Lineare Algebra 2

Anton Deitmar

Sommersemester 2014

Inhaltsverzeichnis

1 Normierte Räume

1.1 Polynome in mehreren Variablen

Sei K ein Körper und $k \in \mathbb{N}$. Ein *Polynom* in den Variablen $X_1, \ldots, X_k$ über dem Körper K ist ein formaler Ausdruck der Form

$$\sum_{j_1=1}^{N} \cdots \sum_{j_k=1}^{N} c_{j_1,\ldots,j_k} X_1^{j_1} \cdots X_k^{j_k}$$

mit Koeffizienten $c_{j_1,\ldots,j_k} \in K$

Beispiele 1.1.1.

- In zwei Variablen: $X^4 + X^3Y + Y^7$.
- Die Determinante ist ein Polynom in n^2-Variablen

$$\det\left((X_{i,j})_{1\le i,j\le n}\right) = \sum_{\sigma\in \mathrm{Per}(n)} \mathrm{sign}(\sigma) X_{1,\sigma(1)} \cdots X_{n,\sigma(n)}.$$

Schreibweise: Sei $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ und $\mathbb{N}_0^k = \mathbb{N}_0 \times \cdots \times \mathbb{N}_0$ (k-mal). Man schreibt ein Polynom in den Variablen $X_1, \ldots, X_k$ in der Form

$$\sum_{\alpha\in\mathbb{N}_0^k} c_\alpha X^\alpha,$$

wobei man abkürzend schreibt

$$X^\alpha = X_1^{\alpha_1} \cdots X_k^{\alpha_k}.$$

Hierbei ist der Koeffizient c_α nur für endlich viele α von Null verschieden. Wie im Fall einer Variablen, kann man die Menge der Polynome in $X_1, \ldots, X_k$ mit der Menge aller Abbildungen

$$\begin{aligned} \mathbb{N}_0^k &\to K, \\ \alpha &\mapsto c_\alpha \end{aligned}$$

identifizieren, die nur für endlich viele α ungleich Null sind.

Die Menge aller Polynome über K bilden einen K-Vektorraum mit der folgenden

Addition und Skalarmultiplikation:

$$\sum_{\alpha\in\mathbb{N}_0^k} c_\alpha X^\alpha + \sum_{\alpha\in\mathbb{N}_0^k} d_\alpha X^\alpha = \sum_{\alpha\in\mathbb{N}_0^k} (c_\alpha + d_\alpha) X^\alpha,$$

$$\lambda\left(\sum_{\alpha\in\mathbb{N}_0^k} c_\alpha X^\alpha\right) = \sum_{\alpha\in\mathbb{N}_0^k} \lambda c_\alpha X^\alpha.$$

Ferner kann man zwei Polynome multiplizieren:

$$\left(\sum_{\alpha\in\mathbb{N}_0^k} c_\alpha X^\alpha\right)\left(\sum_{\beta\in\mathbb{N}_0^k} d_\beta X^\beta\right) = \sum_{\alpha,\beta\in\mathbb{N}_0^k} c_\alpha d_\beta X^{\alpha+\beta} = \sum_{\gamma\in\mathbb{N}_0^k}\left(\sum_{\alpha+\beta=\gamma} c_\alpha d_\beta\right) X^\gamma,$$

wobei Elemente von $\mathbb{N}_0^k$ komponentenweise addiert werden

$$(a_1, \ldots, \alpha_k) + (\beta_1, \ldots, \beta_k) = (\alpha_1 + \beta_1, \ldots, \alpha_k + \beta_k).$$

Man macht sich klar, dass die in dem Produkt auftretende Summe $\sum_{\alpha+\beta=\gamma} c_\alpha d_\beta$ stets endlich ist.

Beispiele 1.1.2.

- $(x + y)^2 = x^2 + 2xy + y^2$,
- $(x + y + z)^2 = x^2 + y^2 + z^2 + 2(xy + xz + yz)$.

Man schreibt $K[X_1, \ldots, X_k]$ für die Menge aller Polynome in den Variablen $X_1, \ldots, X_k$ und Koeffizienten in K. Jedes $f \in K[X_1, \ldots, X_k]$ stiftet eine *polynomiale Abbildung*

$$\tilde{f} : K^k \to K$$

durch einsetzen.

Proposition 1.1.3. *Hat der Körper K unendlich viele Elemente und ist $f \in K[X_1, \ldots, X_k]$ ein Polynom, dessen polynomiale Abbildung $\tilde{f}$ die Nullabbildung ist. Dann ist f das Nullpolynom. Damit ist die lineare Abbildung $f \mapsto \tilde{f}$ injektiv.*

Proof. Die Abbildung $K[X_1, \ldots, X_k] \to \mathrm{Abb}(K^k, K)$, $f \mapsto \tilde{f}$ ist offensichtlich linear. In einer Variablen kennen wir die Proposition schon. Damit ist der Induktionsanfang $k = 1$ gegeben. Nun zu $k \to k + 1$. Sei also $f \in K[X_1, \ldots, X_k, X_{k+1}]$ so dass $\tilde{f} : K^{k+1} \to K$ die Nullabbildung ist. Wir ordnen die Summanden des Polynoms f nach den

Potenzen von X_{k+1}:

$$f(X) = \sum_{j=0}^{N} f_j(X_1, \ldots, X_k) X_{k+1}^j,$$

wobei $f_0, \ldots, f_N$ Polynome in den Variablen $X_1, \ldots, X_k$ sind. Für jedes gegebene $\alpha = (\alpha_1, \ldots, \alpha_k) \in K^k$ ist dann

$$x \mapsto f(\alpha, x) = \sum_{j=0}^{N} f_j(\alpha) x^j$$

die Nullabbildung. Nach der Aussage für eine Variable ist daher jeder Koeffizient $f_j(\alpha)$ gleich Null und da dies für jedes α gilt ist folglich für gegebenes j die Abbildung

$$\alpha \mapsto f_j(\alpha)$$

die Nullabbildung auf K^k. Nach Induktionsvoraussetzung sind die Polynome $f_0, f_1, \ldots, f_N$ alle gleich Null, also ist f gleich Null. □

1.2 Komplexifizierung

Satz 1.2.1. *Jeder komplexe Vektorraum W ist auch ein reeller Vektorraum. Es gilt*

$$\dim_{\mathbb{R}} W = 2 \dim_{\mathbb{C}} W.$$

Ist V ein reeller Vektorraum, so kann man $V_{\mathbb{C}} = V \times V$ zu einem komplexen Vektorraum machen, indem man setzt:

$$(a + bi)(u, w) = (au - bw, aw + bu).$$

Man nennt $V_{\mathbb{C}}$ die Komplexifizierung *von V. Es gilt*

$$\dim_{\mathbb{R}} V = \dim_{\mathbb{C}} V_{\mathbb{C}}.$$

Man identifiziert V mit mit $V \times \{0\} \subset V_{\mathbb{C}}$, dann ist $\{0\} \times V = iV$ und $V_{\mathbb{C}} = V \oplus iV$. Dann ist $(v, w) = v + iw$. Jede $\mathbb{R}$-lineare Abbildung $T : V \to V$ lässt sich in eindeutiger Weise zu

einer $\mathbb{C}$-linearen $T_{\mathbb{C}} : V_{\mathbb{C}} \to V_{\mathbb{C}}$ fortsetzen, indem man definiert

$$T_{\mathbb{C}}(v + iw) = Tv + iTw.$$

Die Abbildung $T \mapsto T_{\mathbb{C}}$ ist eine Injektive Abbildung

$$\mathrm{Lin}_{\mathbb{R}}(V, V) \to \mathrm{Lin}_{\mathbb{C}}(V_{\mathbb{C}}, V_{\mathbb{C}}).$$

Das Bild rechts besteht aus den linearen Abbildungen $S : V_{\mathbb{C}} \to V_{\mathbb{C}}$ mit $S(V) \subset V$.

Beweis. Sei W ein komplexer Vektorraum und sei $v_1, \ldots, v_n$ eine Basis (über $\mathbb{C}$) von W. Wir behaupten, dass dann

$$v_1, iv_1, \ldots, v_n, iv_n$$

eine Basis von W als $\mathbb{R}$-Vektorraum ist.

Lineare Unabhängigkeit. Sei

$$\lambda_1 v_1 + \mu_1 iv_1 + \cdots + \lambda_n v_n + \mu_n iv_n = 0,$$

also

$$(\lambda_1 + i\mu_1)v_1 + \cdots + (\lambda_n + i\mu_n)v_n = 0.$$

Da die Vektoren $v_1, \ldots, v_n$ über $\mathbb{C}$ linear unabhängig sind, folgt

$$(\lambda_1 + i\mu_1) = \cdots = (\lambda_n + i\mu_1) = 0$$

und aus dem Vergleich von Real- und Imaginärteil sehen wir, dass

$$\lambda_1 = \cdots = \lambda_n = \mu_1 = \cdots = \mu_n = 0$$

ist.

Erzeugendensystem. Sei $w \in W$, dann gibt es $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$, so dass $w = \alpha_1 v_1 + \cdots + \alpha_n v_n$. Schreibe $\alpha_j = \lambda_j + i\mu_j$ mit $\lambda_j, \mu_j \in \mathbb{R}$, so folgt

$$w = \lambda_1 v_1 + \mu_1 iv_1 + \cdots + \lambda_n v_n + \mu_n iv_n.$$

Damit ist die Basis-Eigenschaft gezeigt und die Dimensionsaussage folgt.

Zur Komplexifizierung: Man rechnet leicht nach, dass $V_{\mathbb{C}}$ ein $\mathbb{C}$-Vektorraum ist. Sei nun $v_1, \dots, v_n$ eine $\mathbb{R}$-Basis von V. Wir behaupten, dass sie auch eine $\mathbb{C}$-Basis ist. Für die lineare Unabhängigkeit sei

$$0 = \alpha_1 v_1 + \cdots + \alpha_n v_n = \lambda_1 v_1 + \mu_1 i v_1 + \cdots + \lambda_n v_n + \mu_n i v_n,$$

wobei $\lambda_j = \mathrm{Re}(\alpha_j)$ und $\mu_j = \mathrm{Im}(\alpha_j)$. Durch Vergleich von Real- und Imaginärteil folgt

$$\lambda_1 v_1 + \cdots + \lambda_n v_n = \mu_1 v_1 + \cdots + \mu_n v_n = 0,$$

woraus dann $\lambda_j = \mu_j = 0$, also $\alpha_j = 0$ folgt. Der Rest ist klar. □

Beispiele 1.2.2.

- Die Komplexifizierung von $\mathbb{R}^n$ ist $\mathbb{C}^n = \mathbb{R}^n \oplus i\mathbb{R}^n$.
- Fasst man umgekehrt $\mathbb{C} \cong \mathbb{R}^2$ als reellen Vektorraum auf, dann ist $\mathbb{C}^n \cong \mathbb{R}^{2n}$.

Proposition 1.2.3. (a) *Ist W ein komplexer Vektorraum, dann ist*

$$\begin{aligned} J : W &\to W \\ w &\mapsto iw \end{aligned}$$

eine $\mathbb{R}$-lineare Abbildung. Eine beliebige $\mathbb{R}$-lineare Abbildung $T : W \to W$ ist genau dann $\mathbb{C}$-linear, wenn sie mit J vertauscht, wenn also gilt $JT = TJ$.

(b) *Sei V ein endlich-dimensionaler $\mathbb{R}$-Vektorraum und sei $J : V \to V$ eine $\mathbb{R}$-lineare Abbildung mit der Eigenschaft $J^2 = -1$. Dann ist die Dimension von V gerade und V wird durch die Vorschrift*

$$(a + bi)v = av + bJ(v)$$

ein $\mathbb{C}$-Vektorraum. Man nennt eine solche Abbildung J auch eine komplexe Struktur.

Beweis. (a) Die $\mathbb{R}$-Linearität von J ist klar, diese Abbildung ist ja sogar $\mathbb{C}$-linear. Ist $T : W \to W$ eine $\mathbb{C}$-lineare Abbildung, so gilt für $w \in W$,

$$JT(w) = iT(w) = T(iw) = TJ(w).$$

Sei umgekehrt $T : W \to W$ eine $\mathbb{R}$-lineare Abbildung, die mit J vertauscht und sei $\lambda = a + bi \in \mathbb{C}$. Dann gilt für $w \in W$

$$T(\lambda w) = T(aw + biw) = T(aw + bJ(w)) = aT(w) + bJT(w) = aT(w) + biT(w) = \lambda T(w),$$

also ist T komplex-linear.

(b) Sei $J : V \to V$ mit $J^2 = -1$. Dann ist das Minimalpolynom von J gleich $x^2 + 1 = (x - i)(x + i)$. Daher ist das charakteristische Polynom gleich $(x - i)^m(x + i)^n$. Dieses Polynom ist aber nur dann reell, wenn $m = n$, so dass dim $V = 2n$ gerade ist. Man definiert nun

$$(a + bi) \cdot v = av + bJ(v).$$

Dies macht V zu einem $\mathbb{C}$-Vektorraum, wie man leicht nachrechnet, der einzig interessante Teil ist $(\lambda\mu)v = \lambda(\mu v)$ für $\lambda = a + bi$ und $\mu = c + di \in \mathbb{C}$:

$$\begin{aligned}
\lambda(\mu v) &= (a + bi)((c + di)v) \\
&= (a + bJ)((c + dJ)(v)) \\
&= a(c + dJ)(v) + bJ((c + dJ)(v)) \\
&= acv + adJ(v) + bcJ(v) - bdv \\
&= (ac - bd)v + (ad + bc)J(v) \\
&= (ac - bd)v + (ad + bc)iv \\
&= ((ac - bd) + (ad + bc)i)v = (\lambda\mu)v.
\end{aligned}$$

□

1.3 Konvexität

Definition 1.3.1. Eine Menge $K \subset \mathbb{R}^n$ heisst *konvex*, falls für je zwei $x, y \in K$ die Verbindungslinie zwischen ihnen auch in K liegt, wenn also gilt

$$(1 - t)x + ty \in K \quad \forall_{t \in [0,1]}.$$

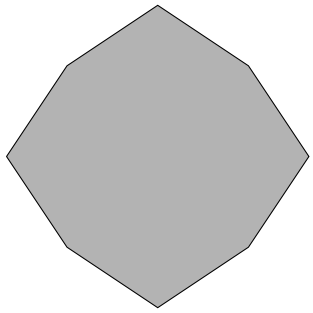


Abbildung 1: konvex

Beispiele 1.3.2.

- Jeder Untervektorraum von $\mathbb{R}^n$ ist konvex.

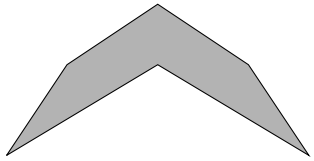


Abbildung 2: nicht konvex

- Sei $\alpha : \mathbb{R}^n \to \mathbb{R}$ eine lineare Abbildung und sei $T \in \mathbb{R}$. Dann ist die Menge $H_\alpha(T) = \{x \in \mathbb{R}^n : \alpha(x) \leq T\}$ eine konvexe Menge, genannt der *Halbraum*, gegeben durch α und T. Diese Menge ist konvex.

  Beweis. Seien $x, y \in H_\alpha(T)$, dann gilt für jedes $t \in [0,1]$,

  $$\alpha((1-t)x + ty) = (1-t)\alpha(x) + t\alpha(y) \leq (1-t)T + tT = T. \qquad \square$$

- Sei $S \subset \mathbb{R}^n$ irgendeine Teilmenge von $\mathbb{R}^n$, dann ist die Menge

  $$\operatorname{conv}(S) = \bigcap_{\substack{K \supset S \\ K \text{ konvex}}} K$$

  eine konvexe Teilmenge von $\mathbb{R}^n$. Es ist die kleinste konvexe Teilmenge, die S enthält und wird deshalb die *konvexe Hülle* von S genannt.

- Sei$S \subset \mathbb{R}^n$, dann lässt sich die konvexe Hülle auch beschreiben als

  $$\operatorname{conv}(S) = \left\{ \sum_{j=1}^{k} \lambda_j v_j : 0 \leq \lambda_j,\ \sum_{j=1}^{k} \lambda_j = 1,\ v_1, \ldots, v_k \in S \right\}.$$

  Beweis. Sei K die konvexe Hülle von S und sei R die rechte Seite. Wir zeigen, dass $S \subset R$ und R ist konvex. Das erste ist klar, für das zweite seien $a, b \in R$, also etwa

  $$a = \sum_{j=1}^{k} \lambda_j v_j, \qquad b = \sum_{j=k+1}^{s} \lambda_j v_j$$

  mit $v_j \in S$ und $\sum_{j=1}^{k} \lambda_j = 1 = \sum_{j=k+1}^{s} \lambda_j$. Für $0 \leq t \leq 1$ gilt dann

  $$(1-t)a + tb = (1-t) \sum_{j=1}^{k} \lambda_j v_j + t \sum_{j=k+1}^{s} \lambda_j v_j.$$

Sei $\mu_j = (1-t)\lambda_j$ falls $j \leq k$ und $\mu_j = t\lambda_j$ sonst. Dann gilt

$$\sum_{j=1}^{s} \mu_j = (1-t) \underbrace{\sum_{j=1}^{k} \lambda_j}_{=1} + t \underbrace{\sum_{j=k+1}^{s} \lambda_j}_{=1} = 1.$$

Damit liegt $(1-t)a + tb = \sum_{j=1}^{s} \lambda_j v_j$ in R, also ist R konvex. Nach Definition von K folgt $K \subset R$. Umgekehrt zeigen wir per Induktion nach k, dass jeder Vektor der Form $\sum_{j=1}^{k} \lambda_j v_j$ mit $v_j \in S$, $\lambda_j \geq 0$ und $\sum_{j=1}^{k} \lambda_j = 1$, bereits in K liegt. Der Fall $k = 1$ ist klar, da $S \subset K$ Sei also der Fall k bereits gezeigt und sei $a = \sum_{j=1}^{k+1} \lambda_j v_j$ mit $v_j \in S$ und $\lambda_j \geq 0$ mit $\sum_j \lambda_j = 1$. Sei $t = \lambda_{k+1}$, dann folgt $0 \leq t \leq 1$. Ist $t = 1$, dann folgt $\lambda_j = 0$ für jedes $j = 1, \ldots, k$ und die Behauptung ist klar. Sei also $t < 1$. Dann ist $\sum_{j=1}^{k} \frac{\lambda_j}{1-t} = 1$ und deshalb ist der Vektor $w = \sum_{j=1}^{k} \frac{\lambda_j}{1-t} v_j$ nach Induktionsvoraussetzung in K. Da K konvex ist, folgt

$$\sum_{j=1}^{k+1} \lambda_j v_j = (1-t)w + tv_{k+1} \in K. \qquad \square$$

1.4 Normen

Unter einer *Norm* auf einem reellen oder komplexen Vektorraum V verstehen wir eine Abbildung $\|.\| : V \to \mathbb{R}$ so dass

- $\|v\| \geq 0$ und $\|v\| = 0 \Leftrightarrow v = 0$ — Definitheit
- $\|\lambda v\| = |\lambda| \, \|v\|$ — Multiplikativität
- $\|v + w\| \leq \|v\| + \|w\|$ — Dreiecksungleichung

Lemma 1.4.1 (Umgekehrte Dreiecksungleichung)**.** *Für jede Norm gilt*

$$\big| \|v\| - \|w\| \big| \leq \|v - w\| .$$

Proof. Aus der Dreiecksungleichung folgt

$$\|v\| = \|v - w + w\| \leq \|v - w\| + \|w\| ,$$

also $\|v\| - \|w\| \leq \|v - w\|$. Durch Vertauschung der Rollen von v und w wird daraus $\|w\| - \|v\| \leq \|v - w\|$, was zusammen die Behauptung liefert. $\square$

Beispiele 1.4.2. • Die *Maximumsnorm* auf $\mathbb{R}^n$, gegeben durch

$$\|x\|_\infty = \max_{j=1}^{n} |x_j|$$

ist eine Norm, denn für $x \in \mathbb{R}^n$ gilt

$$\begin{aligned} \|x\|_\infty = 0 &\Leftrightarrow \max_{j=1}^{n} |x_j| = 0 \\ &\Leftrightarrow |x_1| = \cdots = |x_n| = 0 \\ &\Leftrightarrow x_1 = \cdots = x_n = 0 \\ &\Leftrightarrow x = 0. \end{aligned}$$

Ferner ist für $\lambda \in \mathbb{R}$,

$$\|\lambda x\|_\infty = \max_{j=1}^{n} |\lambda x_j| = |\lambda| \max_{j=1}^{n} |x_j| = |\lambda| \, \|x\|_\infty .$$

Und schliesslich

$$\left\|x + y\right\|_\infty = \max_{j=1}^{n} |x_j + y_j| \leq \max_{j=1}^{n} |x_j| + |y_j| \leq \max_{j=1}^{n} |x_j| + \max_{j=1}^{n} |y_j| = \|x\|_\infty + \left\|y\right\|_\infty .$$

• Die *Summennorm* auf $\mathbb{R}^n$, gegeben durch

$$\|x\|_1 = |x_1| + \cdots + |x_n|$$

ist ebenfalls eine Norm, denn

$$\begin{aligned} \|x\|_1 = 0 &\Leftrightarrow |x_1| + |x_2| + \cdots + |x_n| = 0 \\ &\Leftrightarrow |x_1| = \cdots = |x_n| = 0 \\ &\Leftrightarrow x_1 = \cdots = x_n = 0 \\ &\Leftrightarrow x = 0. \end{aligned}$$

Ferner ist für $\lambda \in \mathbb{R}$,

$$\|\lambda x\|_1 = |\lambda x_1| + \cdots + |\lambda x_n| = |\lambda| \, (|x_1| + \cdots + |x_n|) = |\lambda| \, \|x\|_1 .$$

Und schliesslich

$$\left\|x + y\right\|_1 = |x_1 + y_1| + \cdots + |x_n + y_n| \leq |x_1| + |y_1| + \cdots + |x_n| + |y_n| = \|x\|_1 + \left\|y\right\|_1 .$$

- die *euklidische Norm*
$$\|x\|_2 = \sqrt{x_1^2 + \cdots + x_n^2}.$$
Die Normeigenschaft wird in Abschnitt 2.4 gezeigt.

Definition 1.4.3. Sei $\|.\|$ eine beliebige Norm auf $\mathbb{R}^n$. Setze dann
$$B = B(\|.\|) = \{x \in \mathbb{R}^n : \|x\| \leq 1\}.$$
Dies ist der *abgeschlossene Einheitsball* der Norm.

Lemma 1.4.4. *Sei $B \subset \mathbb{R}^n$ der abgeschlossene Einheitsball einer Norm $\|.\|$. Dann gilt*

(a) *B ist konvex,*

(b) *für jedes $x \in \mathbb{R}^n \neq 0$ ist*
$$\{\lambda \in \mathbb{R} : \lambda x \in B\}$$
ein Intervall der Form $[-a, a]$, $a > 0$.

In (b) ist der Wert $a = \|x\|^{-1}$.

Beweis. Klar. □

Lemma 1.4.5. *Ist $B \subset \mathbb{R}^n$ eine Teilmenge mit den Eigenschaften (a) und (b) aus dem letzten Lemma, dann gibt es genau eine Norm, so dass B der offene Einheitsball ist.*

Beweis. Sei B mit den Eigenschaften (a) und (b) gegeben. Für $x \in \mathbb{R}^n$ definiere
$$N(x) = \begin{cases} a^{-1} & x \neq 0 \text{ mit } a \text{ aus (b)}, \\ 0 & x = 0. \end{cases}$$
Es folgt dann
$$B = \{x \in \mathbb{R}^n : N(x) \leq 1\}.$$
und für jedes $x \neq 0$ in $\mathbb{R}^n$ gilt
$$B \cap \mathbb{R}x = (-N(x)^{-1}, N(x)^{-1})x.$$
Wir behaupten, dass N eine Norm ist. Zunächst ist $N(x) \geq 0$ und $N(x) = 0 \Leftrightarrow x = 0$, also ist N positiv definit. Sei nun $\lambda \in \mathbb{R}$. Ist $\lambda = 0$, so ist $\lambda x = 0$ und damit

$N(\lambda x) = 0 = |\lambda| N(x)$. Dieselbe Aussage folgt, wenn $x = 0$. Sei nun λ und x beide ungleich Null. Dann ist $(-N(x)^{-1}, N(x)^{-1})x = B \cap \mathbb{R}x$ und also

$$\begin{aligned}(-N(\lambda x)^{-1}, N(\lambda x)^{-1})\lambda x &= \mathbb{R}\lambda x \cap B \\ &= \mathbb{R}x \cap B \\ &= (-N(x)^{-1}, N(x)^{-1})x \\ &= (-|\lambda|^{-1}N(x)^{-1}, |\lambda|^{-1}N(x)^{-1})\lambda x\end{aligned}$$

und damit $N(\lambda x) = |\lambda| N(x)$. Zum Schluss die Dreiecksungleichung. Seien $x, y \in \mathbb{R}$, wobei wir beide als $\neq 0$ annehmen können. Seien $\alpha = N(x)^{-1}$ und $\beta = N(y)^{-1}$, dann gilt $N(\alpha x) = 1 = N(\beta y)$, also $\alpha x, \beta y \in B$. Dann ist wegen der Konvexität für jedes $0 \leq t \leq 1$ auch $(1-t)\alpha x + t\beta y \in B$, also $N((1-t)\alpha x + t\beta y) \leq 1$. Sei $t = \frac{\alpha}{\alpha+\beta}$, dann folgt $(1-t)\alpha = t\beta = \frac{\alpha\beta}{\alpha+\beta}$. Also ist

$$N(x+y) = \frac{\alpha+\beta}{\alpha\beta} N\left(\frac{\alpha\beta}{\alpha+\beta}(x+y)\right) \leq \frac{\alpha+\beta}{\alpha\beta} = \frac{N(x)^{-1} + N(y)^{-1}}{N(x)^{-1}N(y)^{-1}} = N(x) + N(y).$$

Die Eindeutigkeit der Norm ist klar. □

Beispiele für Einheitsbälle von Normen $\|.\|$ auf dem $\mathbb{R}^2$, die $\|e_1\| = \|e_2\| = 1$ erfüllen.

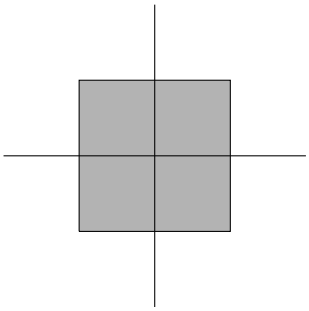


Abbildung 3: Einheitsball der Maximumsnorm $\|.\|_\infty$

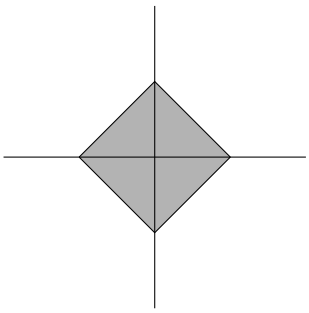


Abbildung 4: Einheitsball der Summennorm $\|.\|_1$

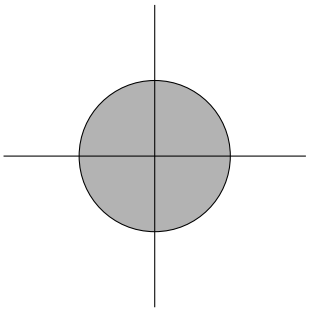


Abbildung 5: Einheitsball der euklidischen $\|.\|_2$

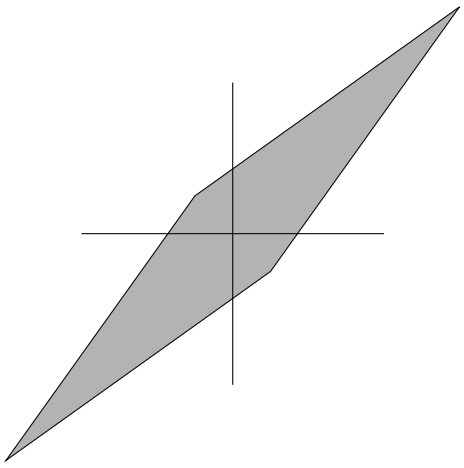


Abbildung 6: Einheitsball einer exotischen Norm

2 Bilinearformen und Skalarprodukte

2.1 Bilinearformen

Definition 2.1.1. Sei V ein endlich-dimensionaler K-Vektorraum. Eine Abbildung

$$b : V \times V \to K$$

heißt *Bilinearform*, falls $b(\cdot, v)$ und $b(v, \cdot)$ für jedes $v \in V$ linear sind. Genauer heißt das

- $b(\lambda v + \mu w, u) = \lambda b(v, u) + \mu b(w, u)$ und
- $b(v, \lambda w + \mu u) = \lambda b(v, w) + \mu b(v, u)$

für alle $v, w \in V$ und alle $\lambda, \mu \in K$.

Beispiele 2.1.2.

- Die Nullabbildung ist eine Bilinearform.
- Die Abbildung $K^n \times K^n \to K$;

  $$(v, w) \mapsto v^t w = v_1 w_1 + v_2 w_2 + \cdots + v_n w_n$$

  ist eine Bilinearform, die sogenannte *kanonische Bilinearform* auf K^n.

  Beweis. Für $\lambda, \mu \in K$ und $v, u, w \in K^n$ rechnen wir

  $$(\lambda v + \mu u)^t w = (\lambda v^t + \mu u^t) w = \lambda v^t w + \mu u^t w$$

  nach den Rechenregeln der Matrizenmultiplikation. Die Linearität im zweiten Argument folgt entweder ebenso oder (in diesem Fall) per Symmetrie:

  $$K \ni v^t w = (v^t w)^t = w^t (v^t)^t = w^t v,$$

  so dass die Linearität im ersten Argument auch die Linearität im zweiten zur Folge hat. □

- Die Abbildung $\mathrm{M}_n(K) \times \mathrm{M}_n(K) \to K$; $(A, B) \mapsto \operatorname{tr}(AB)$ ist eine Bilinearform.

  Beweis. Für $A, B, C \in \mathrm{M}_n(K)$ und $\lambda, \mu \in K$ rechnen wir

  $$\operatorname{tr}((\lambda A + \mu C)B) = \operatorname{tr}(\lambda AB + \mu CB) = \lambda \operatorname{tr}(AB) + \mu \operatorname{tr}(CB).$$

Die Linearität im zweiten Argument folgt ebenso oder wieder durch Symmetrie. □

- Sei $V = K^2$ und $b : V \times V \to K$ gegeben durch

$$b\left(\begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} z \\ w \end{pmatrix}\right) = xw.$$

Dann ist b eine Bilinearform, die nicht symmetrisch ist.

Beweis. Für $s, t, x, y, z, w \in K$ sowie $\lambda.\mu \in K$ rechnen wir

$$\begin{aligned} b\left(\lambda\begin{pmatrix} s \\ t \end{pmatrix} + \mu\begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} z \\ w \end{pmatrix}\right) &= b\left(\begin{pmatrix} \lambda s + \mu x \\ \lambda t + \mu y \end{pmatrix}, \begin{pmatrix} z \\ w \end{pmatrix}\right) \\ &= (\lambda s + \mu x)w = \lambda sw + \mu xw \\ &= \lambda b\left(\begin{pmatrix} s \\ t \end{pmatrix}, \begin{pmatrix} z \\ w \end{pmatrix}\right) + \mu b\left(\begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} z \\ w \end{pmatrix}\right). \end{aligned}$$

Die Linearität im zweiten Argument geht ebenso. Die mangelnde Symmetrie sieht man schnell durch ein Beispiel

$$b\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = 1 \neq 0 = b\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right).$$ □

- Ist S eine Menge und ist $V = \mathrm{Abb}(S, K)$ der Vektorraum aller Abbildungen von S nach K, ist ferner $s_0 \in S$ ein Punkt, dann ist

$$\begin{aligned} b : V \times V &\to K \\ (f, g) &\mapsto f(s_0)g(s_0) \end{aligned}$$

eine Bilinearform.

Beweis. Seien $f, g, h \in V$ und $\lambda, \mu \in K$. Dann gilt

$$\begin{aligned} b(\lambda f + \mu h, g) &= (\lambda f + \mu h)(s_0)g(s_0) \\ &= (\lambda f(s_0) + \mu h(s_0))g(s_0) \\ &= \lambda f(s_0)g(s_0) + \mu h(s_0)g(s_0) \\ &= \lambda b(f, g) + \mu b(h, g). \end{aligned}$$

Die Linearität im zweiten Argument geht ebenso. □

Definition 2.1.3. Sei $\dim V < \infty$ und $b : V \times V \to K$ eine Bilinearform. Dann erhält man eine Abbildung $R : V \to V^*$, durch

$$R(v)(w) = b(w, v).$$

(Die Vertauschung der Reihenfolge ist beabsichtigt.)

Proposition 2.1.4. *Die Menge* $\mathrm{Bil}(V)$ *aller Bilinearformen ist ein Untervektorraum von* $\mathrm{Abb}(V \times V, K)$. *Sei b eine Bilinearform auf V. Dann ist die Abbildung*

$$R_b : v \mapsto b(., v)$$

eine lineare Abbildung $V \to V^*$ *von V in den Dualraum von V. Sei andersherum* $R : V \to V^*$ *eine lineare Abbildung, dann ist*

$$b_R(v, w) = \phi(w)(v)$$

eine Bilinearform. Wir erhalten eine lineare Bijektion

$$\mathrm{Bil}(V) \xrightarrow{\cong} \mathrm{Lin}(V, V^*)$$

von dem Vektorraum aller Bilinearformen auf V zum Vektorraum aller linearen Abbildungen $V \to V^*$.

Beweis. Um zu sehen, dass $\mathrm{Bil}(v)$ ein Untervektorraum ist, müssen wir uns überzeugen, dass mit zwei Bilinearformen b, b' deren Summe $b + b'$ und λb für $\lambda \in K$ wieder bilinear sind, was leicht einzusehen ist.

Die Abbildungen $b \mapsto R_b$ und $R \mapsto b_R$ sind linear und invers zueinander, denn es gilt

$$b_{R_b}(v, w) = R_b(w)(v) = b(v, w)$$

und

$$R_{b_R}(v)(w) = b_R(w, v) = R(v)(w).$$ □

Lemma 2.1.5. *Sei V endlich-dimensional und sei* $b : V \times V \to K$ *eine Bilinearform. Dann sind äquivalent:*

(a) *Zu jedem* $v \in V \setminus \{0\}$ *gibt es ein* $w \in V$ *mit* $b(v, w) \neq 0$.

(b) *zu jedem $w \in V \setminus \{0\}$ gibt es ein $v \in V$ mit $b(v,w) \neq 0$.*

(c) *R ist ein Isomorphismus.*

Ist dies erfüllt, so heißt b nicht ausgeartet.

Beweis. (b)⇔(c): Die Bedingung (b) ist äquivalent zur Injektivität von R. Da $\dim V^* = \dim V$, ist dies äquivalent dazu, dass R ein Isomorphismus ist.

(a)⇔(c) Sei $L : V \to V^*$ gegeben durch $L(v)(w) = b(v,w)$. Dann ist (a) äquivalent zur Injektivität von L. Wir dualisieren R und behaupten, dass L gleich der Komposition $V \xrightarrow{\delta} V^{**} \xrightarrow{R^*} V^*$ ist. Seien hierzu $v, w \in V$, dann gilt $R^*(\delta(v))(w) = \delta_v(R(w)) = R(w)(v) = b(v,w) = L(v)(w)$. Damit ist die Injektivität von L äquivalent zur Surjektivität von R. □

Beispiele 2.1.6.

- Die kanonische Bilinearform auf K^n ist nicht ausgeartet, denn man sieht leicht, dass R injektiv ist.
- Die Spurform $\mathrm{M}_n(K) \times \mathrm{M}_n(K) \to K$; $(A,B) \mapsto \mathrm{tr}(AB)$ ist nicht ausgeartet, denn ist $B \neq 0$ eine Matrix, so kann man durch Zeilentransformationen B in eine Matrix B' transformieren, so dass $\mathrm{Spur}(B') \neq 0$ ist. Dann existiert eine Matrix $S \in \mathrm{M}_n(K)$ so dass $B' = SB$, also $\mathrm{tr}(SB) \neq 0$.
- Sei $V = \mathrm{Abb}(S,K)$ und $s_0 \in S$, dann ist die Punktauswertungsform

$$\begin{aligned} b : V \times V &\to K \\ (f,g) &\mapsto f(s_0)g(s_0) \end{aligned}$$

  genau dann ausgeartet, wenn S mindestens zwei Elemente hat. Ist dann nämlich $s_1 \neq s_0$ ein weiteres Element, dann gilt für die Abbildung

$$f(x) = \begin{cases} 1 & x = s_1, \\ 0 & x \neq s_1, \end{cases}$$

  dass $b(f,g) = 0$ für jedes $g \in V$ aber dennoch ist $f \neq 0$.

Definition 2.1.7. Sei $b : V \times V \to K$ eine Bilinearform und sei $\mathcal{B} = (v_1, \ldots, v_n)$ eine Basis von V. Die *Matrix von b* bezüglich der Basis $\mathcal{B}$ ist die Matrix $B = \mathcal{M}_{\mathcal{B}}(b) \in \mathrm{M}_n(K)$ gegeben durch

$$B_{i,j} = b(v_i, v_j).$$

Beispiel 2.1.8. Sei $n \in \mathbb{N}$ und sei V der reelle Vektorraum aller Polynome $f \in \mathbb{R}[x]$ vom Grad $\leq n$. Sei b die Bilinearform gegeben durch

$$b(f,g) = \int_0^1 f(x)g(x)\,dx.$$

Sei $\mathcal{B}$ die Basis $1, x, x^2, \ldots, x^n$. Schreibe $v_j = d^{j-1}$ für $j = 1, \ldots, n+1$. Dann gilt

$$b(v_i, v_j) = \int_0^1 x^{i-1+j-1}\,dx = \frac{1}{i+j-1}.$$

Also ist die zugehörige Matrix gleich

$$\begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{3} & \cdots & \frac{1}{n+1} \\ \frac{1}{2} & \frac{1}{3} & & & \frac{1}{n+2} \\ \frac{1}{3} & & \ddots & & \frac{1}{n+3} \\ \vdots & & & & \vdots \\ \frac{1}{n+1} & \frac{1}{n+2} & \frac{1}{n+3} & \cdots & \frac{1}{2n+1} \end{pmatrix}.$$

Lemma 2.1.9. *Sei* $\dim V = n$ *und sei* $\mathrm{Bil}(V)$ *die Menge aller Bilinearformen auf* V*. Sei* $\mathcal{B}$ *eine Basis von* V*, dann ist die Abbildung* $b \mapsto \mathcal{M}_{\mathcal{B}}(b)$ *ein linearer Isomorphismus* $\mathrm{Bil}(V) \xrightarrow{\cong} \mathrm{M}_n(K)$*. Insbesondere ist* $\dim \mathrm{Bil}(V) = n^2$*.*

Beweis. Für die Injektivität stellen wir fest, dass die Matrix B die Form b eindeutig festlegt, denn

$$b\left(\sum_{i=1}^n \lambda_i v_i, \sum_{j=1}^n \mu_j v_j\right) = \sum_{i,j} \lambda_i \mu_j b(v_i, v_j) = \sum_{i,j} \lambda_i \mu_j B_{i,j} = \lambda^t B \mu. \qquad (*)$$

Für das letzte Gleichheitszeichen haben wir λ und μ als Spaltenvektoren in K^n aufgefasst. Andererseits kann man (*) auch rückwärts lesen, nämlich indem es für eine gegebene Matrix B eine Bilinearform b definiert, was dann die Surjektivität liefert. □

Beispiel 2.1.10. Im Spezialfall $V = K^n$ bedeutet das Lemma, dass jede gegebene Bilinearform b in der Form

$$b(x,y) = x^t B y$$

für eine eindeutig bestimmte Matrix $B \in \mathrm{M}_n(K)$ geschrieben werden kann.

Satz 2.1.11. *Sei b eine Bilinearform auf V, $\mathcal{B}$ eine Basis, $\mathcal{B}^*$ die duale Basis von V^* und $B = \mathcal{M}_{\mathcal{B}}(b) \in \mathrm{M}_n(K)$.*

(a) *Die Matrix B stellt die lineare Abbildung $R : V \to V^*$ aus Definition 2.1.3 in den Basen $\mathcal{B}$ und $\mathcal{B}^*$ dar, also*

$$B = \mathcal{M}_{\mathcal{B},\mathcal{B}^*}(R).$$

(b) *Es gilt*

$$b \text{ nicht ausgeartet} \Leftrightarrow B \text{ invertierbar.}$$

Beweis. Sei $\mathcal{B} = (v_1, \ldots, v_n)$ und sei $A = \mathcal{M}^{\mathcal{B}}_{\mathcal{B}^*}(R)$. Das heißt $R(v_j) = \sum_{k=1}^n A_{k,j} v_k^*$ für $1 \leq i \leq n$. Es folgt dann

$$B_{i,j} = b(v_i, v_j) = R(v_j)(v_i) = \sum_{k=1}^{n} A_{k,j} v_k^*(v_i) = A_{i,j}.$$

Das ist Teil (a). Teil (b) folgt hieraus mit Lemma 2.1.5. □

Satz 2.1.12 (Basiswechsel für Bilinearformen)**.** *Sei $b \in \mathrm{Bil}(V)$ und seien $\mathcal{B}, C$ Basen von V. Dann gilt*

$$\mathcal{M}_{\mathcal{B}}(b) = S^t \mathcal{M}_C(b) S,$$

wobei $S = S^{\mathcal{B}}_C$ die Basiswechselmatrix ist.

Beweis. Ist $\mathcal{B} = (v_1, \ldots, v_n)$ und $C = (w_1, \ldots, w_n)$ so gilt

$$v_j = \sum_{k=1}^{m} S_{k,j} w_k.$$

Seien $B = \mathcal{M}_{\mathcal{B}}(b)$ und $C = \mathcal{M}_{\mathcal{C}}(b)$. Dann ist $C_{i,j} = b(w_i, w_j)$ und

$$\begin{aligned} B_{i,j} = b(v_i, v_j) &= b\left(\sum_{k=1}^{m} S_{k,i} w_k, \sum_{l=1}^{m} S_{l,j} w_l\right) \\ &= \sum_{k,l} S_{k,i} b(w_k, w_l) S_{l,j} = \sum_{k,l} S_{k,i} C_{k,l} S_{l,j} = (S^t C S)_{i,j}. \end{aligned}$$ □

Definition 2.1.13. Zwei Matrizen $A, B \in \mathrm{M}_n(K)$ heißen *kongruent*, wenn es eine invertierbare Matrix $S \in \mathrm{GL}_n(K)$ gibt, so dass

$$B = S^t A S.$$

Wir stellen fest: A und B stellen genau dann dieselbe Bilinearform bzgl. verschiedener Basen dar, wenn sie kongruent sind.

Erinnerung: A und B heißen *ähnlich* oder *konjugiert*, wenn $B = S^{-1}AS$ gilt.

Beispiele 2.1.14.

- Die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ ist kongruent zur Einheitsmatrix, aber nicht konjugiert zur Einheitsmatrix.
- Wegen
$$\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}\begin{pmatrix} 1 & \\ & 2 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ & 2 \end{pmatrix}$$
sind die Matrizen $\left(\begin{smallmatrix} 1 & \\ & 2 \end{smallmatrix}\right)$ und $\left(\begin{smallmatrix} 1 & \frac{1}{2} \\ & 2 \end{smallmatrix}\right)$ konjugiert, aber sie sind nicht kongruent, weil die Matrix $\left(\begin{smallmatrix} 1 & \frac{1}{2} \\ & 2 \end{smallmatrix}\right)$ nicht symmetrisch ist (siehe nächster Abschnitt).

2.2 Symmetrische Formen

Definition 2.2.1. Eine Bilinearform b auf V heißt *symmetrisch*, wenn

$$b(v, w) = b(w, v)$$

für alle $v, w \in V$ gilt. Sei $\mathrm{Sym}(V)$ der Unterraum der symmetrischen Bilinearformen.

Definition 2.2.2. Eine Matrix $A \in \mathrm{M}_n(K)$ heißt *symmetrisch*, falls $A = A^t$ gilt. Sei $\mathrm{Sym}_n(K)$ der Raum aller symmetrischen Matrizen.

Eine Matrix $(a_{i,j}) \in \mathrm{M}_n(K)$ ist genau dann symmetrisch, wenn $a_{i,j} = a_{j,i}$ gilt. Damit ist jede symmetrische Matrix durch die Werte $a_{i,j}$ mit $i \leq j$ eindeutig festgelegt und es

folgt, dass die Dimension des Raums der symmetrischen Matrizen gleich

$$\dim \mathrm{Sym}_n(K) = n + (n-1) + \cdots + 1 = \frac{n(n+1)}{2}$$

ist.

Lemma 2.2.3. *Eine Bilinearform b auf einem endlich-dimensionalen Raum V ist genau dann symmetrisch, wenn die darstellende Matrix $\mathcal{M}_{\mathcal{B}}(b)$ symmetrisch ist. Hierbei ist $\mathcal{B}$ eine beliebige Basis.*

Beweis. Sei b symmetrisch und B die darstellende Matrix bzgl. der Basis $v_1, \ldots, v_n$. Dann ist $B_{i,j} = b(v_i, v_j) = b(v_j, v_j) = B_{j,i}$, also ist B symmetrisch. Sei umgekehrt B symmetrisch, dann ist $b(v_i, v_j) = b(v_j, v_i)$ und wegen Bilinearität folgt dasselbe für alle Vektoren. □

Satz 2.2.4. *Sei* $\mathrm{Char}(K) \neq 2$. *Sei b eine symmetrische Bilinearform auf dem endlich-dimensionalen Raum V. Dann gibt es eine Basis $v_1, \ldots, v_n$ von V, so dass $b(v_i, v_j) = 0$ für $i \neq j$, d.h. die Form b wird durch eine Diagonalmatrix dargestellt. Eine solche Basis nennt man* Orthogonalbasis *zu b.*

Beweis. Wir beweisen diesen Satz durch Induktion nach n. Für $n = 1$ ist nichts zu zeigen. Wir zeigen $n \to n+1$. Sei $v_1 \neq 0$ in V.

1. Fall. Ist $b(v_1, v) = 0$ für alle $v \in V$, so ergänzen wir v_1 zu einer Basis $v_1, \ldots, v_{n+1}$ von V und in dieser Basis wird b dargestellt durch die Matrix $\begin{pmatrix} 0 & 0 \\ 0 & C \end{pmatrix}$ für eine symmetrische Matrix $C \in \mathrm{M}_n(K)$. Sei $U = \mathrm{Spann}(v_2, \ldots, v_{n+1})$, dann stellt C die Form b eingeschränkt auf U dar. Nach Induktionsvoraussetzung können wir die Basis so wählen, dass C Diagonalgestalt hat und der Beweis ist fertig.

2. Fall. Gibt es ein $v \in V$ mit $b(v_1, v) \neq 0$, dann ist die polynomiale Abbildung

$$\lambda \mapsto b(v_1 + xv, v_1 + xv) = b(v_1, v_1) + 2xb(v_1, v) + x^2 b(v, v)$$

nicht die Nullabbildung (Hier wurde der Voraussetzung $\mathrm{Char}(K) \neq 2$ gebraucht!). Daher können wir v_1 durch einen Vektor der Form $v_1 + \lambda v$ mit $\lambda \in K$ ersetzen so dass

$b(v_1, v_1) \neq 0$ gilt. Sei nun

$$U = \left\{v \in V : b(v, v_1) = 0\right\} = \ker(v \mapsto b(v, v_1)).$$

dann ist U ein Untervektorraum, der v_1 nicht enthält. Ausserdem ist er der Kern eines nichttrivialen linearen Funktionals $V \to K$, nach der Dimensionsformel ist also $\dim U = n$. Sei $v_2, \ldots, v_{n+1}$ eine Basis von U, dann wird b in der Basis $v_1, \ldots, v_{n+1}$ durch eine Matrix der Form $\begin{pmatrix} \lambda & 0 \\ 0 & C \end{pmatrix}$ dargestellt mit $\lambda = b(v_1, v_1)$. Nach Induktionsvoraussetzung kann man $v_2, \ldots, v_{n+1}$ so wählen, dass C diagonal ist. □

Korollar 2.2.5. *Sei* $\mathrm{Char}(K) \neq 2$*. Jede symmetrische Matrix* $A \in \mathrm{Sym}_n(K)$ *ist kongruent zu einer Diagonalmatrix, d.h., es existiert* $S \in \mathrm{GL}_n(K)$ *so dass* $S^t AS$ *eine Diagonalmatrix ist.*

Beweis. Dies ist nur eine Umformulierung des Satzes für Matrizen. □

Beispiel 2.2.6. Hier ein Beispiel, das zeigt, dass die obige Aussage in Charakteristik 2 falsch wird. Sei K ein beliebiger Körper der Charakteristik 2 und sei $A = \left(\begin{smallmatrix} & 1 \\ 1 & \end{smallmatrix}\right) \in \mathrm{M}_2(K)$. Ist dann $S = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{M}_2(K)$ eine beliebige Matrix, dann rechnet man wegen $2 = 0$ nach, dass

$$SAS^t = (ad + bc)A$$

gilt, so dass A also nicht zu einer Diagonalmatrix kongruent ist.

Definition 2.2.7. Sei nun $K = \mathbb{R}$. Eine Bilinearform b auf V heißt *positiv definit*, falls $b(v, v) > 0$ für jedes $v \in V \setminus \{0\}$. Wir schreiben in diesem Fall $b > 0$.

Die Form b heißt *positiv semidefinit*, falls $b(v, v) \geq 0$ für alle $v \in V$. Wir schreiben $b \geq 0$.

Die Form heißt *negativ definit*, falls $-b$ positiv definit ist und ebenso für *negativ semidefinit*.

Definition 2.2.8. Sei b eine symmetrische Bilinearform auf V. Seien $U_1, \ldots, U_k$ Unterräume von V mit

$$V = U_1 \oplus \cdots \oplus U_k.$$

Dann heisst diese Zerlegung von V eine *Orthogonalzerlegung*, falls für $i \neq j$ stets gilt

$$b(U_i, U_j) = 0,$$

wobei $b(U_i, U_j) = \left\{b(u, u') : u \in U_i, u' \in U_j\right\}$.

Satz 2.2.9 (Trägheitssatz von Sylvester)**.** *Sei $K = \mathbb{R}$ der Körper der reellen Zahlen.*

(a) *Sei V endlich-dimensional und b eine symmetrische Bilinearform auf V. Dann existiert eine Orthogonalzerlegung*

$$V = V_0 \oplus V_+ \oplus V_-$$

dergestalt, dass $b = 0$ auf V_0, $b > 0$ auf V_+ und $b < 0$ auf V_-. Dabei ist der Raum V_0 und die Dimensionen $p = \dim V_+$ und $q = \dim V_-$ eindeutig bestimmt. Das Paar $(p, q) \in \mathbb{N}_0^2$ wird die Signatur *der Matrix, oder der dargestellten Bilinearform genannt.*

(b) *Jede symmetrische Matrix $A \in \mathrm{Sym}_n(\mathbb{R})$ ist kongruent zu einer eindeutig bestimmten Diagonalmatrix mit Diagonaleinträgen*

$$\underbrace{1, \ldots, 1}_{p \text{ mal}}, \underbrace{-1, \ldots, -1}_{q \text{ mal}}, 0, \ldots, 0.$$

Beweis. Sei $v_1, \ldots, v_n$ eine Orthogonalbasis von V. Durch Umnummerieren erreichen wir

$$b(v_j, v_j) \begin{cases} > 0 & 1 \le j \le p, \\ < 0 & p+1 \le j \le p+q, \\ = 0 & p+q+1 \le j \le n. \end{cases}$$

Sei dann

$$\begin{aligned} V_+ &= \mathrm{Spann}(v_1, \ldots, v_p) \\ V_- &= \mathrm{Spann}(v_{p+1}, \ldots, v_{p+q}) \\ V_0 &= \mathrm{Spann}(v_{p+q+1}, \ldots, v_n). \end{aligned}$$

Dann erfüllt die Zerlegung $V = V_+ \oplus V_- \oplus V_0$ die Bedingung. Weiter ist V_0 der Raum aller $u \in V$ mit $b(u, v) = 0$ für alle $v \in V$ und damit eindeutig bestimmt. Für die Eindeutigkeit der Dimensionen sei $V = V_0 \oplus V'_+ \oplus V'_-$ eine weitere Zerlegung, dann ist b auf $V_0 \oplus V_+$ positiv semidefinit, also ist $(V_0 \oplus V_+) \cap V'_- = 0$, damit folgt $\dim V_0 + \dim V_+ + \dim V'_- \le \dim V = \dim V_0 + \dim V_+ + \dim V_-$ und damit

$\dim V'_- \leq \dim V_-$. Aus Symmetriegründen folgt Gleichheit und ebenso für V_+.

Für Teil (b) wenden wir (a) auf $V = K^n$ und die durch A gegebene Bilinearform an. Dann folgt aus (a), dass A kongruent ist zu einer Diagonalmatrix mit Diagonaleinträgen $a_1, \ldots, a_n$ mit $a_1, \ldots, a_p > 0$, $a_{p+1}, \ldots, a_{P+q} < 0$ und $a_{p+q+1}, \ldots .a_n = 0$. Sei S die Diagonalmatrix mit Einträgen $s_1, \ldots, s_n$, wobei

$$s_j = \begin{cases} \frac{1}{\sqrt{|a_j|}} & a_j \neq 0, \\ 1 & a_j = 0. \end{cases}$$

Dann ist $S = S^t$ und $S^t A S$ ist eine Diagonalmatrix mit Einträgen in $\{\pm 1, 0\}$ wie verlangt. □

2.3 Skalarprodukte

Sei V ein Vektorraum über $\mathbb{R}$. Ein *Skalarprodukt* auf V ist eine positiv definite symmetrische Bilinearform $\langle v, w\rangle$. Also ist ein Skalarprodukt eine Abbildung $\langle ., .\rangle : V \times V \to \mathbb{R}$, so dass

- $v \mapsto \langle v, w\rangle$ ist linear für jedes $w \in V$,
- $\langle v, w\rangle = \langle w, v\rangle$,
- $\langle v, v\rangle > 0$ falls $v \neq 0$.

Beachte, dass insbesondere $\langle v, v\rangle$ reell sein muss, da > 0 für beliebige komplexe Zahlen nicht definiert ist.

Beispiel 2.3.1. Das *standard Skalarprodukt* auf $\mathbb{R}^n$ ist

$$\langle x, y\rangle = x^t y = x_1 y_1 + \cdots + x_n y_n.$$

Geometrisch ist $\|v\| = \sqrt{\langle v, v\rangle}$ die Länge eines Vektors. Über $\mathbb{C}$ führt dies zu Problemen, denn etwa

$$\begin{pmatrix} 1 \\ i \end{pmatrix}^t \begin{pmatrix} 1 \\ i \end{pmatrix} = 1 - 1 = 0,$$

man erhält also Vektoren der Länge Null! Um das zu verhindern, muss man über $\mathbb{C}$ hermitesche Formen betrachten:

Definition 2.3.2. Sei V ein Vektorraum über $\mathbb{C}$. Eine *hermitesche Form* ist eine Abbildung $\langle .,. \rangle : V \times V \to \mathbb{C}$ mit

- $v \mapsto \langle v, w \rangle$ ist linear für jedes $w \in V$ und
- $\langle w, v \rangle = \overline{\langle v, w \rangle}$ (komplexe Konjugation).

Eine hermitesche Form heißt *Skalarprodukt*, falls zusätzlich gilt

- $\langle v, v \rangle > 0$ für jedes $v \in V \setminus \{0\}$.

Beispiel 2.3.3. Das *standard Skalarprodukt* auf $V = \mathbb{C}^n$ ist

$$\langle v, w \rangle = v^t \overline{w} = v_1 \overline{w_1} + \cdots + v_n \overline{w_n},$$

wobei $\overline{w}$ der Vektor mit den komplex konjugierten Einträgen ist.

Bemerkung. Ist $\langle .,. \rangle$ ein Skalarprodukt auf einem $\mathbb{C}$-Vektorraum V, dann ist für jedes $v \in V$ die Abbildung $T = T_v : w \mapsto \langle v, w \rangle$ eine *konjugiert-lineare Abbildung*, d.h., es gilt

$$T(\lambda w + \mu w') = \overline{\lambda} T(w) + \overline{\mu} T(w').$$

2.4 Euklidische Norm

Sei $\mathbb{K}$ der Körper $\mathbb{R}$ oder $\mathbb{C}$. Sei $\langle .,. \rangle$ ein Skalarprodukt auf dem $\mathbb{K}$-Vektorraum V.

Definition 2.4.1. Die euklidische Norm eines Vektors $v \in V$ ist

$$\|v\| = \sqrt{\langle v, v \rangle}.$$

Man sagt: zwei Vektoren $v, w \in V$ stehen *senkrecht* aufeinander, falls $\langle v, w \rangle = 0$ ist.

Satz 2.4.2 (Pythagoras)**.** *Stehen die Vektoren v, w senkrecht aufeinander, dann ist*

$$\|v\|^2 + \|w\|^2 = \|v + w\|^2 .$$

Beweis. Es gilt

$$\begin{aligned}\|v+w\|^2 &= \langle v+w, v+w\rangle \\ &= \langle v,v\rangle + \underbrace{\langle v,w\rangle}_{=0} + \underbrace{\langle w,v\rangle}_{=0} + \langle w,w\rangle \\ &= \|v\|^2 + \|w\|^2 .\end{aligned}$$

□

Definition 2.4.3. Ein reeller Vektorraum mit einem Skalarprodukt heißt *euklidischer Raum*.

Ein komplexer Vektorraum mit einem Skalarprodukt heißt *unitärer Raum*.

Satz 2.4.4 (Cauchy-Schwarz-Ungleichung)**.** *Sei V ein unitärer oder euklidischer Vektorraum. Dann gilt für alle $v, w \in V$:*

$$|\langle v,w\rangle| \leq \|v\|\,\|w\| .$$

Beweis. Wir können $w \neq 0$ annehmen. Für jedes $t \in \mathbb{R}$ gilt

$$0 \leq \|v-tw\|^2 = \langle v-tw, v-tw\rangle = \|v\|^2 - 2t\,\mathrm{Re}\,\langle w,v\rangle + t^2\|w\|^2 .$$

Dieses quadratische Polynom in t nimmt sein Minimum in $t = \frac{\mathrm{Re}\langle v,w\rangle}{\|w\|^2}$ an. Setzen wir diesen Wert ein, folgt

$$0 \leq \|v\|^2 - 2\frac{\mathrm{Re}\,\langle v,w\rangle^2}{\|w\|^2} + \frac{\mathrm{Re}\,\langle v,w\rangle^2}{\|w\|^4}\|w\|^2 ,$$

also

$$\mathrm{Re}\,\langle v,w\rangle^2 \leq \|v\|^2\,\|w\|^2 .$$

Es gibt nun ein $\theta \in \mathbb{K}$ mit $|\theta| = 1$ so dass $\theta\langle v,w\rangle = |\langle v,w\rangle|$ gilt. Indem wir v durch θv ersetzen, folgt aus dem obigen

$$|\langle v,w\rangle|^2 = \mathrm{Re}\left(|\langle v,w\rangle|^2\right) = \mathrm{Re}\left(\theta^2\langle v,w\rangle^2\right) = \mathrm{Re}\left(\langle \theta v,w\rangle^2\right) = \mathrm{Re}(\langle \theta v,w\rangle)^2 \leq \|\theta v\|^2\|w\|^2 = \|v\|^2\|w\|^2 .$$

□

Satz 2.4.5. *Die Abbildung $\|.\|$ ist eine Norm, also*

- $\|v\| \geq 0$ *und* $\|v\| = 0 \Leftrightarrow v = 0$ — *Definitheit*
- $\|\lambda v\| = |\lambda| \, \|v\|$ — *Multiplikativität*
- $\|v + w\| \leq \|v\| + \|w\|$ — *Dreiecksungleichung*

Beweis. Die ersten beiden Eigenschaften sind klar. Zur Dreiecksungleichung rechne mit der Cauchy-Schwarz-Ungleichung:

$$\begin{aligned} \|v + w\|^2 &= \langle v + w, v + w \rangle \\ &= \langle v, v \rangle + \langle v, w \rangle + \langle w, v \rangle + \langle w, w \rangle \\ &\leq \langle v, v \rangle + 2|\langle v, w \rangle| + \langle w, w \rangle \\ &\leq \|v\|^2 + \|w\|^2 + 2\|v\| \, \|w\| \\ &= (\|v\| + \|w\|)^2 \end{aligned}$$

□

Satz 2.4.6. *Ist W ein komplexer Vektorraum und ist $\langle ., . \rangle : W \times W \to \mathbb{C}$ ein Skalarprodukt, dann ist der Realteil $(v, w) = \mathrm{Re}(\langle v, w \rangle)$ ein Skalarprodukt des reellen Vektorraums W.*

Ist umgekehrt $\langle ., . \rangle$ ein reelles Skalarprodukt des reellen Vektorraums V, dann ist

$$\langle v + iv', w + iw' \rangle_{\mathbb{C}} = \langle v, w \rangle + i \langle v', w \rangle - i \langle v, w' \rangle + \langle v', w' \rangle ,$$

$v, v', w, w' \in V$, ein Skalarprodukt des komplexen Vektorraums $V_{\mathbb{C}}$. Dies ist das eindeutig bestimmte Skalarprodukt auf $V_{\mathbb{C}}$, das $\langle ., . \rangle$ fortsetzt.

Beweis. Die Skalarproduktsaxiome sind für $\mathrm{Re}(\langle ., . \rangle)$ sofort verifiziert. Umgekehrt für die Komplexifizierung ist die Rechnung etwas länger, aber elementar. Zur Vereinfachung kann man benutzen, dass eine Abbildung $\alpha : W \to \mathbb{C}$ von einem komplexen Vektorraum W genau dann $\mathbb{C}$-linear ist, wenn sie $\mathbb{R}$-linear ist und wenn $\alpha(iv) = i\alpha(v)$ gilt.

Zur Eindeutigkeit der Komplexifizierung: Sei $(., .)$ eine weitere Fortsetzung von $\langle ., . \rangle$

zu einem komplexen Skalarprodukt. Jeder Vektor in $V_{\mathbb{C}}$ lässt sich in der Form $v + iv'$ mit $v, v' \in V$ schreiben. Für $v, v', w, w' \in V$ rechnen wir auf Grund der (anti-)Linearität von $(.,.)$,

$$\begin{aligned}(v + iv', w + iw') &= (v, w) + i(v', w) - i(v, w') + (v', w') \\ &= \langle v, w\rangle + i\langle v', w\rangle - i\langle v, w'\rangle + \langle v', w'\rangle \\ &= \langle v + iv', w + iw'\rangle_{\mathbb{C}}\end{aligned}$$

□

Wir haben im letzten Abschnitt gelernt, dass jedes Skalarprodukt eine Norm induziert. Kommt aber jede Norm von einem Skalarprodukt? Und wenn, ist das Skalarprodukt eindeutig bestimmt durch die Norm?

Satz 2.4.7 (Polarisierungsformeln)**.** *Ist V ein reeller Vektorraum und ist $\|.\|$ eine Norm, die durch ein Skalarprodukt gegeben ist. Dann gilt für dieses Skalarprodukt:*

$$\langle v, w\rangle = \frac{1}{4}\left(\|v + w\|^2 - \|v - w\|^2\right).$$

Ist W ein komplexer Vektorraum und ist $\|.\|$ eine Norm, die durch ein komplexes Skalarprodukt gegeben ist, so gilt für dieses Skalarprodukt

$$\langle v, w\rangle = \frac{1}{4}\left(\|v + w\|^2 - \|v - w\|^2\right) + i\frac{1}{4}\left(\|v + iw\|^2 - \|v - iw\|^2\right).$$

Insbesondere ist jeweils das Skalarprodukt durch die Norm eindeutig festgelegt.

Proof. Betrachte zuerst den reellen Fall. Ist $\|.\|$ von $\langle .,.\rangle$ induziert, dann gilt

$$\begin{aligned}\frac{1}{4}\left(\|v + w\|^2 - \|v - w\|^2\right) &= \frac{1}{4}\left(\langle v + w, v + w\rangle - \langle v - w, v - w\rangle\right) \\ &= \frac{1}{4}\left(\langle v, v\rangle + \langle v, w\rangle + \langle w, v\rangle + \langle w, w\rangle - \langle v, v\rangle + \langle v, w\rangle + \langle w, v\rangle - \langle w, w\rangle\right) \\ &= \langle v, w\rangle.\end{aligned}$$

Im zweiten Fall ist die Norm ja ebensogut auch von dem reellen Skalarprodukt $\mathrm{Re}(\langle .,.\rangle)$ induziert. Für dieses gilt nach dem ersten Teil

$$\mathrm{Re}(\langle v, w\rangle) = \frac{1}{4}\left(\|v + w\|^2 - \|v - w\|^2\right).$$

Nun ist $\langle v, w\rangle = \mathrm{Re} + i\,\mathrm{Im}$ und es ist

$$\mathrm{Im}(\langle v, w\rangle) = -\mathrm{Re}(i\langle v, w\rangle) = \mathrm{Re}(\langle v, iw\rangle),$$

woraus die behauptete Formel folgt. □

Satz 2.4.8. *Eine gegebene Norm $\|.\|$ auf einem reellen Vektorraum ist genau dann durch ein Skalarprodukt gegeben, wenn sie die* Parallelogrammidentität

$$\|v + w\|^2 + \|v - w\|^2 = 2\left(\|v\|^2 + \|w\|^2\right)$$

erfüllt.

Beweis. Ist $\|.\|$ von dem Skalarprodukt $\langle ., .\rangle$ induziert, dann gilt

$$\begin{aligned}\|v + w\|^2 + \|v - w\|^2 &= \langle v + w, v + w\rangle + \langle v - w, v - w\rangle \\ &= \langle v, v\rangle + 2\langle v, w\rangle + \langle w, w\rangle + \langle v, v\rangle - 2\langle v, w\rangle + \langle w, w\rangle \\ &= 2\left(\|v\|^2 + \|w\|^2\right).\end{aligned}$$

Sei umgekehrt $\|.\|$ eine Norm, die die Parallelogrammidentität erfüllt. Definiere dann

$$\begin{aligned}\langle v, w\rangle &:= \frac{1}{4}\left(\|v + w\|^2 - \|v - w\|^2\right) \\ &= \frac{1}{4}\left(\|v + w\|^2 + \|v - w\|^2 - 2\|v - w\|^2\right) \\ &= \frac{1}{2}\left(\|v\|^2 + \|w\|^2 - \|v - w\|^2\right).\end{aligned}$$

Wir zeigen, dass $\langle .,. \rangle$ ein Skalarprodukt ist. Dazu rechnen wir

$$\begin{aligned}
\langle v+v', w\rangle - \langle v, w\rangle - \langle v', w\rangle &= \frac{1}{2}\Big(\|v+v'\|^2 + \|w\|^2 - \|v+v'-w\|^2 \\
&\quad - \|v\|^2 - \|w\|^2 + \|v-w\|^2 - \|v'\|^2 - \|w\|^2 + \|v'-w\|^2 \Big) \\
&= \frac{1}{2}\Big(\|v+v'\|^2 - \|w\|^2 - \|v+v'-w\|^2 \\
&\quad \underbrace{- \|v\|^2 - \|v'\|^2}_{=-\frac{1}{2}\left(\|v+v'\|^2+\|v-v'\|^2\right)} + \|v-w\|^2 + \|v'-w\|^2 \Big) \\
&= \frac{1}{2}\Big(\frac{1}{2}\|v+v'\|^2 - \frac{1}{2}\|v-v'\|^2 \underbrace{- \|w\|^2 - \|v+v'-w\|^2}_{-\frac{1}{2}\left(\|v+v'-2w\|^2-\|v+v'\|^2\right)} \\
&\quad + \|v-w\|^2 + \|v'-w\|^2 \Big) \\
&= \frac{1}{2}\Big(-\frac{1}{2}\|v-v'\|^2 - \frac{1}{2}\|v+v'-w\|^2 \\
&\quad \underbrace{+ \|v-w\|^2 + \|v'-w\|^2}_{=\frac{1}{2}\|v+v'-2w\|^2+\frac{1}{2}\|v-v'\|^2} \Big) = 0
\end{aligned}$$

Damit haben wir die Additivität im ersten Argument. Für $n \in \mathbb{N}$ folgt daraus durch iterierte Anwendung

$$\langle nv, w\rangle = \langle v + \cdots + v, w\rangle = \langle v, w\rangle + \cdots + \langle v, w\rangle = n\langle v, w\rangle .$$

Es gilt auch $\langle nv, w\rangle + \langle -nv, w\rangle = \langle 0, w\rangle = 0$, so dass $\langle -nv, w\rangle = -n\langle v, w\rangle$, also insgesamt $\langle kv, w\rangle = k\langle v, w\rangle$ für jedes $k \in \mathbb{Z}$. Mit $p \in \mathbb{Z}$ und $q \in \mathbb{N}$ folgt

$$q\left\langle \frac{p}{q}v, w\right\rangle = \langle pv, w\rangle = p\langle v, w\rangle = q\frac{p}{q}\langle v, w\rangle ,$$

so dass nach Division durch q folgt $\langle rv, w\rangle = r\langle v, w\rangle$ für jede rationale Zahl r. Nach der umgekehrten Dreiecksungleichung gilt für $x, y \in \mathbb{R}$, dass

$$\Big| \|xv - w\| - \|yv - w\| \Big| \leq \|(x-y)v\| = |x-y|\,\|v\|$$

Damit ist die Abbildung $x \mapsto \langle xv, w\rangle = \frac{1}{2}\left(x^2\|v\|^2 + \|w\| - \|xv-w\|^2\right)$ eine stetige Abbildung und da jedes $x \in \mathbb{R}$ der Limes einer Folge aus $\mathbb{Q}$ ist, folgt $\langle xv, w\rangle = x\langle v, w\rangle$. Die Symmetrie $\langle v, w\rangle = \langle w, v\rangle$ ist klar und wegen

$$\langle v, v\rangle = \|v\|^2$$

ist $\langle .,. \rangle$ auch positiv definit, also ein Skalarprodukt. Dieselbe Gleichung zeigt, dass dieses Skalarprodukt die gegebene Norm induziert. □

Beispiele 2.4.9.

- Die *Maximumsnorm* auf $\mathbb{R}^n$,

$$\|x\|_\infty = \max_{j=1}^{n} |x_j|$$

ist eine Norm, die für $n \geq 2$ nicht von einem Skalarprodukt induziert wird, denn für $x = e_1$ und $y = e_2$ gilt

$$\|x + y\|_\infty^2 + \|x - y\|_\infty^2 = 1 + 1 \neq 2(1 + 1) = 2\left(\|x\|_\infty^2 + \|y\|_\infty^2\right),$$

so dass die Parallelogrammidentität nicht erfüllt ist.

- Die *Summennorm* auf $\mathbb{R}^n$,

$$\|x\|_1 = |x_1| + \cdots + |x_n|$$

ist ebenfalls eine Norm, die die Parallelogrammidentität für $n \geq 2$ nicht erfüllt, denn mit denselben Beispielvektoren gilt

$$\|x + y\|_1^2 + \|x - y\|_1^2 = 4 + 4 = 8 \neq 4 = 2\left(\|x\|_1^2 + \|y\|_1^2\right).$$

2.5 Projektion und Orthonormalisierung

Sei $\mathbb{K} = \mathbb{R}$ oder $\mathbb{K} = \mathbb{C}$. Sei V ein endlich-dimensionaler Vektorraum mit Skalarprodukt. Eine Familie $e_1, \ldots, e_n$ von V heißt *orthonormal*, wenn

$$\left\langle e_i, e_j \right\rangle = \begin{cases} 1 & i = j, \\ 0 & i \neq j. \end{cases}$$

Ist die Familie überdies eine Basis, so heißt sie *Orthonormalbasis*.

Satz 2.5.1. *Sei $v_1, \ldots, v_n$ eine gegebene Basis von V. Dann existiert eine Orthonormalbasis $e_1, \ldots, e_n$ mit*

$$\text{Spann}(v_1, \ldots, v_k) = \text{Spann}(e_1, \ldots, e_k)$$

für jedes $1 \leq k \leq n$.

Beweis. Wir konstruieren die e_j induktiv. Als Induktionsanfang sei $e_1 = \frac{1}{\|v_1\|} v_1$. Im Induktionsschritt sei eine orthonormale Familie $e_1, \dots, e_k$ bereits konstruiert mit $\text{Spann}(v_1, \dots, v_j) = \text{Spann}(e_1, \dots, e_j)$ für jedes $1 \leq j \leq k$. Definiere

$$\tilde{v}_{k+1} = v_{k+1} - \langle v_{k+1}, e_1 \rangle e_1 - \cdots - \langle v_{k+1}, e_k \rangle e_k.$$

Da v_{k+1} nicht im Spann der $e_1, \dots, e_k$ liegt, ist $\tilde{v}_{k+1} \neq 0$. Ferner gilt $\left\langle \tilde{v}_{k+1}, e_j \right\rangle = 0$ für jedes $1 \leq j \leq k$. Definiere nun

$$e_{k+1} = \frac{1}{\|\tilde{v}_{k+1}\|} \tilde{v}_{k+1}.$$

Dann ist $e_1, \dots, e_{k+1}$ orthonormal mit $\text{Spann}(v_1, \dots, v_j) = \text{Spann}(e_1, \dots, e_j)$ für jedes $1 \leq j \leq k+1$. □

Beispiel 2.5.2. Sei V der reelle Vektorraum der Polynome vom Grad ≤ 2 mit dem Skalarprodukt $\langle f, g \rangle = \int_0^1 f(x) g(x)\, dx$. Wir orthonormalisieren die natürliche Basis $(v_1, v_2, v_3) = (1, x, x^2)$. Zunächst ist

$$\|v_1\|^2 = \int_0^1 1\, dx = 1,$$

also ist $e_1 = v_1$. Dann ist

$$\langle v_1, v_2 \rangle = \int_0^1 x\, dx = \frac{1}{2}, \quad \langle v_2, v_2 \rangle = \int_0^1 x^2\, dx = \frac{1}{3}.$$

Wir erhalten

$$\tilde{v}_2 = v_2 - \langle v_2, e_1 \rangle e_1 = v_2 - \frac{1}{2} e_1 = x - \frac{1}{2}.$$

Wir rechnen

$$\|\tilde{v}_2\|^2 = \left\langle x - \frac{1}{2}, x - \frac{1}{2} \right\rangle = \int_0^1 x^2\, dx - \int_0^1 x\, dx + \int_0^1 \frac{1}{4}\, dx = \frac{1}{3} - \frac{1}{2} + \frac{1}{4} = \frac{1}{12}.$$

Es folgt $e_2 = \sqrt{12}\tilde{v}_2 = 2\sqrt{3}\left(x - \frac{1}{2}\right) = 2\sqrt{3}x - \sqrt{3}$. Schliesslich ist

$$\tilde{v}_3 = v_3 - \langle v_3, e_2 \rangle e_2 - \langle v_3, e_1 \rangle e_1.$$

Wir rechnen

$$\langle v_3, e_2\rangle = \int_0^1 x^2(2\sqrt{3}x - \sqrt{3})\,dx = \frac{\sqrt{3}}{2} - \frac{\sqrt{3}}{3} = \frac{\sqrt{3}}{6}.$$

Sowie

$$\langle v_3, e_1\rangle = \int_0^1 x^2 = \frac{1}{3}.$$

Es folgt

$$\tilde{v}_3 = x^2 - \frac{\sqrt{3}}{6}(2\sqrt{3}x - \sqrt{3}) - \frac{1}{3} = x^2 - x + \frac{1}{6}.$$

Und weiter

$$\begin{aligned}\|\tilde{v}_3\|^2 &= \int_0^1 \left(x^2 - 2x + \frac{1}{6}\right)^2 dx \\ &= \int_0^1 x^4 - 2x^3 + \frac{4}{3}x^2 - \frac{1}{3}x + \frac{1}{36}\,dx \\ &= \frac{1}{5} - \frac{1}{2} + \frac{4}{9} - \frac{1}{6} + \frac{1}{36} \\ &= \frac{1}{180}\end{aligned}$$

also ist

$$e_3 = \sqrt{180}\tilde{v}_3 = 5\sqrt{5}x^2 - 6\sqrt{5}x + \sqrt{5}.$$

Definition 2.5.3. Sei nun $U \subset V$ ein Unterraum. Definiere den *Orthogonalraum* $U^\perp$ durch

$$U^\perp = \left\{v \in V : \langle v, u\rangle = 0\ \forall_{u\in U}\right\}.$$

Satz 2.5.4. *Es gilt*

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

Beweis. Wir zeigen zunächst $U \cap U^\perp = 0$. Sei also $u \in U \cap U^\perp$. Dann ist $\langle u, u\rangle = 0$, also $u = 0$.

Es bleibt zu zeigen, dass $V = U + U^\perp$. Sei $e_1, \ldots, e_k$ eine ONB von U. Für beliebiges $v \in V$ sei

$$u = \langle v, e_1\rangle\, e_1 + \cdots + \langle v, e_k\rangle\, e_k$$

und $w = v - u$. Dann gilt $v = u + w$, ferner ist $u \in U$ und wir müssen zeigen, dass

$w \in U^\perp$ ist. Hierzu reicht es, zu zeigen, dass $\langle w, e_j \rangle = 0$ für $1 \leq j \leq k$ gilt. Es ist

$$\langle w, e_j \rangle = \langle v, e_j \rangle - \langle u, e_j \rangle = \langle v, e_j \rangle - \langle v, e_j \rangle = 0. \qquad \square$$

Definition 2.5.5. Eine lineare Abbildung $P : V \to V$ heißt *Projektion*, falls

$$P^2 = P$$

gilt.

Satz 2.5.6. *Ist P eine Projektion, so gilt $V = \ker P \oplus \operatorname{Bild} P$. Ist $v = v_{\ker} + v_{\text{Bild}}$ die Zerlegung eines gegebenen $v \in V$, so ist $P(v) = v_{\text{Bild}}$. Mithin ist die Projektion P durch Kern und Bild eindeutig festgelegt.*

Ist umgekehrt $V = U \oplus W$ eine gegebene Zerlegung in Unterräume, dann ist die Abbildung $P(u + w) = u$ für $u \in U$, $w \in W$, eine Projektion mit Kern W und Bild U.

Beweis. Für jedes $v \in V$ ist $v_{\text{Bild}} = Pv$ im Bild, und $v_{\ker} = v - Pv$ ist im Kern, denn

$$Pv_{\ker} = Pv - P^2v = Pv - Pv = 0.$$

Es gilt dann $v = v_{\text{Bild}} + v_{\ker}$ und $P(v) = v_{\text{Bild}}$. Insbesondere ist also $V = \ker P + \operatorname{Bild} P$. Es bleibt zu zeigen $(\operatorname{Bild} P) \cap (\ker P) = 0$, womit diese Zerlegung auch eindeutig bestimmt ist. Sei also w in diesem Schnitt, dann gibt es ein v mit $w = Pv$. daher folgt $0 = Pw = P^2v = Pv = w$.

Die zweite Aussage ist klar. $\square$

Definition 2.5.7. Eine Projektion P heißt *Orthogonalprojektion*, falls

$$(\operatorname{Bild} P) \perp (\ker P).$$

Sei $U \subset V$ ein Unterraum, dann schreiben wir $P_U : V \to V$ für die Orthogonalprojektion mit Bild U und Kern $U^\perp$.

Proposition 2.5.8. *Gilt $U \subset W \subset V$, dann ist*

$$P_U = P_W P_U = P_U P_W.$$

Beweis. Wir haben eine direkte Summenzerlegung

$$V = U \oplus (U^\perp \cap W) \oplus W^\perp.$$

Ist $v \in V$, so schreibe entsprechend $v = u + w + z$. Es gilt $P_U(v) = u$, $P_W(v) = u + w$, sowie

$$\begin{aligned} P_U P_W(v) &= P_U(u + w) = u \\ P_W P_U(v) &= P_W(u) = u. \end{aligned}$$

□

2.6 Selbstadjungierte Endomorphismen

Definition 2.6.1. Sei $(V, \langle ., . \rangle)$ ein endlich-dimensionaler $\mathbb{K}$ Vektorraum mit Skalarprodukt. Eine lineare Selbstabbildung $T : V \to V$ heißt auch *Endomorphismus*.

Satz 2.6.2 (Riesz)**.** *Für jede lineare Abbildung $\alpha : V \to \mathbb{K}$ existiert genau ein Vektor v_α, so dass*

$$\alpha(v) = \langle v, v_\alpha \rangle$$

für jedes $v \in V$ gilt.

Beweis. Ist $\alpha = 0$ setzen wir $v_\alpha = 0$. Ist $\alpha \neq 0$, so gibt es wegen $V = U \oplus U^\perp$ ein $v_0 \in U^\perp$ mit $\alpha(v_0) = 1$. Für beliebiges $v \in V$ gilt dann $v - \mu v_0 \in U$ für $\mu = \alpha(v)$, also ist $v = u + \alpha(v)v_0$. Setze $v_\alpha = \frac{1}{\langle v_0, v_0 \rangle} v_0$. Dann gilt

$$\langle v, v_\alpha \rangle = \frac{\langle v, v_0 \rangle}{\langle v_0, v_0 \rangle} = \frac{\langle u + \alpha(v)v_0, v_0 \rangle}{\langle v_0, v_0 \rangle} = \alpha(v).$$

Schließlich zur Eindeutigkeit: ist w ein zweiter Vektor mit dieser Eigenschaft, dann ist $\langle v, v_\alpha - w \rangle = 0$ für jeden Vektor v, also insbesondere für $v = v_\alpha - w$, woraus $w = v_\alpha$ folgt. □

Definition 2.6.3. Sei $T : V \to V$ linear. Für gegebenes $w \in V$ ist die Abbildung $v \mapsto \langle Tv, w \rangle$ linear, also gibt es einen eindeutig bestimmten Vektor $T^* w$ mit

$$\langle Tv, w \rangle = \langle v, T^* w \rangle$$

für jedes $v \in V$. Die Abbildung $w \mapsto T^* w$ heißt die zu T *adjungierte Abbildung*.

Satz 2.6.4. *Die adjungierte Abbildung T^* ist linear.*

Beweis. Seien $v, w, w' \in V$ und $\lambda \in \mathbb{K}$, so gilt

$$\begin{aligned}\langle v, T^*(\lambda w + w')\rangle &= \langle Tv, \lambda w + w'\rangle \\ &= \overline{\lambda}\,\langle Tv, w\rangle + \langle Tv, w'\rangle \\ &= \overline{\lambda}\,\langle v, T^*w\rangle + \langle v, T^*(w')\rangle \\ &= \langle v, \lambda T^*w + T^*(w')\rangle\,.\end{aligned}$$

Da die Skalarprodukte $\langle v, w\rangle$ für alle v den Vektor w eindeutig festlegen, folgt

$$T^*(\lambda w + w') = \lambda T^*w + T^*(w').$$ □

Proposition 2.6.5. *Seien $S, T : V \to V$ linear.*

(a) *Für alle $v, w \in V$ gilt $\langle v, Tw\rangle = \langle T^*v, w\rangle$.*

(b) *Es gilt*

$$I^* = I, \quad (\lambda T + S)^* = \overline{\lambda}T^* + S^*, \quad (ST)^* = T^*S^*, \quad T^{**} = T.$$

Hier steht I für die Einheitsmatrix und T^{**} für $(T^*)^*$.

Beweis. Für (a) rechne

$$\langle v, Tw\rangle = \overline{\langle Tw, v\rangle} = \overline{\langle w, T^*v\rangle} = \langle T^*v, w\rangle\,.$$

Die erste Aussage von (b) ist klar. Für die zweite rechne

$$\begin{aligned}\langle v, (\lambda S + T)^*w\rangle &= \langle (\lambda S + T)v, w\rangle = \lambda\,\langle Sv, w\rangle + \langle Tv, w\rangle \\ &= \lambda\,\langle v, S^*w\rangle + \langle v, T * w\rangle \\ &= \left\langle v, \overline{\lambda}S^*w + T^*w\right\rangle = \left\langle v, (\overline{\lambda}S^* + T^*)w\right\rangle.\end{aligned}$$

Für die dritte

$$\langle v, (ST)^*w\rangle = \langle STv, w\rangle = \langle Tv, S^*w\rangle = \langle v, T^*S^*w\rangle\,.$$

Für die letzte schließlich benutzen wir (a)

$$\langle Tv, w\rangle = \langle v, T^* w\rangle = \langle T^{**} v, w\rangle .$$ □

Beispiel 2.6.6. Sei $V = \mathbb{C}^n$ und $\langle v, w\rangle = v^t \overline{w}$ das standard Skalarprodukt. Sei $A \in \mathrm{M}_n(\mathbb{C})$, dann gilt

$$\langle Av, w\rangle = (Av)^t \overline{w} = v^t A^t \overline{w} = v^t \overline{\overline{A}^t w} = \left\langle v, \overline{A}^t w \right\rangle .$$

Also ist die adjungierte Abbildung durch die Matrix $\overline{A}^t$ gegeben, die wir deshalb auch die *adjungierte Matrix* nennen und sie als $A^* = \overline{A}^t$ schreiben.

Definition 2.6.7. Ist $\mathbb{K} = \mathbb{C}$, so heisst Eine lineare Abbildung T heißt *selbstadjungiert*, falls $T = T^*$ gilt. Eine Matrix $A \in \mathrm{M}_n(\mathbb{K})$ heißt selbstadjungiert, falls $A = A^*$.

Ist $\mathbb{K} = \mathbb{R}$ so heißt T *symmetrisch*, falls $T = T^*$ und eine Matrix $A \in \mathrm{M}_n(\mathbb{R})$ heißt symmetrisch, wenn $A = A^t$ gilt.

Satz 2.6.8. *Ist T selbstadjungiert, dann ist jeder Eigenwert reell.*

Beweis. Sei λ ein Eigenwert und v ein Eigenvektor. Dann gilt

$$\lambda \langle v, v\rangle = \langle \lambda v, v\rangle = \langle Tv, v\rangle = \langle v, Tv\rangle = \langle v, \lambda v\rangle = \overline{\lambda} \langle v, v\rangle .$$

Da $\langle v, v\rangle \neq 0$, folgt $\lambda = \overline{\lambda}$. □

Beispiel 2.6.9. Sei $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix} \in \mathrm{M}_2(\mathbb{R})$. Dann muss jeder Eigenwert dieser Matrix reell sein. Wir rechnen

$$\begin{aligned} \chi_A(x) &= \det \begin{pmatrix} x-a & -b \\ -b & x-c \end{pmatrix} = (x-a)(x-c) - b^2 \\ &= x^2 - (a+c)x + ac - b^2 \\ &= \left(x - \frac{a+c}{2}\right)^2 - \left(\frac{(a+c)^2}{4} - ac + b^2\right). \end{aligned}$$

Damit die Eigenwerte reell sind, muss also $\left(\frac{(a+c)^2}{4} - ac + b^2\right) \geq 0$ sein. Es ist aber

$$\begin{aligned}\frac{(a+c)^2}{4} - ac + b^2 &= \frac{a^2 + 2ac + c^2 - 4ac}{4} + b^2 \\ &= \frac{a^2 - 2ac + c^2}{4} + b^2 = \frac{(a-c)^2}{4} + b^2 \geq 0.\end{aligned}$$

Proposition 2.6.10. (a) *Ist $T : V \to V$ selbstadjungiert, dann ist*

$$\ker(T) \perp \text{Bild}(T).$$

(b) *Eine Projektion ist genau dann eine Orthogonalprojektion, wenn sie selbstadjungiert ist.*

Beweis. (a) Sei $T = T^*$ und sei $u \in \ker(T)$, sowie $w \in \text{Bild}(T)$, also etwa $w = T(v)$. Dann ist

$$\langle u, w\rangle = \langle u, T(v)\rangle = \langle T(u), v\rangle = \langle 0, v\rangle = 0.$$

Damit folgt $\ker(T) \perp \text{Bild}(T)$.

(b) Sei V ein $\mathbb{K}$-Vektorraum und sei $P : V \to V$ eine Orthogonalprojektion, also $P^2 = P$ und $\ker(P) \perp \text{Bild}(P)$. Nach der Dimensionsformel gilt dann $V = \ker(P) \oplus \text{Bild}(P)$ und ist $v \in V$ mit der Zerlegung $v = u + w$, so ist $P(v) = w$. Nun zeigen wir, dass P selbstadjungiert ist, sei also $v' = u' + w'$ ein zweiter Vektor in V, dann gilt

$$\begin{aligned}\langle P(v), v'\rangle = \langle w, u' + w'\rangle &= \overbrace{\langle w, u'\rangle}^{=0} + \langle w, w'\rangle \\ &= \underbrace{\langle u, w'\rangle}_{=0} + \langle w, w'\rangle = \langle v, P(v')\rangle\,.\end{aligned}$$

Die Umkehrung folgt aus Teil (a). □

2.7 Unitäre und normale Endomorphismen

Definition 2.7.1. Ein Endomorphismus $T : V \to V$ eines Raums mit Skalarprodukt heißt *unitär*, falls $\mathbb{K} = \mathbb{C}$ ist und

$$\langle Tv, Tw\rangle = \langle v, w\rangle \qquad (*)$$

für alle $v, w \in V$ gilt. Ist $\mathbb{K} = \mathbb{R}$ und gilt (*), so heißt T *orthogonal*.

Satz 2.7.2. (a) *T ist genau dann orthogonal/unitär, wenn*

$$TT^* = T^*T = \mathrm{Id}_V$$

gilt. Insbesondere sind orthogonale/unitäre Endomorphismen stets invertierbar.

(b) *Ist T orthogonal/unitär, so gilt*

$$v \perp w \quad \Rightarrow \quad Tv \perp Tw.$$

(c) *Ist T orthogonal/unitär und ist $\lambda \in \mathbb{K}$ ein Eigenwert, so gilt $|\lambda| = 1$.*

Beweis. (a) "⇒" Sei T orthogonal/unitär, dann gilt

$$\langle T^*Tv, w\rangle = \langle Tv, Tw\rangle = \langle v, w\rangle .$$

Damit folgt $T^*T = \mathrm{Id}$ und damit auch $TT^* = \mathrm{Id}$, da $\dim V < \infty$.

"⇐" Sei $T^*T = \mathrm{Id}$, dann gilt $\langle v, w\rangle = \langle T^*Tv, w\rangle = \langle Tv, Tw\rangle$.

(b) ist klar.

(c) Sei λ ein Eigenwert und v ein Eigenvektor, dann gilt

$$|\lambda|^2 \langle v, v\rangle = \langle \lambda v, \lambda v\rangle = \langle Tv, Tv\rangle = \langle v, v\rangle . \qquad \square$$

Beispiel 2.7.3. Sei $V = \mathbb{R}^2$, $\theta \in \mathbb{R}$ und sei

$$k(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

Dann ist $k(\theta)^t k(\theta) = I$, also ist $k(\theta)$ orthogonal.

Definition 2.7.4. Ein Endomorphismus $T : V \to V$ heißt *normal*, falls

$$TT^* = T^*T$$

gilt. Insbesondere folgt

$$T \text{ selbstadjungiert oder orthogonal/unitär} \quad \Rightarrow \quad T \text{ normal.}$$

Eine Matrix $A \in \mathrm{M}_n(\mathbb{C})$ heißt *unitär*, falls A bezüglich des Standard-Skalarproduktes auf $\mathbb{C}^n$ unitär ist, falls also $A^*A = I$ gilt, wobei $A^* = \overline{A}^t$. Sei $\mathrm{U}(n)$ die Menge aller unitären Matrizen in $\mathrm{M}_n(\mathbb{C})$.

Proposition 2.7.5. *Die Menge* $\mathrm{U}(n)$ *ist eine Untergruppe von* $\mathrm{GL}_n(C)$*. Man nennt sie die* unitäre Gruppe*.*

Beweis. Jeder unitäre Endomorphismus ist invertierbar, also gilt $\mathrm{U}(n) \subset \mathrm{GL}_n(\mathbb{C})$. Ist $A \in \mathrm{U}(n)$,so ist $A^{-1} = A^*$ ebenfalls in $\mathrm{U}(n)$. Sind $A, B \in \mathrm{U}(n)$, dann gilt

$$(AB)^*AB = B^*A^*AB = B^*B = I,$$

daher ist $AB \in \mathrm{U}(n)$. □

Korollar 2.7.6. *Eine Matrix* $A \in \mathrm{M}_n(\mathbb{C})$ *ist genau dann unitär, wenn die Zeilen oder die Spalten eine Orthonormalbasis von* $\mathbb{C}^n$ *bilden.*

Beweis. Seien $a_1, \ldots, a_n$ die Spalten von A. Es gilt

$$(A^*A)_{i,j} = \overline{a}_i^t a_j = \overline{\langle a_i, a_j \rangle}.$$

Also gilt $A^*A = I \Leftrightarrow (a_1, \ldots, a_n)$ ist eine ONB. Der Beweis fier die Zeilen geht ebenso indem man $AA^* = I$ benutzt. □

2.8 Der Spektralsatz

Satz 2.8.1 (Spektralsatz für normale Operatoren)**.** *Sei* $\mathbb{K} = \mathbb{C}$ *und sei* $T : V \to V$ *linear. Dann sind äquivalent*

(a) *T ist normal.*

(b) *Es gibt eine Orthonormalbasis von V, die aus Eigenvektoren von T besteht.*

(c) *T ist diagonalisierbar und die Eigenräume stehen senkrecht aufeinander.*

Beweis. (a)⇒(c): Induktion nach $n = \dim V$. Für $n = 0$ ist nichts zu zeigen. Sei also $n \geq 1$ und die Behauptung für alle kleineren Dimensionen gezeigt. Es gibt dann einen Eigenwert $\lambda \in \mathbb{C}$ von T. Sei $U = \mathrm{Eig}(T, \lambda)$ der zugehörige Eigenraum. Für $u \in U$ ist

$$T(T^*u) = T^*(Tu) = T^*(\lambda u) = \lambda T^*u,$$

also ist T^*u wieder in U und somit $T^*U \subset U$. Wir behaupten, dass $T(U^\perp) \subset U^\perp$ und ebenso für T^*. Sei hierzu $v \in U^\perp$. Dann gilt für jedes $u \in U$,

$$\langle Tv, u\rangle = \Big\langle v, \underbrace{T^*u}_{\in U} \Big\rangle = 0.$$

Also ist $T(U^\perp) \subset U^\perp$. Der Beweis für T^* geht genauso. Damit ist dann $T|_{U^\perp}$ normal und da $\dim U^\perp < \dim V$, folgt nach Induktionsvoraussetzung, dass $T|_{U^\perp}$ diagonalisierbar ist mit orthogonalen Eigenräumen. Dies folgt dann auch für T, da V die orthogonale Summe von U und $U^\perp$ ist.

(c)⇒(b) folgt, da die Eigenräume ONBs besitzen, die man zu einer ONB von V zusammenfassen kann.

(b)⇒(a): Sei $e_1, \ldots, e_n$ eine ONB mit $Te_j = \lambda_j e_j$. Dann folgt

$$\begin{aligned}\left\langle T^*e_j, e_i\right\rangle = \langle e_i, Te_i\rangle &= \left\langle e_j\lambda_i e_i\right\rangle \\ &= \overline{\lambda}_i \left\langle e_j, e_i\right\rangle = \overline{\lambda}_j\delta_{i,j} \\ &= \overline{\lambda}_j \left\langle e_j, e_i\right\rangle = \left\langle \overline{\lambda}_j e_j, e_i\right\rangle.\end{aligned}$$

Da dies fier alle i gilt, folgt

$$T^*e_j = \overline{\lambda}_j e_j.$$

Also auch

$$T^*Te_j = \overline{\lambda}_j\lambda_j e_j = TT^*e_j.$$ □

Korollar 2.8.2. *Ist T normal, so folgt für $\lambda \in \mathbb{C}$,*

$$\mathrm{Eig}(T, \lambda) = \mathrm{Eig}(T^*, \overline{\lambda}).$$

Beweis. Dies folgt aus dem Beweisschritt (b)⇒(a). □

Korollar 2.8.3. *Eine Matrix $A \in \mathrm{M}_n(\mathbb{C})$ ist genau dann normal, wenn es eine unitäre Matrix*

$S \in U(n)$ gibt, so dass $S^{-1}AS$ eine Diagonalmatrix ist.

Beweis. Nach dem Satz ist A genau dann normal, wenn es eine ONB $e_1, \dots, e_n$ von $\mathbb{C}^n$ gibt, die aus Eigenvektoren besteht. Für eine beliebige Basis e_j sind diese Eigenschaften aber äquivalent dazu, dass für die Matrix S mit Spalten $e_1, \dots, e_n$ gilt: S ist unitär und $S^{-1}AS$ ist diagonal. □

Satz 2.8.4. *Sei $\mathbb{K} = \mathbb{C}$. Ein Endomorphismus $T : V \to V$ ist genau dann selbstadjungiert, wenn er normal ist und alle Eigenwerte reell sind. Er ist genau dann unitär, wenn er normal ist und alle Eigenwerte den Betrag 1 haben. Insbesondere existiert in beiden Fällen eine ONB aus Eigenvektoren.*

Beweis. Ist T selbstadjungiert, dann ist T normal und die Eigenwerte sind reell. Sei also umgekehrt T normal mit reellen Eigenwerten. Wegen $\mathrm{Eig}(T, \lambda) = \mathrm{Eig}(T^*, \overline{\lambda})$ und $\lambda = \overline{\lambda}$, stimmen T und T^* auf jedem Eigenraum überein, also sind sie gleich.

Ist T unitär, so ist T normal, weil dann $T^* = T^{-1}$ gilt. ferner haben alle Eigenwerte den Betrag 1. Sei also T normal mit Eigenwerten vom Betrag 1. Dann gilt $\mathrm{Eig}(T, \lambda) = \mathrm{Eig}(T^*, \overline{\lambda}) = \mathrm{Eig}(T^*, \lambda^{-1})$. Daher ist $T^*T = \mathrm{Id}$ auf jedem Eigenraum und damit allgemein. □

Definition 2.8.5. Sei $A \in \mathrm{M}_n(\mathbb{C})$ selbstadjungiert. Dann heisst A *positiv definit*, wenn die hermitesche Form $b(v, w) = \langle Av, w\rangle$ positiv definit ist, wenn also gilt

$$v \neq 0 \quad \Rightarrow \quad \langle Av, v\rangle > 0.$$

Hierbei ist $\langle v, w\rangle = v^t\overline{w}$ das übliche Skalarprodukt auf $\mathbb{C}^n$.

Korollar 2.8.6. *Sei $A \in \mathrm{M}_n(\mathbb{C})$ positiv definit. Dann existiert ein $u \in \mathrm{U}(n)$, so dass*

$$uAu^{-1} = \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix},$$

wobei $a_1, \dots, a_n > 0$ gilt.

Beweis. Nach dem Satz existiert ein u so dass uAu^{-1} Diagonalgestalt hat. Da A positiv definit ist, ist auch uAu^{-1} positiv definit und daher müssen alle Eigenwerte $a_1, \ldots, a_n$ strikt positiv sein. □

2.9 Spektraltheorie über $\mathbb{R}$

In diesem Abschnitt ist $(V, \langle ., . \rangle)$ ein endlich-dimensionaler euklidischer Vektorraum, also $\mathbb{K} = \mathbb{R}$.

Lemma 2.9.1. *Ist $T : V \to V$ linear und symmetrisch, also $T^* = T$, dann hat T einen Eigenvektor in V.*

Beweis. Nach Wahl einer ONB reicht es zu zeigen, dass eine Matrix $A \in \mathrm{M}_n(\mathbb{R})$ mit $A^t = A$ einen reellen Eigenwert zu einem Eigenvektor in $\mathbb{R}^n$ hat. Hierzu fasse A als Element von $\mathrm{M}_n(\mathbb{C})$ auf, dann ist A selbstadjungiert und damit ist jeder Eigenwert von A reell, wir müssen zeigen, dass es einen Eigenvektor in $\mathbb{R}^n$ gibt. Sei $C : \mathbb{C}^n \to \mathbb{C}^n$ die komplexe Konjugation. Dann ist C linear über $\mathbb{R}$, nicht aber über $\mathbb{C}$. Da die Matrix A reell ist, vertauscht sie mit C, es gilt also $AC = CA$. Sei $\lambda \in \mathbb{R}$ ein Eigenwert. Da C mit A vertauscht, wirft C den Eigenraum $U = \mathrm{Eig}(T, \lambda)$ in sich. Wegen $C^2 = \mathrm{Id}$ hat C nur die Eigenwerte ± 1, das Minimalpolynom von C ist $x^2 - 1 = (x + 1)(x - 1)$ und daher ist C diagonalisierbar. Nun ist der C-Eigenraum der 1 gleich $\mathbb{R}^n$ und der -1-Eigenraum gleich $i\mathbb{R}$, deshalb kann nicht jeder Eigenraum von A in $\mathrm{Eig}(C, -1)$ liegen, es muss also einen Eigenraum von A geben, der einen Vektor in $\mathbb{R}^n$ enthält. □

Satz 2.9.2 (Spektralsatz für symmetrische Operatoren)**.** *Ist $\mathbb{K} = \mathbb{R}$ und $T : V \to V$ linear, so sind äquivalent*

(a) *T ist symmetrisch.*

(b) *Es gibt eine ONB aus Eigenvektoren.*

(c) *T ist diagonalisierbar und die Eigenräume stehen senkrecht aufeinander.*

Beweis. (a)⇒(c): Induktion nach der Dimension. Ist $\dim V = 1$, so ist die Behauptung klar. Sei also $\dim V \geq 2$. Nach dem Lemma existiert ein $\lambda \in \mathbb{R}$ mit $U = \mathrm{Eig}(T, \lambda) \neq 0$.

Dann gilt $T(U^\perp) \subset U^\perp$, denn ist $v \in U^\perp$ und $u \in U$, so ist

$$\langle Tv, u\rangle = \langle v, Tu\rangle = 0.$$

Nach Induktionsvoraussetzung ist $U^\perp$ eine orthogonale Summe von Eigenräumen, also gilt dies auch für V.

(c)⇒(b) ist klar, da alle Eigenräume ONBs haben.

(b)⇒(a) Sei $e_1, \dots, e_n$ eine ONB mit $Te_j = \lambda_j e_j$. Dann ist

$$\begin{aligned}\left\langle Te_i, e_j\right\rangle &= \lambda_i \left\langle e_i, e_j\right\rangle = \lambda_i \delta_{i,j} = \lambda_j \delta_{i,j} \\ &= \lambda_j \left\langle e_i, e_j\right\rangle = \left\langle e_i, \lambda_j e_j\right\rangle = \left\langle e_i, Te_j\right\rangle.\end{aligned}$$ □

Beispiel 2.9.3. Sei $A = \begin{pmatrix} 1 & i \\ i & 0 \end{pmatrix} \in \mathrm{M}_2(\mathbb{C})$. Dann ist $A = A^t$, aber A ist nicht normal, denn

$$\begin{aligned}AA^* &= \begin{pmatrix} 1 & i \\ i & 0 \end{pmatrix}\begin{pmatrix} 1 & -i \\ -i & 0 \end{pmatrix} = \begin{pmatrix} 2 & -i \\ i & 1 \end{pmatrix}, \\ A^*A &= \begin{pmatrix} 1 & -i \\ -i & 0 \end{pmatrix}\begin{pmatrix} 1 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 2 & i \\ -i & 1 \end{pmatrix}.\end{aligned}$$

Definition 2.9.4. Sei $\mathrm{O}(n) = \mathrm{M}_n(\mathbb{R}) \cap \mathrm{U}(n)$ die Menge aller reellen Matrizen A mit $AA^t = A^tA = I$. Die Menge $O(n)$ der orthogonalen Matrizen ist eine Untergruppe von $\mathrm{GL}_n(\mathbb{R})$.

Korollar 2.9.5 (Spektralsatz für symmetrische Matrizen)**.** *Eine Matrix $A \in \mathrm{M}_n(\mathbb{R})$ it genau dann symmetrisch, wenn es eine Matrix $S \in \mathrm{O}(n)$ gibt so dass $S^{-1}AS$ diagonal ist.*

Beweis. Nach dem Satz ist A genau dann symmetrisch, wenn es eine ONB aus Eigenvektoren $(e_1, \dots, e)n$ gibt. Die Matrix S mit den Spalten $e_1, \dots, e_n$ leistet das Gewünschte. Ist umgekehrt S gegeben, so bilden die Spalten von S eine ONB aus Eigenvektoren. □

Warnung. Eine symmetrische Matrix in $\mathrm{M}_n(\mathbb{R})$ ist immer über $\mathbb{R}$ diagonalisierbar. Für eine orthogonale Matrix gilt das nicht, wie das Beispiel $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ zeigt.

Definition 2.9.6. Eine symmetrische Matrix $A \in \mathrm{M}_n(\mathbb{R})$ heisst *positiv definit*, wenn die symmetrische Bilinearform $(v, w) \mapsto \langle Av, w\rangle = (Av)^t w = v^t Aw$ positiv definit ist.

Korollar 2.9.7. *Sei $A \in \mathrm{M}_n(\mathbb{R})$ positiv definit. Dann existiert ein $k \in \mathrm{O}(n)$, so dass*

$$kAk^{-1} = \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix},$$

wobei $a_1, \ldots, a_n > 0$ gilt.

Beweis. Nach Korollar 2.9.5 existiert ein $k = in\,\mathrm{O}(n)$ so dass kAk^{-1} Diagonalgestalt hat. Da A positiv definit ist, ist auch kAk^{-1} positiv definit und daher müssen alle Eigenwerte $a_1, \ldots, a_n$ strikt positiv sein. □

2.10 Iwasawa- und Cartan-Zerlegung

Sei $n \in \mathbb{N}$ und seien

$$A = \left\{ \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix} : a_1, \ldots, a_n > 0 \right\},$$

$$N = \left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ & & 1 \end{pmatrix} \in \mathrm{GL}_n(\mathbb{R}) \right\},$$

$$K = O(n) = \{k \in \mathrm{M}_n(\mathbb{R}) : k^t k = I\}.$$

Satz 2.10.1 (Iwasawa-Zerlegung)**.** *Die Abbildung*

$$A \times N \times K \to \mathrm{GL}_n(\mathbb{R}),$$
$$(a, n, k) \mapsto ank$$

ist eine Bijektion. Also ist jedes $g \in \mathrm{GL}_n(\mathbb{R})$ eindeutig schreibbar als $g = ank$ mit $a \in A$, $n \in N$, $k \in K$.

Beweis. Sei $g \in G = \mathrm{GL}_n(\mathbb{R})$. Sei $e_1, \ldots, e_n$ die Standard-Basis von $\mathbb{R}^n$. Da g invertierbar ist, ist $ge_n, \ldots, ge_n$ ebenfalls eine Basis von $\mathbb{R}^n$. Wir wenden das

Orthonormalisierungsverfahren aus Satz 2.5.1 auf diese Basis an und erhalten eine ONB $f_1, \ldots, f_n$ mit der Eigenschaft, dass

$$\text{Spann}(ge_1, \ldots, ge_k) = \text{Spann}(f_1, \ldots, f_k),$$

was gerade bedeutet, dass die Basiswechselmatrix von (ge_j) nach (f_j) eine obere Dreiecksmatrix ist. Ausserdem hat sie positive Diagonaleinträge, wie man dem Orthonormalisierungsverfahren ansieht. Die Vorschrift $ke_j = f_j$ definiert ein Element k von $\mathrm{O}(n)$ und die Matrix $S = kg^{-1}$ ist eine obere Dreiecksmatrix mit positiven Diagonaleinträgen, kann also in der Form $S = (an)^{-1}$ geschrieben werden mit $a \in A$ und $n \in N$. Wir erhalten $kg^{-1} = (an)^{-1}$ oder $gk^{-1} = an$ oder $g = ank$, womit die Surjektivität gezeigt ist. Für die Injektivität sei $ank = a'n'k'$, dann ist die obere Dreiecksmatrix $(an)^{-1}a'n'$ gleich der orthogonalen Matrix $k(k')^{-1}$, was nur sein kann, wenn beide die Einheitsmatrix sind. □

Satz 2.10.2 (Cartan-Zerlegung)**.** *Sei A^+ die Menge aller Diagonalmatrizen a in A, deren Einträge der Größe nach geordnet sind, also $a = \mathrm{diag}(a_1, \ldots, a_n)$ mit $a_1 \leq a_2 \leq \cdots \leq a_n$. Dann gilt $\mathrm{GL}_n(\mathbb{R}) = KA^+K$. Genauer kann jedes $g \in \mathrm{GL}_n(\mathbb{R})$ in der Form $g = k_1ak_2$ geschrieben werden, wobei $k_1, k_2 \in K$ und $a \in A^+$. Hierbei ist a eindeutig durch g festgelegt.*

Beweis. Sei $g \in \mathrm{GL}_n(\mathbb{R})$. Die symmetrische Matrix gg^t ist positiv definit, also gibt es ein $a \in A$ so dass $gg^t = kak^t$ geschrieben werden kann. Die Reihenfolge der Matrixeinträge von a kann durch Konjugation mit einer Permutationsmatrix $a \mapsto PaP^{-1}$ geändert werden. Da aber $P \in K$, kann man also annehmen, dass $a \in A^+$. Jedes $a \in A^+$ kann als $a = b^2$ für ein $b \in A^+$ geschrieben werden, wir können also annehmen, dass $gg^t = ka^2k^t = (ka)(ka)^t$ gilt. Sei $h = (ka)^{-1}g$, dann folgt $hh^t = (ka)^{-1}g[(ka)^{-1}g]^t = (ka)^{-1}gg^t(ka)^{-t} = I$. Damit folgt $h \in \mathrm{O}(n) = K$, also haben wir $g = kah$ in der gewünschten Form geschrieben. Die Eigenwerte von a sind dann genau die Quadratwurzeln der Eigenwerte von gg^t, also durch g eindeutig festgelegt. □

3 Multilineare Algebra

In diesem Abschnitt ist K wieder ein beliebiger Körper.

3.1 Tensorprodukt

Definition 3.1.1. Seien U, V, W Vektorräume über K. Eine Abbildung $b : V \times W \to U$ heißt *bilinear*, falls

- $v \mapsto b(v, w)$ ist linear für jedes feste $w \in W$ und
- $w \mapsto b(v, w)$ ist linear für jedes feste $v \in V$.

Wir schreiben $\mathrm{Bil}(V \times W, U)$ für den Vektorraum aller bilinearen Abbildungen $V \times W \to U$.

Beispiele 3.1.2.

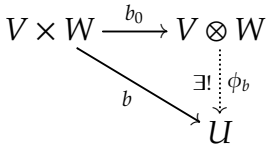
- Bilinearformen sind bilineare Abbildungen.
- Das Matrixprodukt $\mathrm{M}_{m\times n} \times \mathrm{M}_{n\times p} \to \mathrm{M}_{m\times p}$ ist bilinear.
- Die Kommutator-Klammer $[.,.]\,\mathrm{M}_n \to \mathrm{M}_n$, gegeben durch

$$[A, B] = AB - BA$$

  ist bilinear.

Satz 3.1.3. *Zu gegebenen Vektorräumen V und W gibt es einen Vektorraum $V \otimes W$ und eine bilineare Abbildung $b_0 : V \times W \to V \otimes W$ mit der folgenden universellen Eigenschaft:*

Ist $b : V \times W \to U$ eine bilineare Abbildung, dann existiert genau eine lineare Abbildung $\phi_b : V \otimes W \to U$ so dass das Diagramm



kommutiert. Diese universelle Eigenschaft legt den Raum $V \otimes W$ und die universelle Bilinearform b_0 bis auf Isomorphie eindeutig fest.

Diese universelle Eigenschaft induziert einen linearen Isomorphismus

$$\mathrm{Bil}(V \times W, U) \xrightarrow{\cong} \mathrm{Lin}(V \otimes W, U).$$

Wir nennen den Raum $V \otimes W$ das Tensorprodukt *von V und W und schreiben $v \otimes w \in V \otimes W$ für das Element $b_0(v, w)$.*

Beweis. Wir wählen eine Konstruktion, die die universelle Eigenschaft erzwingt. Wir erinnern uns, dass es zu jeder Mächtigkeit einen Vektorraum V mit einer Basis der gegebenen Mächtigkeit gibt. Eine mögliche Konstruktion eines solchen Raumes ist diese: Für eine beliebige Menge $S \neq 0$ sei $K[S]$ der Vektorraum der formalen Summen

$$\sum_{s \in S} \lambda_s s, \quad \lambda_s \in K, \text{ fast alle Null.}$$

Dies wird ein Vektorraum durch

$$\sum_{s \in S} \lambda_s s + \sum_{s \in S} \mu_s s = \sum_{s \in S} (\lambda_s + \mu_s) s, \qquad \lambda \sum_{s \in S} \lambda_s s = \sum_{s \in S} \lambda \lambda_s s.$$

Genauer kann man $K[S]$ auch als die Menge aller Abbildungen $S \to K$, $s \mapsto \lambda_s$ auffassen, die für fast alle s verschwinden.

Ist nun $f : S \to V$ eine beliebige Abbildung, kann man sie in eindeutiger Weise zu einer linearen Abbildung $K[S] \to V$ verlängern, indem man $f\left(\sum_{s \in S} \lambda_s s\right) = \sum_{s \in S} \lambda_s f(s)$ setzt.

Nun zur Situation des Satzes, sei also $b : V \times W \to U$ bilinear und betrachte den Raum $K[V \times W]$. Sei R der Unterraum erzeugt von allen Vektoren der Form

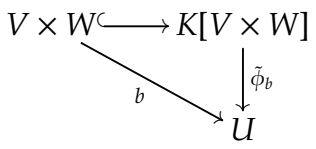
$$(\lambda v + \mu v', w) - \lambda(v, w) - \mu(v', w) \quad \text{oder} \quad (v, \lambda w + \mu w') - \lambda(v, w) - \mu(v, w'),$$

wobei $\lambda \in K$, sowie $v, v' \in V$ und $w, w' \in W$. Wir definieren das Tensorprodukt als den Quotientenraum:

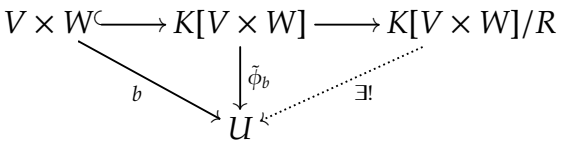
$$V \otimes W = K[V \times W]/R.$$

Wir schreiben die Klasse von (v, w) in $V \otimes W$ als $v \otimes w$. Sei nun $b : V \times W \to U$ bilinear

und sei $\tilde{\phi}_b : K[V \times W] \to U$ die lineare Verlängerung von b, d.h., das Diagramm



kommutiert. Da b bilinear ist, liegt R im Kern von $\tilde{\phi}_b$ und daher existiert genau eine lineare Abbildung $\phi_b : V \otimes W \to U$, die das Diagramm des Satzes kommutativ macht.



Die Eindeutigkeit folgt mit dem üblichen Geplänkel universeller Eigenschaften. □

Ein beliebiges Element $z \in V \otimes W$ eines Tensorprodukts lässt sich immer als Summe schreiben

$$z = \sum_{j=1}^{m} v_j \otimes w_j,$$

mit Vektoren $v_j \in V$ und $w_j \in W$. Die Elemente, die sich in der Form $v \otimes w$ schreiben lassen werden *reine Tensoren* genannt.

Proposition 3.1.4. *Ist $(v_i)_{i\in I}$ eine Basis von V und ist $(w_j)_{j\in J}$ eine Basis von W, dann ist*

$$(v_i \otimes w_j)_{(i,j)\in I\times J}$$

eine Basis von $V \otimes W$.

Sind V und W endlich-dimensional, so hat der Raum $V \otimes W$ die Dimension

$$\dim V \otimes W = (\dim V)(\dim W).$$

Beweis. Wir zeigen zunächst, dass die Familie $(v_i \otimes w_j)$ linear unabhängig ist. Sei also

$$\sum_{i\in I}\sum_{j\in J} \lambda_{i,j} v_i \otimes w_j = 0$$

eine Linearkombination der Null in $V \otimes W$. Hier sind fast alle $\lambda_{i,j}$ gleich Null. Sei

$\alpha : V \to K$ eine Linearform, die lineare Abbildung

$$\begin{aligned} \alpha \times 1 : K[V \times W] &\to W, \\ (v, w) &\mapsto \alpha(v)w \end{aligned}$$

wirft R auf die Null, also existiert eine eindeutig bestimmte lineare Abbildung

$$\begin{aligned} \alpha \otimes 1 : V \otimes W &\to W, \\ v \otimes w &\mapsto \alpha(v)w. \end{aligned}$$

Wir wenden diese Abbildung auf die Linearkombination der Null an und erhalten

$$0 = \sum_{j \in J} \left(\sum_{i \in I} \lambda_{i,j} \alpha(v_i) \right) w_j$$

Da die w_j linear unabhängig sind, folgt für gegebenes $j \in J$,

$$\alpha \left(\sum_{i \in I} \lambda_{i,j} v_i \right) = \sum_{i \in I} \lambda_{i,j} \alpha(v_i) = 0$$

für jede Linearform α. Damit ist aber $\sum_{i \in I} \lambda_{i,j} v_i = 0$ und da die v_i linear unabhängig sind, ist $\lambda_{i,j} = 0$ für alle i, j. Dies ist die Lineare Unabhängigkeit. Es bleibt zu zeigen, dass $(v_i \otimes w_j)$ ein Erzeugendensystem ist. Dies ist aber klar, da $K[V \times W]$ durch alle (v, w) mit $v \in V$ und $w \in W$ erzeugt wird. □

Beispiele 3.1.5.

- Wir können $\mathbb{C}$ als Vektorraum über $\mathbb{R}$ auffassen. Für einen beliebigen $\mathbb{R}$-Vektorraum V sei dann

  $$V_{\mathbb{C}} = \mathbb{C} \otimes_{\mathbb{R}} V.$$

  Dann ist $V_{\mathbb{C}}$ natürlich isomorph zu der Komplexifizierung von V, die in Abschnitt 1.2 definiert wurde.

- Allgemeiner seien $L \supset K$ zwei Körper. Wir fassen L als K-Vektorraum auf und definieren

  $$V_L = L \otimes_K V$$

  für einen beliebigen K-Vektorraum V.

Proposition 3.1.6. *Sind $S : V \to V'$ und $T : W \to W'$ lineare Abbildungen, so induzieren*

sie eine lineare Abbildung

$$S \otimes T : V \otimes W \to V' \otimes W',$$

gegeben durch

$$(S \otimes T)(v \otimes w) = Sv \otimes Tw.$$

Beweis. Die Abbildung $b : V \times W \to V' \otimes W'$ gegeben durch $b(v, w) = Sv \otimes Tw$ ist bilinear, faktorisiert also eindeutig über eine lineare Abbildung $V \otimes W \to V' \otimes W'$ die wir $S \otimes T$ nennen und die das Gewünschte leistet. □

Beispiel 3.1.7. Seien in der Proposition $V = W = V' = W' = K^2$. Seien S und T in der standard Basis durch die Matrizen $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ und $B = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ gegeben. In der Basis $e_1 \otimes e_1, e_1 \otimes e_2, e_2 \otimes e_1, e_2 \otimes e_2$ von $V \otimes W$ ist dann $S \otimes W$ durch die Matrix

$$\begin{pmatrix} a\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} & b\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \\ c\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} & d\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \end{pmatrix} = \begin{pmatrix} a\alpha & a\beta & b\alpha & b\beta \\ a\gamma & a\delta & b\gamma & b\delta \\ c\alpha & c\beta & d\alpha & d\beta \\ c\gamma & c\delta & d\gamma & d\delta \end{pmatrix}$$

gegeben.

Satz 3.1.8. *Seien V, W endlich-dimensionale K-Vektorräume und $A, A' : V \to V$ und $B, B' : W \to W$ linear. Dann gilt*

$$(A \otimes B)(A' \otimes B') = AA' \otimes BB'$$

sowie

$$\operatorname{tr}(A \otimes B) = \operatorname{tr}(A) \operatorname{tr}(B)$$

und

$$\det(A \otimes B) = \det(A)^m \det(B)^n,$$

wobei $n = \dim V$ und $m = \dim W$.

Proof. Für $v \in V$ und $w \in W$ gilt

$$(A \otimes B)(A' \otimes B')(v \otimes w) = (A \otimes B)(A'v \otimes B'w) = AA'(v) \otimes BB'(w).$$

Damit stimmen die beiden Seiten für reine Tensoren überein und da beide Seiten lineare Abbildungen sind, stimmen sie überall überein. Die Formel für die Spur sieht man am Kronecker-Produkt und für die Determinante benutzt man $\det(A \otimes B) = \det((A \otimes I)(I \otimes B)) = \det(A \otimes I)\det(I \otimes B)$. Man sieht etwa $\det(A \otimes I) = \det(A)^m$ wieder am Kronecker-Produkt. □

Satz 3.1.9. *Seien V, W endlich-dimensionale K-Vektorräume und sei V^* der Dualraum von V. Die Abbildung*

$$\begin{aligned} \psi : V^* \otimes W &\to \mathrm{Lin}(V, W), \\ (\alpha, w) &\mapsto [v \mapsto \alpha(v)w] \end{aligned}$$

ist eine lineare Bijektion.

Beweis. Die Abbildung $V^* \times W \to \mathrm{Lin}(V, W)$, $(\alpha, w) \mapsto \psi(\alpha, w)$ ist bilinear, daher verlängert sie zu einer linearen Abbildung wie im Satz. Die Dimensionen der beiden Räume sind gleich, daher reicht es zu zeigen, dass die Abbildung ψ surjektiv ist. Seien $v_1, \ldots, v_n$ und $w_1, \ldots, w_m$ Basen von V und W und sei $v_1^*, \ldots, v_n^*$ die duale Basis von V^*. Ist $T : V \to W$ in diesen Basen durch die Matrix $A = (a_{i,j})$ gegeben und ist $v = \sum_{j=1}^n \lambda_j v_j$ dann gilt

$$T\left(\sum_{j=1}^n \lambda_j v_j\right) = \sum_{j=1}^n \sum_{i=1}^m \lambda_j a_{i,j} w_i.$$

Nun ist $\lambda_j = v_j^*(v)$, also haben wir $T(v) = \sum_{j=1}^n \sum_{i=1}^m v_j^*(v) a_{i,j} w_i$ oder

$$T = \sum_{j=1}^n \sum_{i=1}^m a_{i,j} v_j^* w_i = \sum_{j=1}^n \sum_{i=1}^m a_{i,j} \psi(v_j^* \otimes w_j) = \psi\left(\sum_{j=1}^n \sum_{i=1}^m a_{i,j} v_j^* \otimes w_j\right). \qquad \square$$

3.2 Die zweite äussere Potenz

Definition 3.2.1. Eine bilineare Abbildung $b : V \times V \to W$ heißt *symmetrisch*, falls

$$b(v, w) = b(w, v)$$

und *alternierend*, falls

$$b(v, v) = 0$$

für alle $v, w \in V$ gilt.

Lemma 3.2.2. (a) *Ist b alternierend, so gilt*

$$b(v, w) = -b(w, v)$$

für alle $v, w \in V$.

(b) *Ist* $\mathrm{Char}(K) \neq 2$ *und ist b sowohl symmetrisch als auch alternierend, dann ist $b = 0$.*

Beweis. (a) Es gilt

$$0 = b(v + w, v + w) = b(v, v) + b(v, w) + b(w, v) + b(w, w) = b(v, w) + b(w, v).$$

(b) Folgt aus $b(v, w) = b(w, v) = -b(v, w)$. □

Definition 3.2.3. Sei $S_2(V)$ der Unterraum von $V \otimes V$ aufgespannt von allen Vektoren der Form

$$v \otimes w - w \otimes v.$$

Sei $A_2(V)$ der Unterraum aufgespannt von allen Vektoren der Form

$$v \otimes v.$$

Lemma 3.2.4. *Sei $\phi_b : V \otimes V \to W$ die lineare Abbildung induziert durch die bilineare Abbildung $b : V \times V \to W$. Dann gilt*

$$\begin{aligned} b \text{ symmetrisch} &\Leftrightarrow S_2(V) \subset \ker \phi_b \\ b \text{ alternierend} &\Leftrightarrow A_2(V) \subset \ker \phi_b \end{aligned}$$

Beweis. Dies folgt sofort aus

$$b(v, w) - b(w, v) = \phi(v \otimes w - w \otimes v)$$

und

$$b(v, v) = \phi(v \otimes v)$$

□

Definition 3.2.5. Wir schreiben

$$\mathrm{Alt}(V \times V, W)$$

für den Vektorraum aller alternierenden Abbildungen $a : V \times V \to W$.

Satz 3.2.6. *Für jeden K-Vektorraum V gibt es einen Vektorraum $\bigwedge^2 V$ mit einer alternierenden Abbildung*

$$\wedge : V \times V \to \bigwedge^2 V,$$

die die folgende universelle Eigenschaft haben: Zu jeder alternierenden Abbildung

$$a : V \times V \to W$$

gibt es genau eine lineare Abbildung $\psi_a : \bigwedge^2 V \to W$ so dass das Diagramm

$$\begin{array}{ccc} V \times V & \xrightarrow{\wedge} & \bigwedge^2 V \\ & \searrow^{a} & \downarrow{\scriptstyle \psi_a} \\ & & W \end{array}$$

kommutiert. Diese universelle Eigenschaft induziert einen linearen Isomorphismus

$$\mathrm{Alt}(V \times V, W) \xrightarrow{\cong} \mathrm{Lin}(\bigwedge^2 V, W).$$

Beweis. Definiere

$$\bigwedge^2 V := V \otimes V / A_2(V).$$

Für $v, w \in V$ sei $v \wedge w = [v \otimes w]$ die Nebenklasse von $v \otimes w$. Zur universellen Eigenschaft: Sei $a : V \times V \to W$ alternierend und sei $\phi_a : V \times V \to W$ die lineare Abbildung gemäß Satz 3.1.3. Nach Lemma 3.2.4 liegt $A_2(V)$ im Kern von ϕ_a, so dass ϕ_a in eindeutiger Weise über eine lineare Abbildung $\psi_a : \bigwedge^2 V \to W$ faktorisiert. □

Lemma 3.2.7. *Ist $v_1, \ldots, v_n$ eine Basis von V, so ist $(v_i \wedge v_j) 1 \leq i < j \leq n$ eine Basis von $\bigwedge^2 V$. Es folgt*

$$\dim \bigwedge^2 V = \begin{pmatrix} n \\ 2 \end{pmatrix} = \tfrac{n(n-1)}{2}.$$

Beweis. Da $(v_i \otimes v_j)_{1 \leq i,j \leq n}$ ein Erzeugendensystem von $V \otimes V$ ist, ist $(v_i \wedge v_j)_{1 \leq i,j \leq n}$ ein Erzeugendensystem von $\bigwedge^2 V$. Da $v_i \wedge v_i = 0$ und $v_i \wedge v_j = -v_j \wedge v_i$, ist $(v_i \wedge v_j)_{1 \leq i < j \leq n}$

ein Erzeugendensystem von $\bigwedge^2 V$. Es reicht demnach, die Dimensionsaussage zu zeigen. Sei K^N mit $N = \begin{pmatrix} n \\ 2 \end{pmatrix}$ der Vektorraum mit der Basis $(e_{i,j})_{1 \le i < j \le n}$. Wir konstruieren eine alternierende Abbildung $a : V \times V \to K^N$ wie folgt: Sind

$$v = \sum_{i=1}^{n} \lambda_i v_i \quad \text{und} \quad w = \sum_{j=1}^{n} \mu_j v_j,$$

so setze $a_{i,j} = \lambda_i \mu_j - \lambda_j \mu_i$. Definiere dann

$$a(v, w) = \sum_{1 \le i < j \le n} a_{i,j} e_{i,j}.$$

Diese Abbildung ist alternierend und es gilt für $i < j$,

$$\psi_a(v_i \wedge v_j) = a(v_i, v_j) = e_{i,j}.$$

Damit ist $\psi_a : \bigwedge^2 V \to K^N$ surjektiv und daher ist dim $\bigwedge^2 V \ge N$. Da die $v_i \wedge v_j$ den Raum $\bigwedge^2 V$ erzeugen, gilt $\le$, insgesamt also "=". □

Rechenregeln für das Hut-Produkt:

- $(u + v) \wedge w = u \wedge w + v \wedge w$,
- $u \wedge (v + w) = u \wedge v + u \wedge w$,
- $\lambda(v \wedge w) = (\lambda v) \wedge w = v \wedge (\lambda w)$,
- $v \wedge v = 0, \quad v \wedge w = -w \wedge v$.

3.3 Multilineare Abbildungen

Seien $V_1, \ldots, V_k, W$ Vektorräume über K. Eine Abbildung

$$m : V_1 \times \cdots \times V_k \to W$$

heißt *multilinear*, falls für jedes $1 \le j \le n$ und für fest gewählte Vektoren $v_i \in V$ für $i \ne j$ die Abbildung

$$v \mapsto m(v_1, \ldots, v_{j-1}, v, v_{j+1}, \ldots, v_n)$$

linear ist.

Beispiele 3.3.1.

- Sei $V = K^n$, dann ist die Determinante

$$\det : V \times \cdots \times V \to K$$

eine multilineare Abbildung.

- Die Abbildung

$$\begin{aligned} V_1 \times, \cdots \times V_k &\to V_1 \otimes (V_2 \otimes \cdots \otimes (V_{k-1} \otimes V_k) \dots) \\ (v_1, \dots, v_k) &\mapsto v_1 \otimes \cdots \otimes v_k \end{aligned}$$

ist multilinear.

Wir haben natürliche Isomorphismen

$$(U \otimes V) \otimes W \xrightarrow{\cong} U \otimes V \otimes W \xrightarrow{\cong} U \otimes (V \otimes W)$$

gegeben durch $(u \otimes v) \otimes w \mapsto u \otimes (v \otimes w)$, so dass die Reihenfolge der Klammern letztlich irrelevant ist. Wir können allerdings auch mehrfache Tensorprodukte unabhängig definieren.

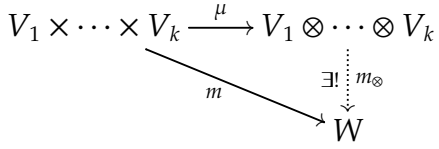
Satz 3.3.2. *Zu gegebenen Vektorräumen $V_1, \dots, V_k$ gibt es einen Vektorraum $V_1 \otimes \cdots \otimes V_k$ und eine multilineare Abbildung*

$$\begin{aligned} \mu : V_1 \times \cdots \times V_k &\to V_1 \otimes \cdots \otimes V_k, \\ (v_1, \dots, v_k) &\mapsto v_1 \otimes \cdots \otimes v_k, \end{aligned}$$

so dass es zu jeder multilinearen Abbildung

$$m : V_1 \times \cdots \times V_k \to W$$

genau eine lineare Abbildung $m_\otimes : V_1 \otimes \cdots \otimes V_k \to W$ gibt, so dass das Diagramm



kommutiert. Die Abbildung $m \mapsto m_\otimes$ ist eine lineare Bijektion

$$\mathrm{Mult}_k(V_1 \times \cdots \times V_k, W) \xrightarrow{\cong} \mathrm{Lin}(V_1 \otimes \cdots \otimes V_k, W).$$

Beweis. Man wiederholt die Konstruktion aus dem Produkt zweier Räume, definiert also $V_1 \otimes \cdots \otimes V_k$ als Quotient des freien Raums $K[V_1 \times \cdots \times V_k]$ und do fort. Die Details seien dem Leser überlassen. □

Definition 3.3.3. Eine multilineare Abbildung $m : V^k \to U$ heißt *symmetrisch*, falls

$$m(v_{\sigma(1)}, \ldots, v_{\sigma(k)}) = m(v_1, \ldots, v_k)$$

für jede Permutation $\sigma \in \mathrm{Per}(n)$ gilt.

Sie heißt *alternierend*, wenn

$$m(v_1, \ldots, v_k) = 0,$$

falls $v_i = v_j$ für ein i und ein $j \neq i$.

Lemma 3.3.4. *Ist m alternierend, dann gilt*

$$m(v_{\sigma(1)}, \ldots, v_{\sigma(k)}) = \mathrm{sign}(\sigma) m(v_1, \ldots, v_k) \qquad (*)$$

für jede Permutation $\sigma \in \mathrm{Per}(n)$. Ist $\mathrm{Char}(K) \neq 2$, so folgt aus (*) für alle σ schon, dass m alternierend ist.

Beweis. Ist $\sigma = \tau_{i,j}$ eine Transposition so gilt

$$\begin{aligned} 0 &= m(v_1, \ldots, \underbrace{v_i + v_j}_{i\text{-te Stelle}}, \ldots, \underbrace{v_i + v_j}_{j\text{-te Stelle}}, \ldots, v_k) \\ &= m(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_k) + m(v_1, \ldots, v_j, \ldots, v_i, \ldots, v_k). \end{aligned}$$

□

Damit folgt die Behauptung falls σ eine Transposition ist. Für die allgemeine Aussage schreibt man σ als Produkt von Transpositionen und zieht bei jeder Transposition einen Faktor (-1) heraus.

Beispiele 3.3.5.

- Ist $V = K^n$, so ist die Determinante $\det : V^n \to K$ alternierend.

- Ist $V = K$, so ist die Abbildung $m : V^k \to K$, gegeben durch $m(a_1, \ldots, a_k) = a_1 \cdots a_k$ symmetrisch.

3.4 Die äußere Algebra

Definition 3.4.1. Eine *Algebra* über dem Körper K ist ein K-Vektorraum A zusammen mit einer bilinearen Abbildung

$$\begin{aligned} A \times A &\to A \\ (a, b) &\mapsto ab, \end{aligned}$$

die *assoziativ* ist, d.h., es gilt

$$(ab)c = a(bc)$$

für alle $a, b, c \in A$. Wir sagen, die Algebra A hat eine *Eins* oder ist eine *Algebra mit Eins*, oder eine *unitale Algebra*, falls es ein Element 1_A in A gibt mit der Eigenschaft

$$1_A a = a 1_A = a$$

für jedes $a \in A$. In dieser Vorlesung betrachten wir nur Algebren mit Eins! Deshalb gilt ab jetzt die **Sprachkonvention, dass Algebra immer Algebra mit Eins heissen soll. Andernfalls sprechen wir von einer *Algebra ohne Eins*.**

Das Einselement ist eindeutig bestimmt, denn ist $1'$ ein zweites Einselement, dann gilt

$$1' = 1' 1_A = 1_A.$$

Beispiele 3.4.2.

- Ist A irgendein K-Vektorraum, dann macht die Nullmultiplikation $ab = 0$ den Raum A zu einer Algebra ohne Eins!
- Der Körper K selbst ist eine K-Algebra.
- $\mathrm{M}_n(K)$ ist mit dem Matrixprodukt eine Algebra mit Eins.
- Ist V irgendein Vektorraum (auch unendlich-dimensional), dann ist die Menge

  $$\mathrm{End}(V) = \mathrm{Lin}(V, V)$$

  eine Algebra mit der Komposition als Multiplikation.

- Ist S eine Menge und ist $A = \mathrm{Abb}(S, K)$ der Vektorraum aller Abbildungen von S nach K. Dann ist A eine Algebra mit dem punktweisen Produkt:

$$fg(s) = f(s)g(s), \qquad s \in S.$$

- Über dem Körper $\mathbb{R}$ der reellen Zahlen betrachtet man die *Quaternionenalgebra* $\mathbb{H}$, dies ist ein vierdimensionaler $\mathbb{R}$-Vektorraum mit einer Basis $\mathbf{1}, i, j, k$. Die Relationen

$$\mathbf{1}x = x\mathbf{1} = x \qquad i^2 = j^2 = -1 \qquad ij = k = -ji$$

definieren eine Algebrenstruktur auf $\mathbb{H}$. Dies ist eine Algebra mit Eins. Diese Algebra ist nichtkommutativ, aber dennoch ist jedes Element $\neq 0$ invertierbar, es handelt sich also um einen sogenannten *Schiefkörper*.

Beweis. Die Tatsache, dass $\mathbb{H}$ in der Tat die Axiome einer Algebra erfüllt, muss man nachrechnen. Bei der Assoziativität reicht es, diese auf den Basiselementen nachzuweisen. Wir zeigen, dass jedes Element $\neq 0$ invertierbar ist. Zunächst stellen wir fest, dass

$$ik = iij = -j \quad \text{und} \quad ki = iji = -iij = j$$

gilt und ebenso $jk = i = -kj$. Für ein Quaternion $z = a + bi + cj + dk$ sei $\overline{z} = a - bi - cj - dk$ definiert. Es folgt

$$\begin{aligned} z\overline{z} &= (a + bi + cj + dk)(a - bi - cj - dk) \\ &= a^2 - abi - acj - adk + abi + b^2 - bck + bdj \\ &\quad + acj + bck + c^2 - cdi + adk - bdj + cdi \\ &= a^2 + b^2 + c^2 + d^2. \end{aligned}$$

Ist $z \neq 0$, dann ist $a^2 + b^2 + c^2 + d^2 \neq 0$ und also ist dann

$$\frac{1}{a^2 + b^2 + c^2 + d^2}\overline{z}$$

ein Inverses zu z. □

Sei V ein K-Vektorraum. Wir schreiben $\bigotimes^k V$ oder $V^{\otimes k}$ für das Tensorprodukt

$V \otimes \cdots \otimes V$ mit k Faktoren. Seien

$$S_k(V) := \text{Spann}\left\{v_1 \otimes \cdots \otimes v_k - v_{\sigma(1)} \otimes v_{\sigma(k)} : \sigma \in \text{Per}(k)\right\}$$
$$A_k(V) := \text{Spann}\left\{v_1 \otimes \cdots \otimes v_k : v_i = v_j \text{ für ein Paar } i \neq j\right\}.$$

Lemma 3.4.3. *Ist $m : V^k \to W$ multilinear, dann gilt*

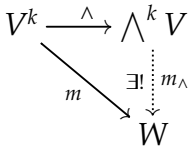
$$\begin{aligned} m \text{ symmetrisch} &\quad\Leftrightarrow\quad S_k(V) \subset \ker(m_\otimes), \\ m \text{ alternierend} &\quad\Leftrightarrow\quad A_k(V) \subset \ker(m_\otimes). \end{aligned}$$

Beweis. Analog zum Beweis von Lemma 3.2.4. □

Satz 3.4.4. *Zu einem Vektorraum V und $k \in \mathbb{N}$ existiert ein Vektorraum $\bigwedge^k V$ und eine alternierende Abbildung*

$$\wedge : V^k \to \bigwedge^k V$$

so dass für jede alternierende Abbildung $m : V^k \to W$ eine eindeutig bestimmte lineare Abbildung $m_\wedge : \bigwedge^k V \to W$ existiert so dass das Diagramm



kommutiert. Die Abbildung $m \mapsto m_\wedge$ ist ein linearer Isomorphismus

$$\text{Alt}_k(V^k, W) \xrightarrow{\cong} \text{Lin}(\bigwedge^k V, W).$$

Beweis. Setze

$$\bigwedge^k V := V^{\otimes k}/A_k(V)$$

und

$$\wedge : v_1 \otimes \otimes v_k \mapsto [v_1 \otimes \cdots \otimes v_k] =: v_1 \wedge \cdots \wedge v_k.$$

Der Beweis ist nun analog zum Beweis von Satz 3.2.6. □

Satz 3.4.5. *Ist $v_1, \dots, v_n$ eine Basis von V, dann ist*

$$(v_{i_1} \wedge \cdots \wedge v_{i_k})_{1 \le i_1 < \cdots < i_k \le n}$$

eine Basis von $\bigwedge^k V$. Insbesondere ist

$$\dim \bigwedge^k V = \begin{pmatrix} n \\ k \end{pmatrix}$$

und damit insbesondere $\bigwedge^k V = 0$ falls $k > n$.

Beweis. Die angegebene Familie ist ein Erzeugendensystem. Es reicht also, die Dimensionsaussage für $1 \le k \le n$ zu zeigen. Hierzu sei $W = K^N$ mit $N = \begin{pmatrix} n \\ k \end{pmatrix}$ mit Basis

$$e_{i_1,\dots,i_k}, \qquad 1 \le i_1 < \cdots < i_k \le n.$$

Fixiere eine Basis $v_1, \dots, v_n$ von V und sei $m : V^k \to K^N$ gegeben durch

$$m(w_1, \dots, w_k) = \sum_{1 \le i_1 < \cdots < i_k \le n} a_{i_1,\dots,i_k} e_{i_1,\dots,i_k},$$

wobei

$$a_{i_1,\dots,i_k} = a_{i_1,\dots,i_k}(w_1, \dots, w_k)$$

definiert ist wie folgt: Ist $w_j = \sum_{i=1}^n \lambda_{i,j} v_i$, dann sei

$$a_{i_1,\dots,i_k} = \det \begin{pmatrix} \lambda_{1,i_1} & \dots & \lambda_{1,i_k} \\ \vdots & & \vdots \\ \lambda_{k,i_1} & \dots & \lambda_{k,i_k} \end{pmatrix}.$$

Es folgt dann

$$m(v_{i_1}, \dots, v_{i_k}) = e_{i_1,\dots,i_k},$$

also $\dim \bigwedge^k V \ge N$. □

Definition 3.4.6. Sei $n = \dim V$, so setze

$$\bigwedge V = \bigoplus_{p=0}^{n} \bigwedge^p V,$$

wobei $\bigwedge^0 V = K$ gesetzt wird. Die kanonische Abbildung

$$\bigwedge^p V \times \bigwedge^q V \to \bigwedge^{p+q} V$$
$$((v_1 \wedge \cdots \wedge v_k), (w_1 \wedge \cdots \wedge w_k)) \mapsto v_1 \wedge \cdots \wedge v_k \wedge w_1 \wedge \cdots \wedge w_k$$

definiert durch bilineare Fortsetzung eine Multiplikation

$$\wedge : \bigwedge V \times \bigwedge V \to \bigwedge V$$
$$(\alpha, \beta) \mapsto \alpha \wedge \beta,$$

die $\bigwedge V$ zu einer K-Algebra macht, die man die *äussere Algebra* nennt.

Beispiele 3.4.7.

- Sei $V = K$, dann hat $\bigwedge V$ die Basis $1, e$ und die Multiplikation ist gegeben durch $e^2 = 0$.
- Sei $V = K^2$. Dann hat $\bigwedge V$ die Basis $1, e_1, e_2, e_1 \wedge e_2$.
- Sei $V = K^3$. Dann hat $\bigwedge V$ die Basis $1, e_1, e_2, e_3, e_1 \wedge e_2, e_1 \wedge e_3, e_2 \wedge e_3, e_1 \wedge e_2 \wedge e_3$.

3.5 Lineare Abbildungen

Sei $T : V \to V$ linear. Die Abbildung

$$m : V^k \to \bigwedge^k V$$
$$(v_1, \ldots, v_k) \mapsto Tv_1 \wedge \cdots \wedge Tv_k$$

ist alternierend. Nach der universellen Eigenschaft existiert eine lineare Abbildung

$$\bigwedge^k T : \bigwedge^k V \to \bigwedge^k V,$$

so dass

$$\bigwedge^k T(v_1 \wedge \cdots \wedge v_k) = Tv_1 \wedge \cdots \wedge Tv_k.$$

Beispiel 3.5.1. Sei die lineare Abbildung $A : K^3 \to K^3$ durch die Matrix

$$A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & j \end{pmatrix}$$

gegeben. Wir bestimmen die Matrix von $\bigwedge^2 A$ in der Basis $e_1 \wedge e_2, e_1 \wedge e_3, e_2 \wedge e_3$. Wir rechnen

$$\begin{aligned} \bigwedge^2 A(e_1 \wedge e_2) &= (Ae_1) \wedge (Ae_2) \\ &= (ae_1 + de_2 + ge_3) \wedge (be_1 + ee_2 + he_3) \\ &= (ae - bd)e_1 \wedge e_2 + (ah - bg)e_1 \wedge e_3 + (dh - eg)e_2 \wedge e_3. \end{aligned}$$

Ebenso rechnet man die anderen Terme durch und erhält am Ende die Matrix

$$\begin{pmatrix} \det\left(\begin{smallmatrix} a & b \\ d & e \end{smallmatrix}\right) & \det\left(\begin{smallmatrix} a & c \\ d & f \end{smallmatrix}\right) & \det\left(\begin{smallmatrix} b & c \\ e & f \end{smallmatrix}\right) \\ \det\left(\begin{smallmatrix} a & b \\ g & h \end{smallmatrix}\right) & \det\left(\begin{smallmatrix} a & c \\ g & j \end{smallmatrix}\right) & \det\left(\begin{smallmatrix} b & c \\ h & j \end{smallmatrix}\right) \\ \det\left(\begin{smallmatrix} d & e \\ g & h \end{smallmatrix}\right) & \det\left(\begin{smallmatrix} d & f \\ g & j \end{smallmatrix}\right) & \det\left(\begin{smallmatrix} e & f \\ h & j \end{smallmatrix}\right) \end{pmatrix}.$$

Satz 3.5.2. *Ist* $\dim V = n$ *und* $T : V \to V$ *linear, so gilt*

$$\bigwedge^n T = \det(T)\mathrm{Id}.$$

Beweis. Sei $v_1 \dots v_n$ eine Basis von V. Der eindimensionale Raum $\bigwedge^n V$ wird von $v_1 \wedge \dots \wedge v_n$ aufgespannt. Sei $(a_{i,j})$ die Matrix von T, d.h.

$$Tv_j = \sum_{i=1}^{n} a_{i,j} v_i.$$

es folgt

$$\begin{aligned}\textstyle\bigwedge^n T(v_1 \wedge \cdots \wedge v_n) &= Tv_1 \wedge \cdots \wedge Tv_n \\ &= \sum_{i_1 \ldots i_n = 1}^{n} a_{i_1,1} \cdots a_{i_n,n} v_{i_1} \wedge \cdots \wedge v_{i_n} \\ &= \sum_{\sigma \in \mathrm{Per}(n)} a_{\sigma(1),1} \cdots a_{\sigma(n),n} \underbrace{v_{\sigma(1)} \wedge \cdots \wedge V_{\sigma(n)}}_{=\mathrm{sign}(\sigma) v_1 \wedge \cdots \wedge v_n} \\ &= \det(T)\, v_1 \wedge \cdots \wedge v_n. \qquad \square\end{aligned}$$

Satz 3.5.3. *Ist* $\dim V = n$ *und* $T : V \to V$ *linear, so gilt*

$$\det(1 - T) = \sum_{j=0}^{n} (-1)^j \operatorname{tr} \textstyle\bigwedge^j T.$$

Beweis. Beide Seiten der Gleichung aendern sich nicht, wenn wir den Körper K durch einen algebraischen Abschluss ersetzen, wir koennen also den Körper als algebraisch abgeschlossen annehmen. Dann ist jede Matrix triangulierbar. Da beide Seiten der Gleichung sich nicht aendern, wenn man T durch eine konjugierte ersetzt, kann man annehmen, dass $T = D + N$, wobei D eine Diagonalmatrix ist und N eine obere Dreiecksmatrix mit Nullen af der Diagonalen. Es gilt dann
$\det(1 - T) = \det(1 - D - N) = \det(1 - D)$. Ferner ist auch
$\operatorname{tr} \bigwedge^j T = \operatorname{tr} \bigwedge^j (D + N) = \operatorname{tr} \bigwedge^j D$, da $\bigwedge^j (D + N) = \bigwedge^j D + \tilde{N}$, wobei $\tilde{N}$ in der Standard-Basis eine obere Dreiecksmatrix mit Nullen auf der Diagonale und $\bigwedge^j D$ ist eine Diagonalmatrix. Insgesamt kann man also T durch D ersetzen und annehmen, dass T eine Diagonalmatrix ist. Diese habe die Diagonaleinträge $\lambda_1, \ldots, \lambda_n$. Dann ist

$$\begin{aligned}\det(1 - T) = (1 - \lambda_1) \cdots (1 - \lambda_n) &= \sum_{j=0}^{n} \sum_{1 \le i_1 < \cdots < i_j \le n} (-1)^j \lambda_{i_1} \cdots \lambda_{i_j} \\ &= \sum_{j=0}^{n} (-1)^j \operatorname{tr} \textstyle\bigwedge^j T. \qquad \square\end{aligned}$$

3.6 Tensorielle Algebra

Definition 3.6.1. Sind A, B Algebren über einem Körper K, dann ist ein *Algebrenhomomorphismus* von A nach B eine lineare Abbildung $\phi : A \to B$, für die

$$\phi(ab) = \phi(a)\phi(b) \quad \text{und} \quad \phi(1) = 1$$

gilt.

Beispiele 3.6.2.

- Der Algebrenhomomorphismus $\mathrm{M}_n(K) \to \mathrm{M}_{2n}(K)$, $A \mapsto \left(\begin{smallmatrix} A & \\ & A \end{smallmatrix}\right)$ ist unital.
- Ist $S \neq \emptyset$ eine Menge und $\mathcal{A} = \mathrm{Abb}(S, K)$ die Algebra aller Abbildungen von S nach K mit punktweiser Addition und Multiplikation. Sei $s_0 \in S$, dann ist die Abbildung $\phi : \mathcal{A} \to K$, $f \mapsto f(s_0)$ ein Algebrenhomomorphismus.

Lemma 3.6.3. *Sei $\phi : \mathcal{A} \to \mathcal{B}$ ein Algebrenhomomorphismus. Ist ϕ bijektiv, so ist die Umkehrabbildung $\phi^{-1} : \mathcal{B} \to \mathcal{A}$ ebenfalls ein Algebrenhomomorphismus. In diesem Fall heisst ϕ ein* Algebrenisomorphismus*.*

Beweis. Wir wissen bereits, dass ϕ^{-1} linear ist. Seien also $b, b' \in \mathcal{B}$, so gilt

$$\phi(\phi^{-1}(bb')) = bb' = \phi(\phi^{-1}(b))\phi(\phi^{-1}(b')) = \phi(\phi^{-1}(b)\phi^{-1}(b')).$$

Da ϕ injektiv ist, folgt

$$\phi^{-1}(bb') = \phi^{-1}(b)\phi^{-1}(b'),$$

also ist ϕ^{-1} ein Algebrenhomomorphismus. Aus $\phi(1) = 1$, folgt durch Anwenden von ϕ^{-1} auch $\phi^{-1}(1) = 1$. Die Umkehrung folgt durch Vertauschung der Rollen von ϕ und ϕ^{-1}. □

Ist I eine Indexmenge und ist für jedes $i \in I$ ein K-Vektorraum V_i gegeben, so ist

$$V = \prod_{i \in I} V_i$$

ein K-Vektorraum, wobei die Addition und die skalare Multiplikation komponentenweise erklaert sind. Wir betrachten den Unterraum

$$\bigoplus_{i \in I} V_i := \left\{ v \in \prod_{i \in I} V_i : v_i = 0 \text{ für fast alle } i \right\}.$$

Man macht sich leicht klar, dass dies in der Tat ein Unterraum ist und dass für endliche Indexmengen diese Notation mit der bisherigen $\oplus$-Notation für Unterraeume kompatibel ist, wenn man jedes V_j als Teilraum von $V = \prod_{i \in I} V_i$ auffasst. Es ist der Teilraum der Elemente des Produktes, die nur an der j-Koordinate einen Eintrag ungleich Null haben duerfen.

Sei nun V ein K-Vektorraum und sei

$$\begin{aligned} T(V) &= K \oplus V \oplus (V \otimes V) \oplus (V \otimes V \otimes V \otimes V) \oplus \dots \\ &= \bigoplus_{n=0}^{\infty} V^{\otimes n}, \end{aligned}$$

wobei $V^{\otimes 0} = K$ und

$$V^{\otimes n} = \underbrace{V \otimes V \otimes \cdots \otimes V}_{n \text{ mal}}$$

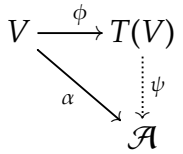
für $n \geq 1$ ist. Die Vorschrift

$$v \cdot w = v \otimes w \in V^{\otimes (m+n)},$$

wenn $v \in V^{\otimes m}$ und $w \in V^{\otimes n}$, macht $T(V)$ zu einer Algebra, die man die *tensorielle Algebra* von V nennt.

Satz 3.6.4 (Universelle Eigenschaft der tensoriellen Algebra)**.** *Sei V ein K-Vektorraum, $\phi = \phi_V : V \to T(V)$ die Abbildung, die V auf die erste Tensorpotenz schickt. Dann hat ϕ folgende universelle Eigenschaft:*

Für jede K-Algebra $\mathcal{A}$ und jede lineare Abbildung $\alpha : V \to \mathcal{A}$ existiert genau ein Algebrenhomomorphismus $\psi : T(V) \to \mathcal{A}$, der α fortsetzt, d.h., so, dass das Diagramm



kommutiert.

Beweis. Sei eine lineare Abbildung $\alpha : V \to \mathcal{A}$ in die Algebra $\mathcal{A}$ gegeben. Wir

definieren eine lineare Abbildung $\psi : T(V) \to \mathcal{A}$ durch $\psi(1) = 1$ und

$$\psi(v_1 \otimes \cdots \otimes v_n) = \alpha(v_1)\alpha(v_2)\cdots\alpha(v_n),$$

wobei rechts das Produkt in $\mathcal{A}$ genommen wird. Nach Definition ist ψ multiplikativ auf den Basiselementen, damit aber auch schon insgesamt multiplikativ. Nach Konstruktion gilt $\psi(\phi(v)) = \alpha(v)$ und damit kommutiert das Diagramm. Sei nun ψ' ein weiterer Algebrenhomomorphismus, für den das Diagramm kommutiert, dann gilt

$$\psi'(v_1 \otimes \cdots \otimes v_n) = \psi'(v_1)\cdots\psi'(v_n) = \alpha(v_1)\cdots\alpha(v_n) = \psi(v_n \otimes \cdots \otimes v_n)$$

und damit $\psi' = \psi$. □

Sei $\phi : \mathcal{A} \to \mathcal{B}$ ein Algebrenhomomorphismus und sei $I = \ker(\phi)$ der Kern. Dann gilt

- I ist ein Untervektorraum von $\mathcal{A}$ und
- $IA \subset I$ und $AI \subset I$, wobei

$$IA = \text{Spann}\left\{ya : y \in I,\ a \in \mathcal{A}\right\}$$

  geschrieben wurde.

Die zweite Eigenschaft schreibt man auch so

$$y \in I, a \in \mathcal{A} \quad \Rightarrow \quad ay, ya \in I.$$

Eine Teilmenge $I \subset \mathcal{A}$ mit diesen beiden Eigenschaften nennt man ein *(zweiseitiges) Ideal* von $\mathcal{A}$.

Beispiel 3.6.5. Ist $M \subset \mathcal{A}$ eine Teilmenge, dann ist der Untervektorraum

$$I = \mathcal{A}M\mathcal{A} = \text{Spann}\left\{amb : a, b \in \mathcal{A},\ m \in M\right\}$$

ein Ideal. Dies ist das kleinste Ideal, das M enthaelt, man nennt es das von M *erzeugte Ideal*.

Beweis. Ist M leer, so ist I das Nullideal. Sei also $M \neq \emptyset$. Die Menge $\mathcal{A}M\mathcal{A}$ ist nach Definition ein Untervektorraum. Ist nun $y \in I$ und $a \in \mathcal{A}$, dann kann man y schreiben

als

$$y = \sum_{j=1}^{n} a_j m_j b_j$$

mit $b_j, b_j \in \mathcal{A}$ und $m_j \in M$. Also sind $ay = \sum_{j=1}^{n} aa_j m_j b_j$ und $ya = \sum_{j=1}^{n} a_j m_j b_j a$ wieder in I. □

Satz 3.6.6. *Ein Unterraum I einer Algebra $\mathcal{A}$ ist genau dann ein Ideal, wenn der Quotientenraum $\mathcal{A}/I$ eine Algebrenstruktur traegt, so dass die Projektion $P : \mathcal{A} \to \mathcal{A}/I$ ein Algebrenhomomorphismus ist. Diese Algebrenstruktur ist dann eindeutig bestimmt.*

Beweis. Sei I ein Ideal. Wir definieren eine Multiplikation auf dem Quotientenraum $\mathcal{A}/I$ durch

$$(a + I)(b + I) = ab + I.$$

Hier ist die Wohldefiniertheit zu pruefen. Seien also $a', b' \in \mathcal{A}$ mit $a + I = a' + I$ und $b' + I = b + I$, das heisst $a - a' \in I$ und $b - b' \in I$. Dann gilt

$$\begin{aligned} ab - a'b' &= ab - a'b + a'b - a'b' \\ &= \underbrace{(a - a')}_{\in I} b + a' \underbrace{(b - b')}_{\in I} \in I, \end{aligned}$$

also $ab + I = a'b' + I$, d.h., die Multiplikation ist wohldefiniert. Wegen der Surjektivität der Projektion $P : \mathcal{A} \to \mathcal{A}/I$ ist diese Multiplikation eindeutig festgelegt. □

Satz 3.6.7 (Homomorphiesatz)**.** *Ist $\phi : \mathcal{A} \to \mathcal{B}$ ein Algebrenhomomorphismus, dann ist das Bild eine Unteralgebra von $\mathcal{B}$ und es gilt*

$$\text{Bild}(\phi) \cong \mathcal{A}/\ker(\phi),$$

wobei eine Isomorphie als Algebren gemeint ist.

Beweis. Der Kern $\ker(\phi)$ ist ein Ideal, so dass die Algebra $\mathcal{A}/\ker(\phi)$ wohldefiniert ist. Die besagte Isomorphie ist uns als eine Isomorphie von Vektorraeumen bereits

bekannt. Sie ist durch ϕ induziert und da ψ ein Algebrenhomomorphismus ist, ist die Isomorphie auch einer. □

Beispiele 3.6.8.

- Sei S eine Menge und $\mathcal{A} = \mathrm{Abb}(S, K)$, sowie $T \subset S$ eine Teilmenge und sei
$$I = \left\{ f \in \mathcal{A} : f|_T = 0 \right\}.$$
Dann ist T ein Ideal und $\mathcal{A}/I \cong \mathrm{Abb}(T, K)$.

- Sind $\mathcal{A}$ und $\mathcal{B}$ Algebren, so ist auch $\mathcal{A} \times \mathcal{B}$ eine Algebra mit der komponentenweisen Multiplikation, also
$$(a, b)(a', b') = (aa', bb').$$
Die Projektion $P : \mathcal{A} \times \mathcal{B} \to \mathcal{A}$ ist ein Algebremnhomomorphismus mit Kern
$$I = \{0\} \times \mathcal{B}.$$

- Sei $1 \leq k \leq n$ und sei $\mathcal{A}$ die Menge aller Matrizen in $\mathrm{M}_n(K)$ der Gestalt $\left(\begin{smallmatrix} A & B \\ & D \end{smallmatrix}\right)$, also der untere linke $(n-k) \times k$-Block ist Null. Dann ist $\mathcal{A}$ eine Unteralgebra mit Eins von $\mathrm{M}_n(K)$ und die Abbildung $\mathcal{A} \to \mathrm{M}_k(K)$, $\left(\begin{smallmatrix} A & B \\ & D \end{smallmatrix}\right) \mapsto A$ ist ein Algebrenhomomorphismus dessen Kern das Ideal I aller Matrizen der Form $\left(\begin{smallmatrix} 0 & B \\ & D \end{smallmatrix}\right)$ ist.

Satz 3.6.9. *Jede Algebra $\mathcal{A}$ mit Eins ist Quotient einer tensoriellen Algebra, d.h. es gibt einen Vektorraum V und ein Ideal I von $T(V)$ so dass $\mathcal{A} \cong T(V)/I$.*

Beweis. Als Vektorraum kann man $V = \mathcal{A}$ selbst nehmen. Die lineare Abbildung $\mathcal{A} \to \mathcal{A}$, die durch die Identitaet gegeben ist, induziert nach der universellen Eigenschaft einen Algebrenhomomorphismus $\psi : T(V) \to \mathcal{A}$, der surjektiv ist, weil die Einschraenkung nach $V \cong \mathcal{A}$ schon surjektiv ist. Sei $I = \ker(\psi)$, so folgt $\mathcal{A} \cong T(V)/I$. □

Beispiele 3.6.10.

- Sei V ein K-Vektorraum. Die aeussere Algebra $\bigwedge^* V$ ist ein Quotient der tensoriellen Algebra, es gibt also einen surjektiven Algebrenhomomorphismus
$$\phi : T(V) \to \bigwedge^* V.$$

Der Kern von ϕ ist das zweiseitige Ideal erzeugt von allen Elementen der Form $v \otimes v$ für $v \in V$.

- Sei $V = \mathbb{R}v_0$ ein eindimensionaler $\mathbb{R}$-Vektorraum. Man kann $\mathbb{C}$ als Quotienten der $\mathbb{R}$-Algebra $T(V)$ schreiben. Der Kern ist das Ideal erzeugt von $v_0 \otimes v_0 + 1$.

3.7 Die symmetrische Algebra

Sei V ein K-Vektorraum und sei I das Ideal von $T(V)$ erzeugt von der Teilmenge

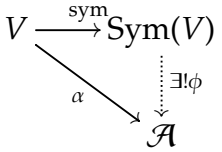
$$M = \Big\{ v \otimes w - w \otimes v : v, w \in V \Big\}.$$

Sei

$$\mathrm{Sym}(V) = T(V)/I.$$

Man nennt $\mathrm{Sym}(V)$ die *symmetrische Algebra* über V. Man schreibt das Bild von $v_1 \otimes \cdots \otimes v_n$ in $\mathrm{Sym}(V)$ als $v_1 \cdots v_n$.

Satz 3.7.1. *Die Algebra* $\mathrm{Sym}(V)$ *ist kommutativ. Die kanonische Abbildung* $\mathrm{sym} : V \to \mathrm{Sym}(V)$ *ist injektiv.* $\mathrm{Sym}(V)$ *ist die universelle kommutative Algebra mit einer linearen Abbildung von* V*, genauer heisst das: Ist* $\alpha : V \to \mathcal{A}$ *eine lineare Abbildung in eine kommutative Algebra, so existiert genau ein Algebrenhomomorphismus* $\phi : \mathrm{Sym}(V) \to \mathcal{A}$ *der das Diagramm*



kommutativ macht.

Beweis. Der kanonische Algebrenhomomorphismus $T(V) \to \mathcal{A}$ über den α faktorisiert, annulliert das Ideal I, da $\mathcal{A}$ kommutativ ist. Daher existiert genau ein ϕ, welches das Diagramm kommutativ macht. □

Satz 3.7.2. *Sei $V \neq 0$ endlich-dimensional, dann ist die Algebra* $\mathrm{Sym}(V)$ *unendlich-dimensional. Sie kann geschrieben werden als*

$$\mathrm{Sym}(V) = \bigoplus_{j=0}^{\infty} \mathrm{Sym}_j(V),$$

wobei $\mathrm{Sym}_j(V)$ *das Bild von* $V^{\otimes n}$ *ist. Es gilt*

$$\mathrm{Sym}_k(V)\,\mathrm{Sym}_j(V) \subset \mathrm{Sym}_{k+j}(V).$$

Ist $e_1, \ldots, e_n$ eine Basis von V, dann ist

$$\left(e_1^{p_1} \cdots e_n^{p_n}\right)_{p_1+\cdots+p_n=j}$$

eine Basis von $\mathrm{Sym}_j(V)$*, wobei die p_j in $\mathbb{N}_0$ liegen. In diesem Fall definiert die Vorschrift*

$$\begin{aligned} \mathrm{Sym}(V) &\to K[X_1, \ldots, X_n], \\ e_j &\mapsto X_j \end{aligned}$$

einen Algebrenisomorphismus.

Beweis. Schreibe $\mathrm{Sym}(V) = T(V)/I$ wie oben. Dann wird $\mathrm{Sym}(V)$ von den Elementen der Form $v_1 \cdots v_n$, genannt *Monome*, aufgespannt, da $T(V)$ von den reinen Tensoren aufgespannt wird. Dann ist $\mathrm{Sym}_j(V)$ der Spann der Monome der Laenge j und $\mathrm{Sym}(V)$ ist die Summe aller $\mathrm{Sym}_j(V)$. Es ist zu zeigen, dass $\mathrm{Sym}_j \cap \mathrm{Sym}_k = 0$ für $k \neq j$ gilt. Dies folgt allerdings automatisch, wenn wir die Aussage über die Basis zeigen. Es ist nun

$$v_1 \otimes \cdots \otimes v_k \otimes v_{k+1} \otimes \cdots \otimes v_m - v_1 \otimes \cdots \otimes v_{k+1} \otimes v_{k+} \otimes \cdots \otimes v_m$$

in I, hier wurden zwei aufeinanderfolgende Faktoren vertauscht. Das bedeutet, dass man in $\mathrm{Sym}(V)$ in einem Monom $v_1 \cdots v_m$ ebenfalls zwei aufeinanderfolgende Faktoren vertauschen kann. Ist nun $e_1, \ldots, e_n$ eine Basis von V, dann kann man in einem gegebenen Monom $v_1 \cdots v_m$ jdes v_j in der Basis entwickeln und alles ausdistribuieren, so dieht man , dass $\mathrm{Sym}(V)$ von den Monomen der Gestalt $e_{i_1} \cdots e_{i_m}$ erzeugt wird. Indem man benachbarte Faktoren vertauscht, kann man ein solches Monom immer in die Form $e_1^{p_1} \cdots e_n^{p_n}$ bringen, so dass die behauptete Basis schon

einmal ein Erzeugendensystem ist. Um die lineare Unabhängigkeit zu zeigen betrachten wir die lineare Abbildung $\alpha : V \to K[x_1, \ldots, x_n]$ definiert durch $\alpha(e_j) = x_j$, so induziert diese nach der universellen Eigenschaft einen Algebrenhomomorphismus $\phi : \mathrm{Sym}(V) \to K[x_1, \ldots, x_n]$ dessen Bild von $x_1, \ldots, x_n$ erzeugt wird, der also surjektiv ist. Da die Monome der Form $e_1^{p_1} \cdots e_n^{p_n}$ gerade auf die Monome im Polynomring abgebildet werden, die bekanntermassen eine Basis von $K[x_1, \ldots, x_n]$ bilden, ist ϕ ein Algebrenisomorphismus und die Monome eine Basis von $\mathrm{Sym}(V)$ wie behauptet. □

4 Moduln über einem Hauptidealring

4.1 Ringe

Definition 4.1.1. Ein *kommutativer Ring mit Eins* ist eine abelsche Gruppe $(R, +)$ mit einer weiteren Verknüpfung $\times$, die assoziativ ist,

$$(ab)c = a(bc)$$

und kommutativ

$$ab = ba$$

und das Distributivgesetz erfüllt:

$$a(b + c) = ab + ac.$$

Ferner existiert ein Element $1_R \in R$ mit

$$1_R a = a$$

für jedes $a \in R$. Dieses Element ist dann eindeutig bestimmt und wird 1 geschrieben.

Wenn wir im Folgenden *Ring* schreiben, meinen wir immer einen kommutativen Ring mit Eins.

Ein Ring ist also dasselbe wie ein Körper, bis auf die Tatsache, dass nicht jedes Element $\neq 0$ invertierbar sein muss.

Beispiele 4.1.2.

- $(\mathbb{N}, +, \times)$ ist **kein** Ring, da es keine inversen Elemente der Addition gibt.
- $(\mathrm{M}_n(K), +, \times)$ ist kein kommutativer Ring für $n \geq 2$, da Matrixmultiplikation nicht kommutativ ist.
- Jeder Körper ist ein Ring.
- $\mathbb{Z}$ ist ein Ring, der kein Körper ist.
- Ist K ein Körper, dann ist die Menge der Polynome $K[x]$ ein Ring.

- Der einfachste Ring ist der *Nullring* $N = \{0\}$. In diesem Ring gilt $0 = 1$. Ist R ein Ring, in dem $0 = 1$ gilt, dann ist R der Nullring, denn für $a \in R$ gilt

$$a = 1a = 0a = (1-1)a = a - a = 0.$$

  Der Nullring ist ein dummes Beispiel und wir werden uns im Folgenden in der Regel auf Ringe mit $0 \neq 1$ einschränken.

- Sei $\alpha = \sqrt{2} \in \mathbb{R}$. Dann gilt $\alpha^2 = 2$. Wir definieren

$$\mathbb{Z}[\sqrt{2}] = \left\{k + l\alpha : k, l \in \mathbb{Z}\right\}.$$

  Wegen $(k + l\alpha)(m + n\alpha) = km + 2ln + (kn + lm)\alpha$ ist $\mathbb{Z}[\sqrt{2}]$ ein Unterring von $\mathbb{R}$.

- Der *Gaußsche Zahlring* ist definiert als

$$\mathbb{Z}[i] = \left\{a + bi : a, b \in \mathbb{Z}\right\} \subset \mathbb{C}.$$

- Ist R ein Ring, dann definiert man den Polynomring $R[x]$ genau wie im Körperfall. Elemente sind formale Ausdrücke der Form

$$a_0 + \cdots + a_n x^n$$

  und die Multiplikation ist definiert durch

$$(a_0 + \cdots + a_n x^n)(b_0 + \cdots + b_m x^m) = c_0 + \cdots + c_{m+n} x^{m+n},$$

  wobei $c_k = \sum_{i+j=k} a_i b_j$. Insbesondere kann man also den Uebergang von einem Ring zum Polynomring wiederholen und erhaelt den *Polynomring in mehreren Unbekannten*,

$$R[X_1, \ldots, X_r].$$

  Die Elemente dieses Rings sind formale Ausdruecke der Form

$$\sum_{\alpha} c_\alpha X^\alpha,$$

  wobei α durch $\mathbb{N}_0^r$ laeuft, $c_\alpha \in R$ ein Koeffizient ist, der nur für endlich viele α nicht Null ist und

$$X^\alpha = X_1^{\alpha_1} X_2^{\alpha_2} \cdots X_r^{\alpha_r}$$

ist.

- Im Polynomring $R[x]$ gilt

$$(a_0 + a_1x + \cdots + a_nx^n)(b_0 + b_1x + \cdots + b_mx^m) = c_0 + c_1x + \cdots + c_{n+m}x^{n+m},$$

wobei $c_0 = a_0b_0, c_1 = a_0b_1 + a_1b_0$ und allgemein

$$c_k = \sum_{i+j=k} a_ib_j.$$

Also haengt der Koeffizient c_k nur von den Koeffizienten $a_0, \ldots, a_k$ und $b_0, \ldots b_k$ ab und nicht von denen hoeheren Grades. Dasselbe gilt für die Addition. Daher kann man Addition und Multiplikation des Polynomrings $R[x]$ auch auch die Menge aller Koeffizientenfolgen $(a_0, a_1, \ldots)$ ausdehnen, die nicht notwendigerweise endlich sind. Alternativ kann man diese Menge $R^{\mathbb{N}_0} = \text{Abb}(N_0, R)$ auch als Menge aller formalen Reihen

$$\sum_{j=0}^{\infty} a_jx^j$$

beschreiben. Der so entstehende Ring wird der Ring der *formalen Potenzreihen* genannt und als

$$R[[x]]$$

geschrieben.

- Sei p eine Primzahl und sei $\mathbb{Z}_{(p)}$ die Menge aller rationalen Zahlen $\frac{a}{b} \in \mathbb{Q}$ für die der Nenner b zur Primzahl p teilerfremd ist, also von p nicht geteilt wird. Dies ist ein Unterring von $\mathbb{Q}$.

Beispiel 4.1.3. Sei $m \in \mathbb{N}$ und sei $R = \mathbb{Z}/m$ gleich der Menge $\{0, 1, \ldots, m-1\}$. Wir definieren Addition und Multiplikation wie folgt

$$a \boxplus b = \text{Rest von } a + b \text{ nach Division durch } m.$$

Und die Multiplikation

$$a \boxtimes b = \text{Rest von } ab \text{ nach Division durch } m.$$

Man verifiziert, dass $\mathbb{Z}/m$ mit diesen Operationen ein Ring ist.

Zweite Definition: Auf $\mathbb{Z}$ definiert man folgende Äquivalenzrelation $a \sim b \Leftrightarrow a - b \in m\mathbb{Z}$. Sei $\mathbb{Z}/m$ die Menge $\mathbb{Z}/\sim$ der Äquivalenzklassen. Es ist klar, dass es genau m Äquivalenzklassen gibt $[0], [1], \ldots, [m-1]$. Addition und Multiplikation werden wie folgt definiert

$$[a] + [b] = [a + b], \quad [a][b] = [ab].$$

Hier ist Wohldefiniertheit zu prüfen: etwa $a \sim a'$, $b \sim b'$, dann ist zu zeigen, dass $(a + b) \sim (a' + b')$ und $ab \sim a'b'$. Für die erste Aussage betrachte

$$(a + b) - (a' + b') = a - a' + b - b' \in M\mathbb{Z}.$$

Für die zweite:

$$ab - a'b' = ab - a'b + a'b - a'ba = (a - a')b + a'(b - b') \in m\mathbb{Z}.$$

Definition 4.1.4. Ein Element $0 \neq a \in R$ eines Rings heißt *invertierbar* oder *Einheit* des Rings, wenn es ein $b \in R$ gibt mit $ab = 1$. Die Menge $R^\times$ der invertierbaren Elemente ist eine abelsche Gruppe bzgl. der Multiplikation. Ein Ring R ist genau dann ein Körper, wenn $R^\times = R \setminus \{0\}$ gilt.

Beispiele 4.1.5.

- Die Einheiten von $\mathbb{Z}$ sind ± 1.
- Sei K ein Körper und sei $R = K[x]$ der Polynomring. Die Einheiten von R sind genau die konstanten Polynome $\neq 0$.
- Die Einheiten des Rings $R = \mathbb{Z}[\sqrt{-5}]$ sind genau die Zahlen 1 und -1.

  Beweis. Seien $a, b \in R$ mit $ab = 1$. Da $a, b \in \mathbb{C}$ ist, gilt diese Gleichung auch dort, also ist auch $1 = |ab|^2 = |a|^2|b|^2$. Damit gilt $|a|^2 \leq 1$ oder $|b|^2 \leq 1$. Nehmen wir $|a|^2 \leq 1$ an. Sei $a = k + il\sqrt{5}$, dann ist $|a|^2 = k^2 + 5l^2$ und da $k, l \in \mathbb{Z}$, folgt $l = 0$ und $a = k = \pm 1$. Damit ist auch $b = \pm 1$ und die Beauptung ist gezeigt. □
- Die Einheiten des Rings $\mathbb{Z}/m$ sind genau die Zahlen $1 \leq x \leq m - 1$, die zu m teilerfremd sind. Dies zeigt man mit Hilfe der Division mit Rest (Übungsaufgabe!)

Definition 4.1.6. Ein Element $a \neq 0$ eines Rings R heißt *Nullteiler*, falls es ein $b \neq 0$ gibt mit $ab = 0$.

Ein Ring R mit $0 \neq 1$ heißt *nullteilerfrei*, oder *integer*, oder *Integritätsring*, falls es keine Nullteiler in R gibt, wenn also gilt

$$ab = 0 \quad \Rightarrow \quad a = 0 \text{ oder } b = 0.$$

Beispiele 4.1.7.

- Der Nullring ist kein Integritätsring.
- Körper sind Integritätsringe.
- Jeder Unterring eines Integritätsrings ist ein Integritätsring. So ist zum Beispiel $\mathbb{Z}[\sqrt{-5}]$ ein Integritätsring, da er ein Unterring des Körpers $\mathbb{C}$ ist.
- $\mathbb{Z}$ ist ein Integritätsring.
- $\mathbb{Z}/m$ ist nur dann ein Integritaetsring, wenn m eine Primzahl ist.
- Ist R ein Integritätsring, dann auch der Polynomring $R[x]$.

  Beweis. Seien $f, g \in R[x]$, beide $\neq 0$. Wir zeigen $fg \neq 0$. Sei dazu

  $$f(x) = a_0 + \cdots + a_n x^n,$$
  $$g(x) = b_0 + \cdots + b_m x^m$$

  mit $a_n \neq 0 \neq b_m$. Dann gilt

  $$f(x)g(x) = c_0 + \cdots + c_{m+n} x^{m+n},$$

  wobei $c_k = \sum_{i+j=k} a_i b_j$. Insbesondere ist dann $c_{m+n} = a_n b_m \neq 0$, da R ein Integritätsring ist. □

- Sind R, S Ringe, dann ist auch das kartesische Produkt $R \times S$ ein Ring, indem man die Operationen Komponentenweise definiert. Das Nullelement ist $(0, 0)$ und die Eins ist $(1, 1)$. Dieser Ring ist kein Integritaetsring, auch wenn R und S welche sind, denn es gilt
  $$(0, 1) \cdot (1, 0) = (0, 0).$$

Definition 4.1.8. Seien R, S Ringe. Ein *Ringhomomorphismus* ist eine Abbildung $\phi : R \to S$ so dass

- ϕ ist ein Gruppenhomomorphismus $(R, +) \to (S, +)$,

- $\phi(1) = 1$,
- $\phi(ab) = \phi(a)\phi(b)$.

Beispiele 4.1.9.
- Die Inklusionen $\mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$ sind Ringhomomorphismen.
- Sei $m \in \mathbb{N}$. Die Projektion $\mathbb{Z} \to \mathbb{Z}/m$ ist ein Ringhomomorphismus.
- Ist $R = K[x]$ ein Polynomring und ist $\alpha \in K$. dann ist die Abbildung $\delta_\alpha : K[x] \to K$, die $f(x)$ auf $f(\alpha)$ schickt, ein Ringhomomorphismus.

Satz 4.1.10. *Ein Ring R ist genau dann ein Integritaetsring, wenn R ein Unterring eines Körpers ist.*

In dem Fall gibt es bis auf Isomorphie genau einen Körper Quot(R)*, der R enthaelt und von R erzeugt wird. Jeder injektive Ringhomomorphismus $\phi : R \to L$ mit einem Körper L setzt in eindeutiger Weise zu einem Homomorphismus* Quot(R) $\to L$ *fort.*

Beweis. Ist R Unterring eines Körpers, dann ist er offen sichtlich integer. Sei umgekehrt R ein Integritaetsring. Wir wollen einen Körper $K = \text{Quot}(R)$ konstruieren. Dieser soll aus den Quotienten $\frac{a}{b}$ bestehen, mit $a, b \in R$ und $b \neq 0$, so dass die ueblichen Rechenregeln, also $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ und $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$ gelten. Man konstruiert K genauso, wie man $\mathbb{Q}$ aus $\mathbb{Z}$ konstruiert: Auf der Menge $R \times R \setminus \{0\}$ definiert man eine Aequivalenzrelation durch

$$(a, b) \sim (c, d) \quad :\Leftrightarrow \quad ad = bc.$$

Man sieht leicht, dass dies eine Arquivalenzrelation ist, der schwerste Teil ist die Transitivitaet: Seien also $(a, b) \sim (c, d)$ und $(c, d) \sim (e, f)$, dann gilt also

$$ad = bc \quad \text{und} \quad cf = de.$$

Damit folgt $afcd = becd$, also $cd(af - be) = 0$ und da wir in einem Integritaetsring sind und $cd \neq 0$, folgt $af = be$, also $(a, b) \sim (e, f)$, d.h. es gilt Transitivitaet.

Sei $K = (R \times R \setminus \{0\}) / \sim$. Wir schreiben die Aequivalenzklassen als Brueche, also

$\frac{a}{b} = [(a,b)]$. Wir definieren dann die Addition und Multiplikation durch

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \quad \text{und} \quad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}.$$

Hierbei ist natuerlich Wohldefiniertheit zu pruefen. Wir tun das für die Addition. Sei also $\frac{a}{b} = \frac{a'}{b'}$ und $\frac{c}{d} = \frac{c'}{d'}$. Wir muessen dann zeigen, dass $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$ gilt. Wir wollen also zeigen

$$ab'dd' + bb'cd' \stackrel{!}{=} a'bdd' + bb'c'd. \tag{*}$$

Wir haben

$$ab' = a'b \quad \text{und} \quad cd' = c'd.$$

Durch direktes Anwenden dieser beiden Formeln folgt allerdings die Behauptung (*) und damit die Wohkldefiniertheit der Addition. Die Multiplikation geht aehnlich und der Nachweis, dass es sich um einen Körper handelt, ist leicht. Der interessante Punkt ist hier nur, warum jedes Element $\neq 0$ invertierbar ist: Sei $\frac{a}{b} \neq 0$, dann ist insbesondere $b \neq 0$, also liegt auch $\frac{b}{a}$ in K und es gilt $\frac{a}{b}\frac{b}{a} = \frac{ab}{ab} = \frac{1}{1}$ und dies ist die Eins in K.

Wir muessen nun zeigen, dass R durch die Abbbildung $x \mapsto \frac{x}{1}$ in K eingebettet wird. Wegen

$$\frac{x}{1} + \frac{y}{1} = \frac{x+y}{1} \quad \text{und} \quad \frac{x}{1}\frac{y}{1} = \frac{xy}{1}$$

ist diese Abbildung ein Ringhomomorphismus. Er ist injektiv, denn $\frac{x}{1} = \frac{y}{1}$ ist aequivalent zu der Identitaet $1 \cdot x = 1 \cdot y$ in R. Also koennen wir R als einen Unterring von K auffassen und K besteht komplett aus Elementen, die Quotienten von Elementen aus R sind.

Wir zeigen zum Schluss, dass ein gegebener injektiver Ringhomomorphismus $\phi : R \to L$ in einen Körper L stets in eindeutiger Weise nach $K = \mathrm{Quot}(R)$ fortgesetzt werden kann. Sei diese Fortsetzung mit ψ beezeichnet. Wir definieren

$$\psi\left(\frac{a}{b}\right) = \phi(a)/\phi(b).$$

Dies ist moeglich, da ϕ injektiv ist und damit $\phi(b) \neq 0$ und damit invertierbar ist. Wir

zeigen, dass ψ ein Ringhomomorphismus ist:

$$\begin{aligned}\psi\left(\frac{a}{b}+\frac{c}{d}\right) &= \psi\left(\frac{ad+bc}{bd}\right)\\ &= \frac{\phi(ad+bc)}{\phi(bd)}\\ &= \frac{\phi(a)\phi(d)+\phi(b)\phi(c)}{\phi(b)\phi(d)}\\ &= \frac{\phi(a)}{\phi(b)}+\frac{\phi(c)}{\phi(d)}\\ &= \psi\left(\frac{a}{b}\right)+\psi\left(\frac{c}{d}\right).\end{aligned}$$

Die Multiplikation geht ebenso. Ist nun η ein weiterer Ringhomomorphismus $K \to L$, der ϕ fortsetzt, dann gilt

$$\begin{aligned}\eta\left(\frac{a}{b}\right) &= \frac{\eta(a)}{\eta(b)}\\ &= \frac{\phi(a)}{\phi(b)}\\ &= \psi\left(\frac{a}{b}\right),\end{aligned}$$

also folgt $\eta = \psi$. Zum guten schluss folgt die Eindeutigkeit von Quot(R) nach dem ueblichen Schemna aus der universellen Eigenschaft (Existenz und Eindeutigkeit von ψ). □

4.2 Ideale

Definition 4.2.1. Sei R ein Ring (kommutativ mit Eins). Ein *Ideal* in R ist eine Teilmenge $I \subset R$ mit den folgenden Eigenschaften

- I ist eine additive Untergruppe von R und
- ist $r \in R$ und $a \in I$, dann ist $ra \in I$. Kurz geschrieben lautet diese Bedingung

$$RI \subset I.$$

Beispiele 4.2.2.

- 0 und der ganze Ring R sind Ideale.
- Sei $I \subset R$ ein Ideal. Enthält I ein invertierbares Element, so ist $I = R$.

- Ist $\phi : R \to S$ ein Ringhomomorphismus, dann ist $\ker(\phi) = \left\{x \in R : \phi(x) = 0\right\}$ ein Ideal.

  Beweis. Da ϕ ein additiver Gruppenhomomorphismus ist, ist der Kern eine Untergruppe. Sei also $a \in I$ und $r \in R$. Dann folgt $\phi(ar) = \phi(a)\phi(r) = 0\phi(r) = 0$, also ist $ar \in I$. □

- Ist $r \in R$, so ist die Menge

  $$(r) = rR = \left\{rx : x \in R\right\}$$

  ein Ideal. Ein solches Ideal nennt man *Hauptideal*.

- Ist $a \in R$, so ist die Menge

  $$\mathrm{Ann}(a) := \left\{r \in R : ra = 0\right\}$$

  ein Ideal, genannt der *Annullator* von a.

Definition 4.2.3. In der Regel ist nicht jedes Ideal ein Hauptideal. Ein *Hauptidealring* ist ein Ring R, der

(a) nullteilerfrei ist und in dem

(b) jedes Ideal ein Hauptideal ist.

Beispiele 4.2.4.

- Jeder Körper K ist ein Hauptidealring, denn er hat nur zwei Ideale, $\{0\} = (0)$ und $K = (1)$.

- $\mathbb{Z}$ ist ein Hauptidealring.

  Beweis. Sei $I \subset \mathbb{Z}$ ein Ideal. Ist $I \cap \mathbb{N} = \emptyset$, dann ist auch $I \cap (-\mathbb{N}) = \emptyset$ und daher $I = \{0\} = (0)$. Ist $I \cap \mathbb{N} \neq \emptyset$, dann gibt es eine kleinste natürliche Zahl $m \in I$. Wir behaupten, dass $I = (m) = m\mathbb{Z}$. Klar ist $(m) \subset I$. Se also $k \in I$, dann existiert ein $p \in (m)$ so dass $0 \leq k - p < m$. Da m minimal in $I \cap \mathbb{N}$ ist, folgt $k - p = 0$, also $k = p \in (m)$. □

- Ist K ein Körper, so ist der Polynomring $K[x]$ ein Hauptidealring.

Beweis. Sei $I \neq 0$ ein Ideal und sei $g \in I \setminus \{0\}$ ein Polynom von minimalem Grad. Sei $f \in I$ beliebig, dann ist $\text{grad}(f) \geq \text{grad}(g)$, also existieren nach der *Division mit Rest* Polynome q, r mit

$$f = qg + r$$

und $\text{grad}(r) < \text{grad}(g)$. Dann ist $r = f - qg \in I$ und da der Grad von g minimal war, ist $r = 0$, also $f = gq \in (g)$. □

- Der Polynomring $\mathbb{Z}[x]$ ist kein Hauptidealring.

  Beweis. Betrachte das Ideal I, das von 2 und x erzeugt wird, also

  $$I = 2\mathbb{Z}[x] + x\mathbb{Z}[x].$$

  Wäre I ein Hauptideal (g), so müsste g, da $2 \in I$, den Grad Null haben, also gleich einer Zahl $m \in \mathbb{N}$ gewählt werden können. Da m dann die Zahl 2 teilt, folgte $m = 2$, aber $x \in I$ und $x \notin (2)$. □

- Der Ring $R = \mathbb{Z}[\sqrt{-5}]$ ist kein Hauptidealring, denn das Ideal $I = \alpha R + 3R$, das von $\alpha = i\sqrt{5}$ und 3 erzeugt wird, ist kein Hauptideal. *Angenommen*, es wäre eines, etwa $I = \eta R$. Da $\alpha \in I$, folgt $\alpha = \eta z$ für ein $z \in R$. Dann ist $5 = |\alpha|^2 = |\alpha|^2|z|^2 = 5|z|^2$. Nun ist für jedes $(a + b\alpha) \in R$ das Quadrat des Betrages $a^2 + 5b^2$ in $\mathbb{Z}$, also ist $|z| = 1$ und damit $z = \pm 1$, wir können $\eta = \alpha$ annehmen. Dann ist aber $3 = \alpha w$ für ein $w \in R$, was zu $9 = |3|^2 = |\alpha|^2|w|^2 = 5|w|^2$ führt, also ist 9 in $\mathbb{Z}$ ein Vielfaches von 5, *Widerspruch!*

Definition 4.2.5. Ein Integritätsring R heißt *euklidischer Ring*, falls es eine Abbildung $\delta : R \setminus 0 \to \mathbb{N}_0$ gibt, so dass zu je zwei $a, b \in R \setminus \{0\}$ zwei Elemente $q, r \in R$ existieren mit

$$a = bq + r$$

und $r = 0$ oder $\delta(r) < \delta(b)$. Man nennt δ die *Gradabbildung* des euklidischen Rings.

Proposition 4.2.6. *Jeder euklidische Ring ist ein Hauptidealring.*

Beweis. Sei $I \neq 0$ ein Ideal und sei $g \in I \setminus \{0\}$ ein Element von minimalem Grad, also $\delta(g)$ minimal unter allen $\delta(f)$ mit $f \in I$. Da $g \in I$, folgt $(g) \subset I$. Sei $f \in I$ beliebig, dann ist also $\delta(f) \geq \delta(g)$, also existieren Elemente q, r mit

$$f = qg + r$$

und $\delta(r) < \delta(g)$. Dann ist $r = f - qg \in I$ und da der Grad von g minimal war, ist $r = 0$, also $f = gq \in (g)$. □

Beispiele 4.2.7.

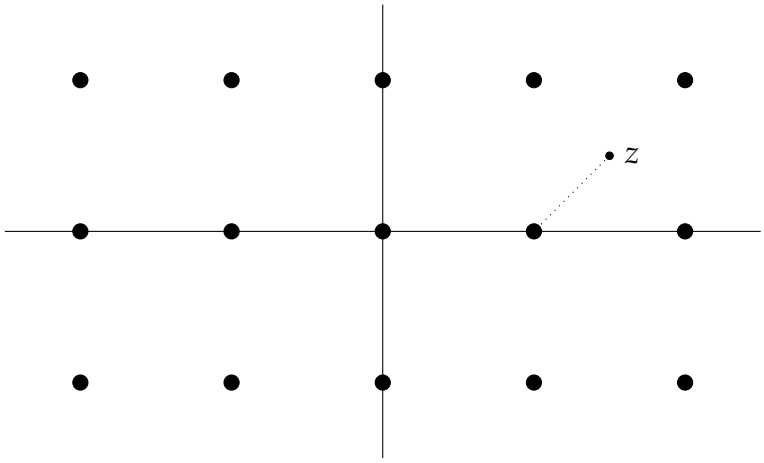
- $\mathbb{Z}$ ist ein euklidischer Ring mit $\delta(k) = |k|$.
- Sei K ein Körper, dann ist der Polynomring $K[x]$ euklidisch mit $\delta(f) = \text{grad}(f)$.
- Der Ring $R = \mathbb{Z}[i] = \mathbb{Z} \oplus \mathbb{Z}i$ aller komplexer Zahlen $m + ni$ mit $m, n \in \mathbb{Z}$ ist ein euklidischer Ring mit

$$\delta(m + ni) = m^2 + n^2, \quad \text{also} \quad \delta(z) = |z|^2 = z\bar{z}.$$

Beweis. Beachte zunaechst, dass die Funktion δ auf ganz $\mathbb{C}$ definiert ist und mutliplikativ ist, d.h., für $z, w \in \mathbb{C}$ gilt stets

$$\delta(zw) = \delta(z)\delta(w).$$

Wir stellen fest, dass für jedes $z \in \mathbb{C}$ der Abstand zum naechsten Punkt $c \in R$ stets $\leq \frac{1}{\sqrt{2}}$ ist.



Mit anderen Worten, zu jedem $z \in \mathbb{C}$ existiert ein $c \in R$ mit $\delta(z - c) \leq \frac{1}{2}$. Seien nun $a = m + ni$ und $b = k + li$ in $\mathbb{Z}[i] \setminus \{0\}$ und sei $z = \frac{a}{b} \in \mathbb{C}$. Dann existiert also ein $c \in \mathbb{Z}[i]$ mit $\delta(z - c) \leq \frac{1}{2}$. Setze $r = a - bc \in R$. Dann ist

$$\delta(r) = \delta(b)\delta\left(\frac{a}{b} - c\right) \leq \delta(b)\frac{1}{2} < \delta(b).$$

Damit ist $R = \mathbb{Z}[i]$ ein euklidischer Ring, also insbesondere ein Hauptidealring. □

Definition 4.2.8. Sei R ein Ring und $I \subset R$ ein Ideal. Wir zeigen gleich, dass die Relation

$$x \sim y \quad :\Leftrightarrow \quad x - y \in I$$

eine Äquivalenzrelation auf R ist. Die Menge der Äquivalenzklassen $R/\sim$ schreiben wir als R/I. Die Äquivalenzklasse der Null ist I.

Satz 4.2.9. (a) *Die Relation $\sim$ zu einem gegebenen Ideal ist eine Äquivalenzrelation.*

(b) *Auf der Menge R/I gibt es genau eine Ringstruktur, so dass die Projektion $\pi : R \to R/I$ ein Ringhomomorphismus ist. Für diesen Ringhomomorphismus gilt $I = \ker(\pi)$, also ist jedes Ideal der Kern eines Ringhomomorphismus.*

(c) *Sei $\sim$ eine Äquivalenzrelation so dass es auf der Quotientenmenge $R/\sim$ eine Ringstruktur gibt so dass die Projektion $\pi : R \to R/\sim$ ein Ringhomomorphismus ist, dann gibt es genau ein Ideal I mit*

$$x \sim y \quad \Leftrightarrow \quad x - y \in I.$$

Beweis. (a) Da I eine Untergruppe ist, sind Reflexivität und Symmetrie klar. Für die Transitivität sei $x \sim y$ und $y \sim z$, also $x - y, y - z \in I$. Dann ist die Summe dieser beiden Elemente, also $x - z$ ebenfalls in I, also $x \sim z$.

(b) Wir definieren Addition und Multiplikation durch $[a] + [b] = [a + b]$ und $[a][b] = [ab]$. Hier ist Wohldefiniertheit zu prüfen. Seien $a \sim a'$ und $b \sim b'$, also $a - a', b - b' \in I$, dann folgt

$$(a + b) - (a' + b') = (a - a') + (b - b') \in I$$

also folgt $(a + b) \sim (a' + b')$ und damit die Wohldefiniertheit der Addition. Für die Multiplikation rechne

$$\begin{aligned} ab - a'b' &= ab - ab' + ab' - a'b' \\ &= a(b - b') + (a - a')b' \in I. \end{aligned}$$

Die Eindeutigkeit der Ringstruktur ist wegen der Surjektivität von π klar.

(c) Sei $\sim$ eine solche Äquivalenzrelation und sei $I = \ker(\pi)$. Dann ist I ein Ideal und es

gilt

$$\begin{aligned} x \sim y &\Leftrightarrow \pi(x) = \pi(y) \\ &\Leftrightarrow \pi(x - y) = 0 \\ &\Leftrightarrow x - y \in I. \end{aligned}$$

□

Beispiel 4.2.10. Der Ring $\mathbb{Z}/m$ ist gleich $\mathbb{Z}/(m) = \mathbb{Z}/m\mathbb{Z}$.

Ein Ideal $\mathfrak{m}$ eines Rings R heisst *maximales Ideal*, wenn $\mathfrak{m} \neq R$ und $\mathfrak{m}$ ist maximal in der Menge aller Ideale $I \neq R$, also mit anderen Worten:

(a) $1 \notin \mathfrak{m}$ und

(b) ist I ein Ideal mit $\mathfrak{m} \subset I$ und $I \neq R$, dann ist $\mathfrak{m} = I$.

Satz 4.2.11. (a) *Jedes Ideal $I \neq R$ liegt in einem maximalen Ideal.*

(b) *Jedes Element von $R \setminus R^\times$ liegt in einem maximalen Ideal.*

(c) *Ein Ideal J ist genau dann maximal, wenn R/J ein Körper ist.*

Proof. (a) Sei $I \neq R$ ein Ideal und sei S die menge aller Ideale J mit $1 \notin J$ und $J \supset I$. Dann ist S mit der Inklusion partiell geordnet und die Kettenbedingung ist erfüllt, denn sei $\emptyset \neq K \subset S$ eine Kette, also eine linear geordnete Teilmenge und sei $\mathfrak{a} = \bigcup_{J \in K} J$, dann ist $\mathfrak{a}$ wieder ein Ideal und es gilt $I \subset \mathfrak{a}$, sowie $1 \notin \mathfrak{a}$. Dieses $\mathfrak{a}$ ist dann eine obere Schranke zu K. Nach dem Lemma von Zorn gibt es ein maximales Element $\mathfrak{m}$ in S, also liegt I in einem maximalen Ideal.

(b) Sei $r \in R \setminus R^\times$ eine Nichteinheit und sei $I = (r) = rR$ das Hauptideal. Dann gilt $1 \notin I$, da r nicht invertierbar ist. Also gibt es nach Teil (a) ein maximales Ideal, das I und damit auch r enthaelt.

(c) Sei J ein maximales Ideal und sei $r \in R \setminus J$. Wegen der Maximalitaet von J muss das Ideal $\langle r, J \rangle = rR + J$ gleich dem ganzen Ring sein, also auch die Eins enthalten, es gibt also $r' \in R$ und ein $\alpha \in J$ mit $rr' + \alpha = 1$ oder $rr' \in 1 + J$, so dass in R/J gilt $(r + J)(r' + J) = rr' + J = 1 + J$, das heisst, dass r im Quotienten R/J invertierbar ist, also ist in R/J jedes Element $\neq 0$ inverierbar, d.h., R/J ist ein Körper.

Sei umgekehrt R/J ein Körper und sei $r \in R \setminus J$, dann ist r modulo J invertierbar, also existiert ein $r' \in R$ mit $rr' \in 1 + J$, so dass $1 \in rR + J$, also ist J maximal. □

Beispiele 4.2.12.
- Die maximalen Ideale von $\mathbb{Z}$ sind genau die Hauptideale $p\mathbb{Z}$, wobei p eine Primzahl ist.
- Die maximalen Ideale von $R = \mathbb{C}[x]$ sind genau die Hauptideale der Form $I_\lambda = (x - \lambda)\mathbb{C}[x]$ für $\lambda \in \mathbb{C}$. Die Abbildung $f(x) \mapsto f(\lambda)$ induziert einen Isomorphismus
$$R/I_\lambda \cong \mathbb{C}.$$

Definition 4.2.13. Ein Ideal $I \neq R$ eines Rings R heisst *Primideal*, falls

$$ab \in I \quad \Rightarrow \quad a \in I \text{ oder } b \in I.$$

Satz 4.2.14. *Ein Ideal I von R ist genau dann ein Primideal, wenn R/I integer ist.*

Beweis. Sei I ein Primideal und seien $[a], [b] \in R/I$ mit $[a][b] = [0]$, also $0 = [ab]$ was soviel heisst wie $ab \in I$. Da I ein Primideal ist, folgt $a \in I$ oder $b \in I$, also sagen wir, es sei $a \in I$. das heisst aber $[a] = [0]$, also ist $[a]$ in R/I das Nullelement, damit ist R/I integer.

Sei umgekehrt R/I integer und seien $a, b \in R$ mit $ab \in I$. Das bedeutet $[0] = [ab] = [a][b]$. Da R/I integer ist, folgt $[a] = [0]$ oder $[b] = [0]$ also sagen wir $[a] = [0]$, also $a \in I$ und damit ist I ein Primideal. □

4.3 Teilbarkeit

Definition 4.3.1. Seien a, b Elemente eines Rings R.

(a) Man sagt *a teilt b* oder ist ein *Teiler* von b, falls es ein $c \in R$ gibt so dass $ac = b$. in diesem Fall schreibt man $a \mid b$. Ist a kein Teiler von b, so schreibt man $a \nmid b$.

(b) a und b heißen *assoziiert*, wenn es eine Einheit $u \in R^\times$ gibt mit $a = bu$.

Beispiele 4.3.2.
- Für zwei natürliche Zahlen m, n gilt m teilt n in $\mathbb{Z}$ genau dann, wenn m ein Teiler im üblichen Sinne ist.
- Zwei Elemente a, b in $\mathbb{Z}$ sind genau dann assoziiert, wenn $a = \pm b$ gilt.

Lemma 4.3.3. *Für zwei Elemente a, b eines Integritaetsrings R sind äquivalent*

(i) $a \mid b$ *und* $b \mid a$,

(ii) $aR = bR$,

(iii) *a und b sind assoziiert.*

Beweis. (i)⇒(iii): Es gelte $a = bc$ und $b = ad$. Wir nehmen an, dass $a \neq 0$, da sonst auch $b = 0$. Es ist $a = bc = acd$, also $a(1 - cd) = 0$ und da $a \neq 0$ und R integer ist, folgt $cd = 1$, also sind c, d Einheiten und a und b sind assoziiert.

(iii)⇒(ii) Es sei $a = bu$ mit einer Einheit u. Wegen $uR = R$ folgt dann $aR = buR = bR$.

(ii)⇒(i) Sei $aR = bR$, dann folgt $a \in bR$, also gibt es ein $c \in R$ mit $a = bc$, also $b \mid a$. Ebenso folgt $b \mid a$. □

Definition 4.3.4. Sei R ein Integritätsring und p ein Element, das weder Null noch eine Einheit ist.

(a) Das Element p heißt *irreduzibel*, falls aus der Gleichung $p = ab$ in R stets folgt, dass a oder b eine Einheit ist.

(b) Das Element p heißt *Primelement*, falls aus $p \mid ab$ stets folgt $p \mid a$ oder $p \mid b$.

Beispiele 4.3.5.

- In $R = \mathbb{Z}$ sind die Primelemente genau die Elemente der Form $\pm p$, wobei p eine Primzahl ist.
- In $R = \mathbb{C}[x]$ sind die Primelemente genau die Elemente $c(x - a)$ mit $c \in \mathbb{C}^\times$, $a \in \mathbb{C}$.
- In $R = \mathbb{R}[x]$ sind die Primelemente genau die Polynome der Form $c(x - \alpha)$ für ein $\alpha \in \mathbb{R}$ oder $c(x^2 + ax + b)$, falls dieses Polynom keine reelle Nullstelle hat.

Proposition 4.3.6. *Sei R ein Integritätsring. Dann ist jedes Primelement von R auch irreduzibel.*

Beweis. Seien p ein Primelement und sei $p = ab$. Dann teilt p das Produkt ab also teilt p einen der Faktoren, sagen wir a. Das heißt $a = pc = abc$, also $a(1 - bc) = 0$, also $bc = 1$, so dass b eine Einheit ist. □

Beispiel 4.3.7. In dem Integritätsring $R = \mathbb{Z}[\sqrt{-5}]$ ist das Element 3 irreduzibel, aber kein Primelement.

Beweis. Sei $\alpha = i\sqrt{5}$. Wir zeigen, dass 3 irreduzibel ist. Ist $3 = zw$ in R, dann folgt $9 = |3|^2 = |z|^2|w|^2$. Ist $|z|^2 = 1$, dann ist $z = \pm 1$ eine Einheit. Ist $|z|^2 = 9$, dann ist $|w|^2 = 1$ und w ist eine Einheit. *Angenommen,* $|z|^2 = 3$. Sei $z = a + b\alpha$, dann ist $3 = |z|^2 = a^2 + 5b^2$, also ist $b = 0$, da der Betrag sonst zu gross wäre. Dann ist $3 = a^2$, aber 3 ist kein Quadrat in $\mathbb{Z}$, *Widerspruch!* Also ist 3 irreduzibel.

Wir zeigen, dass 3 kein Primelement ist. Hierzu beachte, dass $3 \mid 9 = (2 + \alpha)(2 - \alpha)$, aber 3 teilt keinen der Faktoren, denn würde 3 etwa $2 + \alpha$ teilen, also $2 + \alpha = 3z$, dann ist $9 = |2 + \alpha|^2 = |3|^2|z|^2$, also $|z| = 1$ und damit ist $z = \pm 1$, was ein Widerspruch ist. □

Satz 4.3.8. *Sei R ein Hauptidealring und sei $p \in R$. Dann sind äquivalent*

(a) *p irreduzibel,*

(b) *p ist ein Primelement.*

Beweis. Wir müssen nur (a)⇒(b) zeigen: Sei p irreduzibel und p teile ab und $p \nmid a$. Wir muessen zeigen, dass p das Element b teilt. Sei I das von p und a erzeugte Ideal, also $I = aR + pR$. Dann ist dies ein Hauptideal, also etwa $I = (c)$. Dann folgt $c \mid a$ und $c \mid p$, also etwa $cd = p$. Da p irreduzibel ist, ist c oder d eine Einheit. Ist d eine Einheit, so ist $pR = cR = I = aR + pR$, also ist $a \in pR$, d.h. p teilt a, was der Voraussetzung widerspricht. Also ist c eine Einheit, d.h., $I = R$ und es gibt $r, s \in R$ mit $ar + ps = 1$, also $b = abr + psb = p(r + sb)$, also $p \mid b$ wie verlangt. □

Korollar 4.3.9. *In einem Hauptidealring R lässt sich jedes Element von $R \setminus \{0\}$, das keine Einheit ist, als endliches Produkt von Primelementen Schreiben.*

Beweis. Da jedes irreduzible Element prim ist, genügt es, eine Zerlegung in irreduzible zu konstruieren. Sei $a \in R$ ungleich Null und keine Einheit. *Angenommen*, a lässt sich nicht als Produkt von Irreduziblen schreiben. Dann ist a reduzibel und kann selbst als Produkt $a_1 a_1'$ von Nichteinheiten geschrieben werden. Da a kein Produkt von Irreduziblen ist, gilt dasselbe für mindestens einen der Faktoren, sagen wir a_1, und a_1 kann als Produkt $a_2 a_2'$ zweier Nichteinheiten geschrieben werden. Iteration liefert eine Folge von Elementen

$$a = a_0, a_1, \cdots \in R$$

so dass a_{j+1} ein Teiler von a_j, aber nicht assoziiert zu a_j ist. Also folgt für die Hauptideale

$$(a) = (a_0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \dots$$

Man prüft leicht nach, dass die Vereinigung einer aufsteigenden Folge von Idealen wieder ein Ideal ist, also ist

$$\bigcup_{j \in \mathbb{N}} (a_j)$$

wieder ein Ideal in R, also ein Hauptideal (b). Dann ist $b \in (a_j)$ für ein j und daher

$$(b) \subset (a_j) \subset (a_{j+1}) \subset (b),$$

woraus Gleichheit folgt, ein *Widerspruch!* Daher ist die Annahme falsch, also ist jedes Element als Produkt von Irreduziblen darstellbar. □

Lemma 4.3.10. *Gilt in einem Integritätsring R die Gleichung*

$$p_1 \cdots p_r = q_1 \cdots q_s$$

für Primelemente p_j und irreduzible Elemente q_i, dann ist $r = s$ und nach Umnummerierung ist jedes p_j assoziiert zu q_j.

Beweis. Da $p_1 \mid q_1 \cdots q_s$, gibt es ein j mit $p_1 \mid q_j$. Nach Umnummerierung können wir $p_1 \mid q_1$ annehmen. Es folgt $q_1 = \varepsilon_1 p_1$, wobei ε_1 auf Grund der Irreduzibilität von q_1 eine Einheit ist. Da wir uns in einem Integritätsring befinden, folgt

$$p_2 \cdots p_r = \varepsilon_1 q_2 \cdots q_s.$$

Wir iterieren diesen Vorgang und können die q_i so umnummerieren, dass p_j zu q_j assoziiert ist. Insbesondere folgt $r \leq s$. Ist $r < s$ erhalten wir

$$1 = \varepsilon q_{r+1} \cdots q_s,$$

woraus folgt, dass q_s eine Einheit ist, was ein Widerspruch ist, also ist $r = s$. □

Definition 4.3.11. Ein Integritätsring R heißt *faktoriell*, falls jede Nichteinheit in $R \setminus \{0\}$ als Produkt von Primelementen darstellen lässt, das heißt wenn wir eine sogenannte **eindeutige Primfaktorzerlegung** haben.

Satz 4.3.12. *Jeder Hauptidealring ist faktoriell. Insbesondere ist $\mathbb{Z}$ faktoriell und für jeden Körper K ist der Polynomring $K[x]$ faktoriell.*

Beweis. Folgt aus Korollar 4.3.9 und Lemma 4.3.10. □

Beispiel 4.3.13. Der Ring $R = \mathbb{Z}[\sqrt{-5}]$ is nicht faktoriell, denn wir haben die Zerlegungen

$$6 = 2 \cdot 3 = \left(1 + \sqrt{-5}\right) \cdot \left(1 - \sqrt{-5}\right)$$

und unter den Elementen $2, 3, \left(1 + \sqrt{-5}\right), \left(1 - \sqrt{-5}\right)$ sind keine zwei assoziiert, denn die Einheiten dieses Rings sind ± 1.

Definition 4.3.14. Sei R ein faktorieller Ring. Sei P ein Vertretersystem der Primelemente modulo Assoziiertheit, also P enthalte zu jeder Klasse von assoziierten Primelementen genau ein Element. Hat man ein solches P fest gewählt, kann man jede Nichteinheit $z \in R \setminus \{0\}$ eindeutig in der Form

$$z = \varepsilon \prod_{p \in P} p^{k_p}$$

schreiben, wobei ε eine Einheit ist und $k_p \in \mathbb{N}_0$, fast alle Null sind. Sind dann

$$z = \varepsilon \prod_{p \in P} p^{k_p}, \qquad w = \eta \prod_{p \in P} p^{n_p}$$

zwei solche Darstellungen, dann ist klar, dass z das Element w genau dann teilt, wenn $k_p \leq n_p$ für jedes $p \in P$ gilt. Wir definieren wir den *größten gemeinsamen Teiler* der Elemente z, w als

$$\mathrm{ggT}(z, w) = \prod_{p \in P} p^{\min k_p, n_p},$$

sowie das *kleinste gemeinsame Vielfache* als

$$\mathrm{kgV}(z, w) = \prod_{p \in P} p^{\max k_p, n_p}$$

Beispiele 4.3.15.

- Im Fall $R = \mathbb{Z}$ kann man die Menge der Primzahlen als P nehmen.
- Im Fall $R = K[x]$ für einen Körper K sind die Einheiten genau die konstanten in

$K^\times$, also ist jedes Polynom zu einem eindeutig bestimmten normierten Polynom assoziiert. Damit kann man als P die Menge aller normierter Primpolynome wählen.

- Im Allgemeinen hat man keine kanonische Wahl für P. Daher hängen die Begriffe ggT und kgV dann von der Wahl von P ab und sind daher nur bis auf Assoziiertheit definiert.

Satz 4.3.16. *Seien a, b zwei von Null verschiedene Elemente eines Hauptidealrings R.*

(a) *Ein Element z teilt genau dann sowohl a als auch b, wenn z den* ggT *von a und b teilt.*

(b) *Ein Element w ist genau dann ein Vielfaches sowohl von a als auch von b, wenn w ein Vielfaches von* $\mathrm{kgV}(a, b)$ *ist.*

(c) *Für den größten gemeinsamen Teiler $d = \mathrm{ggT}(a, b)$ gilt dann*

$$aR + bR = dR.$$

Insbesondere gibt es Elemente $x, y \in R$ mit

$$\mathrm{ggT}(a, b) = ax + by.$$

Beweis. (a) und (b) sind klar, wenn man die Produktzerlegungen betrachtet.

(c) Das Ideal $aR + bR$ ist ein Hauptideal, etwa $aR + bR = d'R$. Wegen $a, b \in (d')$ ist d' dann ein gemeinsamer Teiler von a und b, teilt demnach d. Andererseits teilt d auch a und b und teilt demnach d', so dass d und d' assoziiert sind. □

Korollar 4.3.17. *Sei R ein Hauptidealring und $p \in R \setminus \{0\}$. Dann sind äquivalent;*

(a) *p ist ein Primelement.*

(b) *R/pR ist ein Körper.*

Beweis. Sei p ein Primelement und sie $\bar{z} \in R/pR \setminus \{0\}$ die Äquivalenzklasse von $z \in R$. Dass $\bar{z} \neq 0$ ist bedeutet, dass $z \notin pR$ ist, was bedeutet, dass p in der Primfakorzerlegung

von z nicht vorkommt und damit ist $\mathrm{ggT}(z,p) = 1$. Daher ist $zR + pR = R$, also gibt es $x, y \in R$ mit $zx + py = 1$, oder $\bar{z}\bar{x} = 1$ in R/pR, so dass $\bar{z}$ invertierbar ist.

Für die Umkehrung sei R/pR ein Körper und p teile ein Produkt ab. Dann ist $\bar{a}\bar{b} = 0$ und daher $\bar{a} = 0$ oder $\bar{b} = 0$, also $p \mid a$ oder $p \mid b$. □

Beispiel 4.3.18. $\mathbb{Z}/m$ ist genau dann ein Körper, wenn $m = p$ eine Primzahl ist. In diesem Fall schreibt man $\mathbb{F}_p = \mathbb{Z}/p$.

4.4 Lokalisierung

Sei R ein Integritaetsring und sei $S \subset R$ eine *multiplikativ abgeschlossene Teilmenge*, d.h., wir fordern

- $0 \notin S$, $1 \in S$,
- $x, y \in S \;\Rightarrow\; xy \in S$.

Beispiele 4.4.1.

- Sei $f \in R \setminus \{0\}$ und sei $S = \{1, f, f^2, \dots\}$, dann ist S eine multiplikativ abgeschlossene Teilmenge.
- Ist $\mathfrak{p} \subset R$ ein Primideal, dann ist das Komplement $S = R \setminus \mathfrak{p}$ eine multiplikativ abgeschlossene Teilmenge.
- Da R ein Integritaetsring ist, ist $S = R \setminus \{0\}$ eine multiplikativ abgeschlossene Teilmenge.

Definition 4.4.2. Sei S eine multiplikativ abgeschlossene Teilmenge des Integritaetsrings R. Die *Lokalisierung* von R nach S ist der Unterring $S^{-1}R$ des Quotientenkoerpers $\mathrm{Quot}(R)$, der von R und

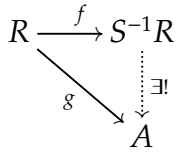
$$S^{-1} = \{s^{-1} : s \in S\}$$

erzeugt wird. Da S multiplikativ abgeschlossen ist, gilt

$$S^{-1}R = \left\{ \frac{a}{s} : a \in R,\ s \in S \right\}.$$

Proposition 4.4.3. *Die Lokalisierung $S^{-1}R$ ist der kleinste Ring, in dem S invertierbar wird. Genauer gilt folgende universelle Eigenschaft: Ist A ein Ring und $g : R \to A$ ein*

Ringhomomorphismus dergestalt, dass $g(S) \subset A^\times$, dann existiert genau ein Ringhomomorphismus $S^{-1}R \to A$ der das Diagramm



kommutativ ist.

Beweis. Sei $g : R \to A$ mit $g(S) \subset A^\times$. Wir definieren dann $\psi : S^{-1}R \to A$ durch $\psi\left(\frac{a}{s}\right) = g(a)g(s)^{-1}$. Dann ist ψ der eindeutig bestimmte Ringhomomorphismus, der das Diagramm kommutativ macht. □

Beispiele 4.4.4.

- Ist $R = \mathbb{Z}$ und $S = \mathbb{Z} \setminus \{0\}$, dann ist $S^{-1}\mathbb{Z} = \mathbb{Q}$.
- Ist $R = K[x]$ der Polynomring über einem Körper K, dann ist der Quotientenkoerper der Körper $K(x)$ der *rationalen Funktionen* über K.

4.5 Moduln

Definition 4.5.1. Ein *Modul* über einem Ring R ist eine abelsche Gruppe M mit einer Abbildung

$$\begin{aligned} R \times M &\to M \\ (\lambda, m) &\mapsto \lambda m, \end{aligned}$$

so dass für alle $\lambda, \mu \in R$ und alle $m, n \in M$ gilt

- $1_R m = m$,
- $(\lambda\mu)m = \lambda(\mu m)$,
- $(\lambda + \mu)m = \lambda m + \mu m, \quad \lambda(m + n) = \lambda m + \lambda n.$

Beispiele 4.5.2.

- Für einen Körper K sind die K-Moduln genau die K-Vektorraeume.
- Der Ring R selbst ist ein R-Modul und eine Teilmenge $T \subset R$ ist genau dann ein Untermodul, wenn T ein Ideal ist.

- Jede abelsche Gruppe $(M, +)$ ist auf genau eine Weise ein Modul unter $R = \mathbb{Z}$, denn $km = m + \cdots + m$ mit k-Kopien, wenn $k \in \mathbb{N}$ und es ist das Inverse, wenn $k < 0$. Es gilt also
$$\left\{\text{abelsche Gruppen}\right\} \;=\; \left\{\mathbb{Z}\text{-Moduln}\right\}$$
Es gilt auch, dass ein Gruppenhomomorphismus zwischen zwei abelschen Gruppen dasselbe ist, wie ein $\mathbb{Z}$-Modulhomomorphismus.

- Sei K ein Körper und R der Polynomring $K[x]$. Sei V ein K-Vektorraum und $T : V \to V$ ein Endomorphismus. Dann wird V ein R-Modul durch
$$(f(x))v := f(T)v.$$
Ist also $f(x) = a_0 + \cdots + a_n x^n$, so ist
$$f(x)v = a_0 v + a_1 Tv + \cdots + a_n T^n v.$$

Definition 4.5.3. Eine *R-lineare Abbildung* oder ein *Modulhomomorphismus* zwischen zwei Moduln ist ein Gruppenhomomorphismus $\phi : M \to N$ mit der Eigenschaft
$$\Phi(rm) = r\phi(m)$$
für jedes $m \in M$ und jedes $r \in R$.

Definition 4.5.4. Ein *Untermodul* eines R-Moduls M ist eine Teilmenge $N \subset M$, die mit den Strukturen von M selbst wieder ein Modul ist.

Beispiel 4.5.5. Eine Teilmenge $I \subset R$ ist genau dann eine Untermodul, wenn sie ein Ideal ist.

Definition 4.5.6. Seien $M_1, \ldots, M_k$ Untermoduln eines Moduls M, dann ist die *Summe* der Moduln definiert als
$$U = M_1 + \cdots + M_k := \left\{m_1 + \cdots + m_k : m_j \in M_j\right\} \subset M.$$
Dies ist ein Untermodul, wie man leicht sieht. Gilt zusätzlich
$$m_1 + \cdots + m_k = m_1' + \cdots + m_{k'}' \quad \Rightarrow \quad k = k', m_1 = m_1', \ldots, m_k = m_k'$$
wobei $m_j, m_j' \in M_j$ für $1 \leq j \leq k$, so sagen wir, die Summe ist **direkt** und schreiben dies

als

$$U = M_1 \oplus \cdots \oplus M_k.$$

Dann ist die Summe $U + V$ zweier Untermoduln genau dann direkt, wenn $U \cap V = 0$ gilt. Ist $U \oplus V = M$, sagen wir, die Moduln U und V sind *komplementär*.

Beispiel 4.5.7. Ein Untervektorraum hat stets einen komplementären Unterraum. Dies gilt für Moduln nicht. Hier ist das Beispiel: Sei $R = \mathbb{Z}$ und $M = \mathbb{Z}$ also Modul betrachtet. Dann ist $2M = 2\mathbb{Z}$ ein Untermodul ohne Komplementärmodul.

Definition 4.5.8. Sind $N_1, \ldots, N_k$ Moduln über R, die nicht Untermoduln eines gemeinsamen Moduls sind, so lässt sich die direkte Summe $N_1 \oplus \cdots \oplus N_k$ auch konstruieren. Setze

$$M = N_1 \times \cdots \times N_k,$$

so ist N_j via $n \mapsto (0, \ldots, 0, n, 0, \ldots, 0)$ als Untermodul von M auffassen und es gilt dann

$$M = \bigoplus_{j=1}^{k} N_j.$$

Definition 4.5.9. Ist $U \subset M$ ein Untermodul, so definieren wir eine Äquivalenzrelation $\sim$auf M durch

$$m \sim n \quad :\Leftrightarrow \quad m - n \in U.$$

Wir schreiben M/U für die Menge der Äquivalenzklassen.

Lemma 4.5.10. *M/U trägt eine eindeutig bestimmte Struktur eines R-Moduls, so dass die Projektion $\pi : M \to M/U$ ein Modulhomomorphismus ist. Der Kern von π ist U.*

Beweis. Man definiert $[m] + [n] = [m + n]$ und $r[m] = [rm]$ und weist Wohldefiniertheit wie üblich nach. □

Beispiel 4.5.11. Im Falle $R = \mathbb{Z}$ betrachte den Modul $M = \mathbb{Z}$ und den Untermodul $k\mathbb{Z}$ für ein $k \in \mathbb{N}$. Dann ist $M/U = \mathbb{Z}/k\mathbb{Z}$ der uebliche Restklassenmodul.

Definition 4.5.12. Sei M ein R-Modul. Ein*Erzeugendensystem* ist eine Familie $(m_i)_{i \in I}$ in M so dass jedes $m \in M$ als Linearkombination

$$m = \sum_{i \in I} r_i m_i,$$

mit $r_i \in R$, fast alle Null, geschrieben werden kann. Eine Familie $(v_i)_{i\in I}$ heißt *linear unabhängig*, wenn es nur eine Linearkombination der Null gibt, wenn also aus

$$\sum_{i\in I} r_i m_i = 0$$

schon $r_i = 0$ für alle i folgt. Ein linear unabhängiges Erzeugendensystem nennt man eine *Basis* des Moduls. Ein Modul heißt *freier Modul*, wenn er eine Basis hat. Er heißt *endlich-frei*, falls er eine endliche Basis hat.

Bemerkung. Nicht jeder Modul hat eine Basis. Als Beispiel sei $m \in \mathbb{N}$ und betrachte $\mathbb{Z}/m$ als $\mathbb{Z}$-modul. Dann gibt es in $\mathbb{Z}/m$ keine linear unabhängige Familie, denn für jedes $z \in \mathbb{Z}/m$ gilt $mz = 0$, aber $m \neq 0$ in $\mathbb{Z}$.

Proposition 4.5.13. *Ist M ein endlich-freier Modul eines Rings R, dann ist M isomorph zu R^n für ein n und dieses n ist eindeutig bestimmt, man nennt es die* Dimension *von M.*

Proof. Sei $m_1, \dots, m_s$ eine Basis von M und sei J ein maximales Ideal von R. Dann ist M/JM ein Vektorraum über dem Körper $k = R/J$. wir behaupten, dass $m_1, \dots, m_s$ eine Basis ist. Es ist klar, dass es ein Erzeugendensystem ist, seien also $\lambda_1, \dots, \lambda_s \in R$ mit

$$\lambda_1 m_1 + \cdots + \lambda_s m_s \equiv 0 \mod JM,$$

also $\lambda_1 m_1 + \cdots + \lambda_s m_s \in JM$. Nun ist JM die Menge aller Linearkombinationen der Form

$$\sum_{\nu=1}^{k} \alpha_\nu v_\nu,$$

wobei $\alpha_\nu \in J$ und $v_\nu \in M$ ist. Schreibt man jedes v_ν als Linearkombination der Basis $m_1, \dots, m_s$ und nutzt aus, dass J ein Ideal ist, sieht man, dass die Elemente von JM genau die Elemente von der Form

$$\mu_1 m_1 + \cdots + \mu_s m_s$$

sind für die $\mu_1, \dots, \mu_s \in J$ gilt. Insbesondere gibt es also $\mu_1, \dots, \mu_s \in J$, so dass

$$\lambda_1 m_1 + \cdots + \lambda_s m_s = \mu_1 m_1 + \cdots + \mu_s m_s.$$

Da aber die m_j eine Basis bilden, folgt $\lambda_1 = \mu_1, \dots, \lambda_s = \mu_s$, die liegen alle in J, also folgt $\lambda_1 \equiv 0, \dots, \lambda_s \cong 0 \mod J$, damit sind die $m_1, \dots, m_s$ linear unabhängig in M/JM. Damit

ist s die Dimension des R/J-Vektorraums M/JM, haengt also nicht von der Wahl der Basis ab. □

Definition 4.5.14. Sei M ein R=Modul. Die *Länge* des Moduls M, geschrieben $\ell(M) = \ell_R(M)$ ist das Supremum der Längen ℓ von Ketten von Untermoduln

$$0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_\ell = M$$

Beispiele 4.5.15.

- Ist $R = K$ ein Körper, dann ist die Länge eines Moduls (=Vektorraums) gleich seiner Dimension.
- Eine abelsche Gruppe $(M, +)$, aufgefasst als $\mathbb{Z}$-Modul hat genau dann endliche Länge, wenn sie endlich ist. Die Länge des $\mathbb{Z}$-Moduls $\mathbb{Z}/m$ für $m \in \mathbb{N}$ ist gleich der Anzahl aller Primteiler von m, mit Vielfachheit gezaehlt.

Lemma 4.5.16. *Sei R ein Hauptidealring und sei $a \in R \setminus \{0\}$ mit Primfaktorzerlegung $a = \varepsilon p_1 \cdots p_r$. Dann hat der Restklassenmodul R/aR die Länge $\ell_R(R/aR) = r$.*

Beweis. Sei $\pi : R \to R/aR$ die Projektion. Die Untermoduln $U \subset R/aR$ entsprechen bijektiv ihren Urbildern unter π und dies sind die Ideale I von R, die aR enthalten, so dass die Länge mit dem Supremum aller Längen von Idealketten der Art

$$aR \subsetneq I_1 \subsetneq \cdots \subsetneq I_l = R$$

übereinstimmt. Da R ein Hauptidealring ist, wird jedes I_ν von einem Element a_ν erzeugt. Die Inklusion $I_\nu \subsetneq I_{\nu+1}$ bedeutet, dass a_ν ein echter Teiler von $a_{\nu+1}$ ist. Daher müssen die Potenzen in der Primfaktorzerlegung absteigen und die maximale Länge einer solchen Kette ist r. □

Lemma 4.5.17. *Ist M die direkte Summe zweier Untermoduln L und N, so gilt*

$$\ell(M) = \ell(L) + \ell(N).$$

Beweis. Seien

$$0 \subsetneq L_1 \subsetneq \cdots \subsetneq L_r = M_1,$$
$$0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_s = M_2$$

echt aufsteigende Ketten von Untermoduln, dann ist

$$0 \subsetneq (L_1 \oplus 0) \subsetneq \cdots \subsetneq (L_r \oplus 0) \subsetneq (L_r \oplus N_1) \subsetneq \cdots \subsetneq (L_r \oplus N_r) = M$$

eine Kette in M, also ist $\ell(L) + \ell(N) \leq \ell(M)$.

Für die umgekehrte Richtung sei

$$0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_\ell = M$$

eine echt aufsteigende Kette von Untermoduln. Seien π_L und π_N die Projektionen auf die beiden Summanden L und N. Ist etwa $M_j \cap L = M_{j+1} \cap L$, dann behaupten wir, dass $\pi_N(M_j) \neq \pi_N(M_{j+1})$ ist, denn gilt auch hier Gleichheit, dann gibt es zu $m \in M_{j+1}$ ein $\tilde{m} \in M_j$ mit $\pi_N(m) = \pi_N(\tilde{m})$, also ist $m - \tilde{m} \in \ker \pi_N \cap M_{j+1} = L \cap M_{j+1} = L \cap M_j$ und damit ist $m \in M_{j+1}$, was ein Widerspruch zu $M_j \neq M_{j+1}$ ist. Damit wächst bei jedem j entweder $M_j \cap L$ oder $\pi_N(M_j)$ und so folgt $\ell \leq \ell(L) + \ell(N)$. □

Lemma 4.5.18. *Sei R ein Hauptidealring und Q ein Modul mit*

$$Q \cong \bigoplus_{j=1}^{n} R/\alpha_j R,$$

wobei $\alpha_j \in R \setminus 0$ Nichteinheiten so dass $\alpha_j \mid \alpha_{j+1}$ für $1 \leq j \leq n-1$, dann sind die α_j bis auf Assoziiertheit durch den Modul Q eindeutig bestimmt.

Beweis. Aus technischen Gründen invertieren wir die Nummerierung der α_j und betrachten zwei Zerlegungen

$$Q \cong \bigoplus_{j=1}^{n} R/\alpha_j R \cong \bigoplus_{j=1}^{m} R/\beta_j R,$$

mit $\alpha_{j+1} \mid \alpha_j$ und desgleichen für β_i. Falls es einen Index $k \leq \min(m, n)$ mit $\alpha_k R \neq \beta_k R$ gibt, so wähle k minimal mit dieser Eigenschaft. Da $\alpha_i R = \beta_i R$ für $1 \leq i < k$, und da $\alpha_{k+1}, \ldots, \alpha_n$ sämtlich Teiler von α_k sind, zerlegt sich $\alpha_k Q$ zu

$$\begin{aligned} \alpha_k Q &\cong \bigoplus_{i=1}^{k-1} \alpha_k \cdot (R/\alpha_i R) \\ &\cong \bigoplus_{i=1}^{k-1} \alpha_k \cdot (R/\alpha_i R) \oplus \bigoplus_{j=k}^{m} \alpha_k \cdot (R/\beta_j R) \end{aligned}$$

As Lemma 4.5.16 und Lemma 4.5.17 folgt $\ell\left(\alpha_k \cdot (R/\beta_j R)\right) = 0$ für $k \leq j \leq m$. Dies bedeutet aber insbesondere $\alpha_k \cdot (R/\beta_k R) = 0$, oder $\alpha_k R \subset \beta_k R$. Analog zeigt man $\alpha_k R \supset \beta_k R$, also $\alpha_k R = \beta_k R$, also gibt es solches k gar nicht. □

4.6 Der Elementarteilersatz

Definition 4.6.1. Wir betrachten Matrizen über einem beliebigen Ring R. Eine Matrix $A \in \mathrm{M}_n(R)$ heißt *invertierbar*, falls es eine Matrix $B \in \mathrm{M}_n(R)$ gibt, mit $AB = BA = I$.

Lemma 4.6.2. *Sei R ein kommutativer Ring mit Eins. Eine Matrix $A \in \mathrm{M}_n(R)$ ist genau dann invertierbar, wenn* $\det(A) \in R$ *eine Einheit ist.*

Beweis. Sei $A^\#$ die Komplementärmatrix. Man stellt fest, dass in dem Beweis der Formel

$$AA^\# = A^\#A = \det(A)I$$

nirgends benutzt wurde, dass man über einem Körper rechnet. Er gilt also auch über R. Ist also $\det(A) \in R^\times$, so ist $\det(A)^{-1}A^\#$ eine inverse zu A.

Für die Umkehrung sei A invertierbar. Man stellt fest, dass auch die Formel

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

über beliebigen Ringen gilt. Ist B eine Inverse, so folgt $\det(A)\det(B) = 1$, also ist $\det(A)$ eine Einheit. □

Beispiel 4.6.3. Eine Matrix $A \in \mathrm{M}_n(\mathbb{Z})$ ist genau dann in $\mathrm{M}_n(\mathbb{Z})$ invertierbar, wenn gilt $\det(A) = \pm 1$. Wir bestimmen also mal die Inverse zu $\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$. Es ist

$$\begin{aligned}
\left(\begin{array}{cc|cc} 1 & 2 & 1 & \\ 1 & 1 & & 1 \end{array}\right) &\rightsquigarrow \left(\begin{array}{cc|cc} 1 & 2 & 1 & \\ 0 & -1 & -1 & 1 \end{array}\right) \\
&\rightsquigarrow \left(\begin{array}{cc|cc} 1 & 2 & 1 & \\ 0 & 1 & 1 & -1 \end{array}\right) \\
&\rightsquigarrow \left(\begin{array}{cc|cc} 1 & 0 & -1 & 2 \\ 0 & 1 & 1 & -1 \end{array}\right).
\end{aligned}$$

Wir stellen also fest, dass $\begin{pmatrix} -1 & 2 \\ 1 & -1 \end{pmatrix}$ die gesuchte Inverse ist.

Satz 4.6.4 (Elementarteilersatz für Matrizen)**.** *Sei R ein Hauptidealring und $A \in \mathrm{M}_n(R)$ eine quadratische Matrix über R. Dann existieren invertierbare Matrizen*

$S, T \in \mathrm{GL}_n(R)$ *mit*

$$SAT = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix},$$

wobei $d_{k+1} = \cdots = d_n = 0$ *für ein* k *und* $d_j \mid d_{j+1}$ *für* $1 \leq j \leq k-1$ *gilt. Dabei sind die* d_j *bis auf Assoziiertheit eindeutig bestimmt, man nennt sie die* Elementarteiler *der Matrix* A.

Beweis. Wir wenden Zeilen und Spaltentransformationen an, diese sind jeweils durch Multiplikation von links oder rechts mit invertierbaren Matrizen gegeben. Unsere Transformationen sind

(a) Multiplikation einer Zeile (oder Spalte) mit einer Einheit,

(b) Addition des r-fachen einer Zeile (oder Spalte) zu einer anderen,

(c) Vertauschen von zwei Zeilen (oder Spalten).

Es kommt noch eine weitere Transformation hinzu. Nimm hierzu an, dass die erste Spalte von A wie folgt aussieht: $(a, *, \ldots, *, b, * \ldots)^t$, wobei b an der k-ten Position steht. Sei $d = \mathrm{ggT}(a, b)$, dann existieren $x, y \in R$ mit $d = ax + by$. Es gilt dann $c = \mathrm{ggT}(x, y) = 1$, denn cd teilt d. Also existieren $r, w \in R$ mit $rx - wy = 1$. Die Matrix

$$S = \begin{pmatrix} x & & y & \\ & I & & \\ w & & r & \\ & & & I \end{pmatrix},$$

ist invertierbar und Multiplikation von links mit S liefert die erste Spalte $(d, *, \alpha d, *)^t$, so dass man anschließend, das α-fache der ersten Spalte von der k-ten abziehen kann, wiederholt dieses und erhält eine erste Spalte der Form $(d, 0, \ldots, 0)^t$.

Durch Rechtsmultiplikation mit invertierbaren Matrizen kann man dies auch mit der ersten Zeile ausfuehren und bringt A in die Form $\begin{pmatrix} d & 0 \\ 0 & B \end{pmatrix}$ für ein eventuell anderes d. Man addiert nun die erste Zeile zur zweiten und wiederholt die Spaltentrafos für die

zweite Zeile bis man zu eine Matrix der Form

$$\begin{pmatrix} d & rd \\ d' & sd' \\ 0 & * \end{pmatrix}$$

kommt. Hierbei ist d' ein Teiler von d. Dies führt zu

$$\begin{pmatrix} d' & 0 \\ 0 & td' \\ 0 & * \end{pmatrix}$$

Man wiederholt den Vorgang mit den anderen Zeilen, bis man eine Matrix der Gestalt

$$\begin{pmatrix} d & \\ & dB \end{pmatrix}$$

erhält (wieder ein anderes d). Man wiederholt dies nun mit B an Stelle von A und erhält die Behauptung durch Iteration.

Zur Eindeutigkeit: Sei $M = AR^n = \text{Bild}(A)$ und sei $F = \left\{x \in R^n : \exists_{r \in R} rx \in M\right\}$. Dann ist $F/M = \bigoplus_{j=1} kR/\alpha_j R$ und die Eindeutigkeitsaussage aus Lemma 4.5.18 liefert die Eindeutigkeit. □

Satz 4.6.5 (Elementarteilersatz für Moduln)**.** *Sei R ein Hauptidealring und F ein endlich-freier Modul, sowie $M \subset F$ ein Untermodul. Dann existieren Elemente $x_1, \ldots, x_k$ von F, die Teil einer Basis sind, sowie Koeffizienten $a_1, \ldots, a_k \in R$ mit*

- *$a_i \mid a_{i+1}$ falls $1 \leq i \leq k-1$ und*
- *$a_1 x_1, \ldots, a_k x_k$ ist eine Basis von M.*

Die a_j sind bis auf Assoziiertheit durch M eindeutig bestimmt, sie werden die Elementarteiler *von M genannt.*

Insbesondere folgt: Ein Untermodul eines endlich-freien Moduls ist endlich-frei!

Beweis. Sei $b_1, \ldots, b_n$ eine Basis von F. Wir zeigen durch Induktion nach n, dass M endlich erzeugt ist, und zwar durch höchstens n Erzeuger. Für $n = 1$ ist M ein Ideal

und also durch ein Element erzeugt. Sei also $n > 1$. Setze $F' = \sum_{j=1}^{n-1} Rb_j$ und $F'' = Rb_n$. Sei $\pi : F \to F''$ die Projektion, dann hat man eine kurze exakte Sequenz

$$0 \to F' \to F \to F'' \to 0.$$

Die Moduln $M \cap F'$ und $\pi(M)$ sind erzeugt durch $n-1$ bzw einen Erzeuger und man zeigt wie im Körperfall, dass ein Erzeugendensystem von $M \cap F'$ erweitert um ein Urbild eines Erzeugers von $\pi(M)$ ein Erzeugendensystem von M bildet, M ist also endlich erzeugt mit $\leq n$ Erzeugern. Sei $z_1, \ldots, z_n$ ein Erzeugendensystem von M und betrachte die Matrix A der linerän Abbildung $F \cong K^n \to K^n \cong F$ gegeben durch $b_j \mapsto z_j$. Fasse die Matrizen S und T aus Satz 4.6.4 als Basiswechsel auf, so folgt die Behauptung. □

Proposition 4.6.6. *Sei R ein Hauptidealring.*

(a) *Je zwei Basen eines endlich-freien Moduls M haben die gleiche Länge, wir nennen diese Zahl die* Dimension *von M.*

(b) *Ist M endlich-frei und $N \subset M$ ein Untermodul, dann ist N endlich-frei und* $\dim(N) \leq \dim(M)$.

Beweis. (a) gilt für beliebige Ringe und wurde schoin in Proposition 4.5.13 bewiesen. (b) folgt ebenso aus dem Elementarteilersatz. □

4.7 Der chinesische Restsatz

Definition 4.7.1. Zwei Ideale I, J in einem Ring heißen *teilerfremd*, falls $I + J = R$ gilt.

Beispiel 4.7.2. In $R = \mathbb{Z}$ sind die Hauptideale $m\mathbb{Z}$ und $n\mathbb{Z}$ genau dann teilerfremd, wenn die Zahlen m und n keine echten gemeinsamen Teiler haben, wenn also m und n teilerfremd sind.

Beweis. Seien die Ideale teilerfremd, dann ist $1 \in m\mathbb{Z} + n\mathbb{Z}$, es gibt also $a, b \in \mathbb{Z}$ mit $am + bn = 1$. Wuerden nun m und n von einer Primzahl p geteilt, dann wuerde auch 1 von p geteilt, was ein Widerspruch ist.

Seien umgekehrt die Zahlen m und n teilerfremd. Das Ideal $m\mathbb{Z} + n\mathbb{Z}$ ist ein Hauptideal, also von der Form $g\mathbb{Z}$ für ein $g \in \mathbb{N}$. Dann ist $m \in g\mathbb{Z}$ also folgt $g|m$ und ebenso $g|n$ und daher ist $g = 1$, also sind die Ideale $m\mathbb{Z}$ und $n\mathbb{Z}$ teilerfremd. □

Definition 4.7.3. Sind I und J Ideale, so definieren wir das Ideal IJ als

$$IJ = \left\{ \sum_{j=1}^{n} a_j b_j : a_j \in I,\ b_j \in J \right\}.$$

Sind etwa beides Hauptideale, $I = (a)$ und $J = (b)$, dann ist auch IJ ein Hauptideal, nämlich $IJ = (ab)$.

Lemma 4.7.4. *Sind die Ideale I und J teilerfremd, dann gilt*

$$IJ = I \cap J.$$

Beweis. Die Inklusion "$\subset$" gilt auch ohne die Teilerfremdheit, da $IJ \subset IR = I$ und ebenso für J.

Zum Beweis von "$\supset$" seien also I und J teilerfremd, also gibt es Elemente $a \in I$ und $b \in J$ mit $1 = a + b$. Sei dann $x \in I \cap J$, dann ist $x = ax + bx$ und da axund bx beide in IJ liegen, ist $x \in IJ$. □

Satz 4.7.5 (Chinesischer Restsatz)**.** *Sei R ein Ring und $I_1, \ldots, I_r$ seien parweise teilerfremde Ideale. Sei $I = I_1 \cdots I_r = I_1 \cap \cdots \cap I_r$, dann liefern die kanonischen Projektionen einen Isomorphismus*

$$R/I \cong \prod_{\nu=1}^{r} R/I_\nu.$$

Beweis. Da $I_\nu \supset I$ für jedes ν, gibt es kanonische Projektionen $\pi_\nu : R/I \to R/I_\nu$, also einen Ringhomomorphismus

$$\pi : R/I \to \prod_{\nu=1}^{r} R/I_\nu.$$

Injektivität: Sei $\pi(\bar{x}) = 0$, und $x \in R$ ein Urbild von $\bar{x}$. Dann ist $x \in I_\nu$ für jedes ν. Nun sind die I_ν paarweise teilerfremd, also gibt es beispielsweise $a \in I_1$, $b \in I_2$ mit $a + b = 1$. Dann ist $x = 1 \cdot x = (a + b)x = ax + bx$. Da $x \in I_2$ und $a \in I_1$, ist $ax \in I_1 I_2$ und ebenso für bx, also ist $x \in I_1 I_2$. Nun ist $I_1 I_2$ immer noch teilerfremd zu $I_3, \ldots, I_r$, denn sind $a \in I_1$

und $b \in I_3$ mit $a + b = 1$ und $x \in I_2$ und $y \in I_3$ mit $x + y = 1$, so gilt

$$1 = (a+b)(x+y) = \underbrace{ax}_{\in I_1 I_2} + \underbrace{ay + bx + by}_{\in I_3}.$$

Also kann man induktiv fortfahren und erhält schließlich $x \in I_1 \cdots I_r = I$, d.h., π ist injektiv.

Surjektivität. Für die Surjektivität reicht es, zu zeigen, dass es Elemente $x_j \in R$ gibt, mit $\pi_j(x_j) = 1$ und $\pi_k(x_j) = 0$ für $k \neq j$. Modulo Umnummerierung reicht es, x_1 nachzuweisen. Seien $a \in I$ und $b \in I_2 \cdots I_r$ mit $a + b = 1$. Dann ist $x_1 = b$ das gewünschte Element. □

Korollar 4.7.6. *Sei R ein Hauptidealring und sei*

$$a = \varepsilon p_1^{\nu_1} \cdots p_r^{\nu_r}$$

eine Primfaktorzerlegung mit einer Einheit und paaweise nicht assoziierten Primelementen p_i. Ist $\pi_i : R \to R/p_i^{\nu_i} R$ jeweils die kanonische Projektion, dann ist der Homomorphismus

$$\pi : R \to \prod_{i=1}^{r} R/p_i^{\nu_i} R$$

surjektiv mit Kern aR, induziert also einen Isomorphismus

$$R/aR \cong \prod_{i=1}^{r} R/p_i^{\nu_i} R.$$

Beweis. Klar nach Chinas Restsatz, da nichtassoziierte Primelemente teilerfremd sind. □

4.8 Endlich erzeugte Moduln über Hauptidealringen

Definition 4.8.1. Sei M ein Modul des Hauptidealrings R. Der *Torsionsuntermodul* ist definiert als

$$T = \left\{ x \in M : \exists_{r \in R}\ r \neq 0,\ rx = 0 \right\}.$$

Dann ist T ein Untermodul. M heißt *Torsionsmodul*, falls M mit T übereinstimmt.

Beispiele 4.8.2.

- Ist M eine abelsche Gruppe als $\mathbb{Z}$-Modul aufgefasst, dann ist der Torsionsuntermodul genau die Menge der Elemente endlicher Ordnung.
- $\mathbb{Z}/m$ ist ein Torsionsmodul unter $\mathbb{Z}$.
- Ist K ein Körper und ist $R = K[x]$. Sei V ein R-Modul, der als K-Vektorraum endliche Dimension hat. Dann ist V ein Torsionsmodul.

  Beweis. Sei T der Operator auf V, durch den x operiert. Sei $f(x)$ das charakteristische Polynom von T. Dann ist $f(T)v = 0$ für jedes v, also ist jedes v Torsion. □

Satz 4.8.3. *Sei M ein endlich erzeugter Modul über einem Hauptidealring R und $T \subset M$ sein Torsionsmodul. Dann gibt es einen endlich-erzeugten freien Untermodul $F \subset M$, etwa $F \cong R^d$, sowie Nichteinheiten $\alpha_1, \ldots, \alpha_n \in R \setminus 0$, mit $\alpha_j \mid \alpha_{j+1}$ für $1 \leq j \leq n-1$ und*

$$M = F \oplus T, \quad T \cong \bigoplus_{j=1}^{n} R/\alpha_j R.$$

Dabei ist d eindeutig bestimmt und wird der Rang *von M genannt. Die Elemente $\alpha_1, \ldots, \alpha_n$ sind eindeutig bestimmt bis auf Assoziiertheit.*

Es gilt ferner

$$T \cong \bigoplus_{\nu=1}^{N} R/p_\nu^{e_\nu} R,$$

wobei $p_1, \ldots, p_N$ Primelemente sind und $e_1, \ldots, e_N \in \mathbb{N}$ und die Primpotenzen $p_\nu^{e_\nu}$ sind bis auf Reihenfolge und Assoziiertheit eindeutig bestimmt.

Beweis. Da M endlich erzeugt ist, gibt es einen surjektiven Homomorphismus $\phi : R^r \to M$, also $M \cong R^r/\ker(\phi)$. Nach dem Elementarteilersatz für Moduln existiert eine Basis $x_1, \ldots, x_r$ von R^r und Elemente $\alpha_1, \ldots, \alpha_n \in R$ mit $\alpha_1 \mid \cdots \mid \alpha_n$, so dass $\alpha_1 x_1, \ldots, \alpha_n x_n$ eine Basis von $\ker \phi$ ist. Wir setzen $\alpha_{n+1} = \cdots = \alpha_r = 0$ und betrachten den surjektiven Homomorphismus

$$\psi : R^r = \bigoplus_{j=1}^{r} R \to \bigoplus_{j=1}^{r} R/\alpha_j R.$$

mit $\psi(\gamma_1, \dots, \gamma_r) = (\bar{\gamma}_1, \dots, \bar{\gamma}_r)$. Nach Konstruktion ist $\ker \phi = \ker \psi$ und daher

$$M \cong R^r / \ker \phi \cong R^{n-r} \oplus \bigoplus_{j=1}^{n} R/\alpha_j R,$$

wobei wir eventuelle Sumanden mit $\alpha_j \in R^\times$, also $R/\alpha_j R = 0$ unterdrücken. Die Summe $\bigoplus_{j=1}^{n} R/\alpha_j R$ ist genau der Torsionsmodul der rechten Seite und daher ist die Zerlegung eindeutig.

Der Zusatz folgt, indem man die Primfaktorzerlegung der α_j betrachtet und den chinesischen Restsatz benutzt. Die Eindeutigkeit der Primpotenzen folgt aus der Eindeutigkeit der α_j und der Eindeutigkeit der Primfaktorzerlegung. □

4.9 Jordan-Normalform

Wir betrachten nun den Fall $R = K[x]$ für einen Körper K. Ein Modul über R besteht aus einem K-Vektorraum V zusammen mit einem Endomorphismus $T : V \to V$, wobei $x \in R$ durch T operiert. Ein Modulhomomorphismus $\Phi : (V, T) \to (W, S)$ ist eine lineare Abbildung $\Phi : V \to W$ mit $\Phi T = S\Phi$.

Zu $\lambda \in K$ sei p_λ das Primelement $p_\lambda(x) = x - \lambda$ in R. Sei $W = R/p_\lambda^k$ für ein $k \in \mathbb{N}$. Dann ist W ein K-Vektorraum der Dimension k mit der Basis
$v_1 = [(x-\lambda)^{k-1}], v_2 = [(x-\lambda)^{k-2}], \dots, v_k = [(x-\lambda)^0]$. Sei $T : W \to W$ der durch x induzierte Operator, dann folgt $(T - \lambda)v_j = v_{j+1}$, wenn wir formal $v_{k+1} = 0$ setzen. Mit anderen Worten, in der Basis $v_1, \dots, v_k$ ist T durch die Jordan-Matrix

$$J_k(\lambda) = \begin{pmatrix} \lambda & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{pmatrix}$$

gegeben.

Satz 4.9.1 (Jordan-Normalform)**.** *Sei $T : V \to V$ ein Endomorphismus des endlich-dimensionalen K-Vektorraums V. Nimm an, dass das charakteristische Polynom χ_T in Linearfaktoren zerfällt. Dann hat V eine Basis bezüglich der T durch eine*

Jordan-Matrix der Form

$$\begin{pmatrix} J_{k_1}(\lambda_1) & & \\ & \ddots & \\ & & J_{k_s}(\lambda_s) \end{pmatrix}$$

dargestellt wird.

Beweis. Der R-Modul (V, T) ist Torsion, hat also eine Zerlegung der Form

$$\bigoplus_{j=1}^{N} R/p_j^{s_j}R,$$

wobei die p_j Primelemente sind. Da χ_T durch Null operiert, ist $\chi_T R \subset p_j^{s_j}R$ für jedes j. Das bedeutet $p_j \mid \chi_T$. Da χ_T in Linearfaktoren zerfällt, muss p_j selbst einer sein, also $p_j(x) = x - \lambda_j$. Damit folgt die Behauptung nach unseren Vorbemerkungen. □

4.10 Der Hauptsatz über endlich-erzeugte abelsche Gruppen

Satz 4.10.1. *Sei G eine endlich-erzeugte abelsche Gruppe, dann gibt es eine eindeutig bestimmte Zahl $r \in \mathbb{N}_0$ und eindeutig bestimmte Primzahlpotenzen $q_1 \leq q_2 \leq \cdots \leq q_s$ so dass*

$$G \cong \mathbb{Z}^r \oplus \bigoplus_{j=1}^{s} \mathbb{Z}/q_j\mathbb{Z}.$$

Beweis. Folgt direkt aus Satz 4.8.3 für den Ring $R = \mathbb{Z}$, denn $\mathbb{Z}$-Moduln sind dasselbe wie abelsche Gruppen. □

Index