigt man auf diese Weise, dass

$$|\{e_{i,j} \text{ mit } e_{i,j} = l\}| = \dim_k(\pi^{l-1}T/\pi^l T) - \dim_k(\pi^l T/\pi^{l+1}T).$$

Die rechte Seite hängt dabei nur vom Isomorphietyp von T ab. Der Isomorphietyp von T wiederum ist vom Isomorphietyp von M eindeutig bestimmt. Damit ist der Beweis der Eindeutigkeit vollständig erbracht.
Wir fassen unser Hauptresultat nochmals zusammen.

Satz 5.2.24 *Sei R ein euklidischer Ring und M ein endlich erzeugter R-Modul. Dann gibt es $r \in \mathbb{N}_0$, irreduzible Elemente $\pi_1, \ldots, \pi_t$, sowie natürliche Zahlen $e(1,j) \geq \cdots \geq e(s,j) \geq 0$, $j = 1, \ldots, t$, so dass*

$$\begin{aligned} M &\cong R^r \oplus T_{\pi_1}(M) \oplus \cdots T_{\pi_t}(M), \text{ wobei} \\ T_{\pi_j}(M) &\cong R/(\pi_j^{e_{1,j}}) \oplus R/(\pi_j^{e_{2,j}}) \oplus \cdots \oplus R/(\pi_j^{e_{s,j}}). \end{aligned}$$

Die Zahlen r sowie die Invariantenteiler (und damit auch die Elementarteiler) sind eindeutig (bis auf Assoziiertheit) durch den Isomorphietyp von M bestimmt.

Abschließend notieren wir den sogenannten Hauptsatz über endlich erzeugte abelsche Gruppen. Man erinnere sich, dass die endlich erzeugten abelschen Gruppen genau die endlich erzeugten $\mathbb{Z}$-Moduln sind.

Folgerung 5.2.25 *Für eine endlich erzeugte abelsche Gruppe A gibt es ein $r \in \mathbb{N}_0$, sowie Primzahlen $p_1, \ldots, p_t$ sowie natürliche Zahlen $e_{1,j} \geq \cdots \geq e_{s,j} \geq 0$, $j = 1, \ldots, t$, so dass*

$$\begin{aligned} A &\cong \mathbb{Z}^k \oplus T_{p_1}(A) \oplus \cdots T_{p_t}(A), \text{ wobei} \\ T_{p_j}(A) &\cong \mathbb{Z}/(p_i^{e_{1,j}}) \oplus \mathbb{Z}/(p_i^{e_{2,j}}) \oplus \cdots \oplus \mathbb{Z}/(p_i^{e_{s,j}}). \end{aligned}$$

6 Allgemeine und Jordansche Normalform

Definition 6.0.1 Sei R ein kommutativer Ring mit 1.
(a) Seien $A, B \in R^{n\times m}$. Dann heißt A äquivalent zu B, in Zeichen $A \sim B$, falls es $P \in \mathrm{Gl}_n(R)$ und $Q \in \mathrm{Gl}_m(R)$ gibt, so dass

$$B = P^{-1}AQ$$

gilt.
(b) Seien $A, B \in M_n(R) = R^{n\times n}$. Dann heißt A konjugiert oder ähnlich zu B, in Zeichen $A \approx B$, falls es $S \in \mathrm{Gl}_n(R)$ gibt, so dass

$$B = S^{-1}AS$$

gilt.

Wir werden im Folgenden in jeder Äquivalenzklasse von Matrizen in $M_n(K)$, K ein Körper, bezüglich der Äquivalenzrelation $\approx$ einen kanonischen Vertreter bestimmen. Diesen Vertreter nennen wir dann die allgemeine Normalform von A. Auf diese Weise können wir entscheiden, ob zwei gegebene Matrizen A und B konjugiert sind.

Definition 6.0.2 Sei $A \in M_n(K) = K^{n\times n}$. Dann heißt die Matrix

$$M_A(x) := xE - A \in M_n(K[x])$$

die charakteristische Matrix von A.

Sei V ein K-Vektorraum, und sei $A \in End_K(V)$ fest gewählt. Betrachte V als $K[x]$-Modul mittels

$$K[x] \times V \to V,\ (f, v) \mapsto f \cdot v := f(A)v.$$

Sei $\dim_K V < \infty$.
Dann ist V ein endlich erzeugter $K[x]$-Torsionsmodul. Da $K[x]$ ein euklidischer Ring ist, können wir Theorem 5.2.24 auf V anwenden. Die resultierende Zerlegung des $K[x]$-Moduls V in eine endliche direkte Summe von zyklischen $K[x]$-Torsionsmoduln ist die Grundlage der allgemeinen Theorie der Normalformen.
Im Folgenden werden wir nicht mehr zwischen $A \in \mathrm{End}_K(V)$ und einer darstellenden Matrix $A \in K^{n\times n}$ unterscheiden. Dies stellt zwar einen kleinen Missbrauch der Notation dar, da die darstellende Matrix von der Wahl einer Basis in V abhängt, vereinfacht jedoch die Notationen erheblich. Sämtlich Definitonen und Resultate sind aber aus offensichtlichen Gründen davon unabhängig.
Wenn wir V als $K[x]$-Modul mittels einer Matrix A betrachten, dann schreiben wir im weiteren $V = V_A$, um anzudeuten, dass $f(x) \cdot v := f(A)v$ für alle Polynome $f \in K[x]$ und alle $v \in V$.

Satz 6.0.3 *Seien $A, B \in M_n(K)$. Dann sind folgende Aussagen äquivalent:*
(i) A ist konjugiert zu B, in Zeichen, $A \approx B$.
(ii) $V_A \simeq V_B$ als $K[x]$-Moduln.
(iii) $K[x]^n/\langle M_A(x)\rangle \simeq K[x]^n/\langle M_B(x)\rangle$ als $K[x]$-Moduln.
(iv) $M_A(x)$ und $M_B(x)$ sind äquivalent, in Zeichen, $M_A(x) \sim M_B(x)$.
(v) $M_A(x)$ und $M_B(x)$ haben die selben Elementarteiler.
(vi) $M_A(x)$ und $M_B(x)$ haben die selben Invariantenteiler.

Lemma 6.0.4 *Seien $A \in M_n(K)$ und $c_1(x) \mid c_2(x) \mid \ldots \mid c_n(x)$ die Polynome aus dem Elementarteilersatz, so dass*

$$K[x]^n/\langle M_A(x)\rangle \simeq \bigoplus_{i=1}^{n} K[x]/(c_i(x))$$

gilt. Dann gilt:
(a) $\chi_A(x) = \prod_{i=1}^{n} c_i(x)$.
(b) $\mu_A(x) = c_n(x)$.

Der Satz 6.0.3 rechtfertigt die folgende Definition.

Definition 6.0.5 Sei $A \in M_n(K)$. Seien $g_1(x), \ldots, g_r(x)$ die Elementarteiler von $M_A(x)$. oE seien die g_i normiert. Dadurch sind die g_i durch A eindeutig bestimmt (nicht nur bis auf Einheiten in $K[x]$). Wir nennen die g_i im weiteren auch die Elementarteiler der Matrix A. Analog bezeichnen wir die normierten Invariantenteiler von $M_A(x)$ auch als die Invariantenteiler von A.

Zu $g(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in K[x], \deg(g) = n \geq 1$, betrachte

$$B_g := \begin{pmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ & 1 & & & -a_2 \\ & & \cdots & & \cdots \\ & & & \cdots & \cdots \\ & & & 0 & -a_{n-2} \\ & & & 1 & -a_{n-1} \end{pmatrix}$$

Für $n = 1$ ist $B_g = (-a_0)$. Wir nennen B_g die Begleitmatrix zu g.

Lemma 6.0.6 *Sei $g(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in K[x], \deg(g) = n \geq 1$ und $B = B_g$ die Begleitmatrix. Dann gilt:*
(i) Das charakteristische Polynom von B ist gegeben durch $\chi_B(x) = g(x)$.
(ii) Es gilt:

$$M_B(x) \sim \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & g \end{pmatrix}$$

Folgerung 6.0.7 *Es seien $g_1(x), \ldots, g_r(x) \in K[x]$ normierte Polynome vom Grad ≥ 1 mit*

$$g_i \mid g_{i+1}, \quad i = 1, \ldots, r-1.$$

Sei

$$B = B_{g_1,\ldots,g_r} = \begin{pmatrix} B_{g_1} & & \\ & \ddots & \\ & & B_{g_r} \end{pmatrix} \in M_n(K),$$

wobei $n = \sum_{i=1}^{r} \deg(g_i(x))$. Dann hat B die Elementarteiler $g_1, \ldots, g_r$.

Satz 6.0.8 *(Frobeniussche Normalform) Sei $A \in M_n(K)$. Dann ist A zu genau einer Matrix $B_{g_1,\ldots,g_r}$ ähnlich, wobei $g_1, \ldots, g_r$ normierte Polynome vom Grad ≥ 1 sind mit $g_1 \mid g_2 \mid \ldots \mid g_r$. Die Polynome $g_1, \ldots, g_r$ sind hierbei genau die Elementarteiler der charakteristischen Matrix $M_A(x)$.*

Lemma 6.0.9 *Sei $g = h_1 \cdots h_k$ ein Produkt von paarweise teilerfremden Polynomen $h_1, \ldots, h_k \in K[x]$ vom Grad ≥ 1. Dann gilt:*

$$B_g \approx \begin{pmatrix} B_{h_1} & & \\ & \ddots & \\ & & B_{h_k} \end{pmatrix}.$$

Satz 6.0.10 *(Weierstraßsche Normalform) Sei $A \in M_n(K)$. Dann gibt es ein bis auf Reihenfolge eindeutig bestimmtes System $h_1, \ldots, h_m$ von Potenzen normierter irreduzibler Polynome, so dass A zu der Matrix*

$$B_{h_1,\ldots,h_m} = \begin{pmatrix} B_{h_1} & & \\ & \ddots & \\ & & B_{h_m} \end{pmatrix}$$

ähnlich ist. Die Polynome $h_1, \ldots, h_r$ sind hierbei genau die Invariantenteiler der charakteristischen Matrix $M_A(x)$.

Falls K ein algebraisch abgeschlossener Körper ist (z.B. $K = \mathbf{C}$), so kommen als Invariantenteiler nur Potenzen von linearen Polynomen vor. Sei also

$$h(x) = (x - \alpha)^e, \quad e \geq 1.$$

Lemma 6.0.11 *Sei K beliebig und $h(x) = (x - \alpha)^e, e \geq 1$. Dann gilt:*

$$B_h \approx J(\alpha, e) := \begin{pmatrix} \alpha & & & & 0 \\ 1 & \alpha & & & 0 \\ & \ddots & \ddots & & \vdots \\ & & \ddots & \alpha & 0 \\ & & & 1 & \alpha \end{pmatrix}.$$

Satz 6.0.12 *(Jordansche Normalform) Sei $A \in M_n(K)$ und das charakteristische Polynom $\chi_A(x)$ zerfalle vollständig in Linearfaktoren. Dann gibt es bis auf die Reihenfolge eindeutig bestimmtes System von Jordanmatrizen $J_1, \ldots, J_m$, so dass*

$$A \approx \begin{pmatrix} J_1 & & \\ & \ddots & \\ & & J_m \end{pmatrix}$$

Bemerkung 6.0.13 (1) Wegen

$$\chi_A(x) = \prod_j h_j(x) = \prod_j (x - \alpha_j)^{e_j}$$

sind die α_j genau die Eigenwerte von A.
(2) Aus der Jordanschen Normalform lässt sich auch das Minimalpolynom direkt ablesen. Sortiere dazu die Jordankästchen nach Eigenwerten und Größe,

$$\begin{pmatrix} J(\alpha_1, e_{1,1}) & & & & & & & & \\ & \ddots & & & & & & & \\ & & J(\alpha_1, e_{1,n_1}) & & & & & & \\ & & & \ddots & & & & & \\ & & & & \ddots & & & & \\ & & & & & J(\alpha_s, e_{s,1}) & & & \\ & & & & & & \ddots & & \\ & & & & & & & J(\alpha_s, e_{1,n_s}) \end{pmatrix}$$

mit $e_{i,1} \leq e_{i,2} \leq \ldots \leq e_{i,n_i}$. Dann gilt:

$$\mu_A(x) = \prod_{i=1}^{s} (x - \alpha_i)^{e_{i,n_i}}.$$

(3) Die folgenden drei Aussagen sind äquivalent:

(i) A ist diagonalisierbar.

(ii) Die Jordansche Normalform ist eine Diagonalmatrix.

(iii) Jedes Jordankästchen hat Rahmengröße 1.

(4) Die Dimension des Eigenraums zum Eigenwert α_i ist gegeben durch die Anzahl n_i der Kästchen zum Eigenwert α_i.

Ende des Protokolls

Das Protokoll endet an dieser Stelle. In diesen letzten drei Vorlesungen wird zunächst die Hermitesche Normalform einer ganzzahligen Matrix sowie Anwendungen besprochen. Im weiteren wird in groben Zügen der LLL-Algorithmus diskutiert. Die Inhalte sind im wesentlichen dem Buch von Henri Cohen, A course in computational algebraic number theory, entnommen. Hier finden Sie auch weitere Algorithmen für endlich erzeugte $\mathbb{Z}$-Moduln.