Lineare Algebra II

Dr. Malte Witte

Sommersemester 2012

Inhaltsverzeichnis

0 Einführung

0.1 Organisatorisches

- Vorlesung: Di 09:00-11:00, D1, Do 14:00-16:00 D1
- Zentralübung: Fr: 09:00-11:00 D1 bei Jakob Schütt (findet diese Woche statt).
- Übungsgruppen: Mo, Di: Einschreiben über PAUL. Die Übungen diese Woche finden nicht statt.
- Studienbegleitseiten: Unbedingt Anmelden bei moodle

  `https://moodle.math.uni-paderborn.de`.

  Kurspasswort GAUSS. Dort stehen die Übungsaufgaben, wichtige Infos, Diskussionsforen.
- Sprechstunde: Di 13:00-14:00 D3 221
- Übungsblätter: erscheinen wöchentlich am Dienstag, 4 Aufgaben à 6P + 1 Zusatzaufgabe (6 Bonuspunkte). Abgabe am darauffolgenden Dienstag bis 9:00 Uhr in den vorgesehenen Zettelkästen. Abgabe mit Partner aus der selben Übungsgruppe, handschriftlich. NICHT ABSCHREIBEN! Besprechung der Lösung in der Zentralübung.
- Präsenzübungen: erscheinen wöchentlich am Donnerstag; für die Kleingruppen.
- Klausur: (2 Stunden) am Anfang der Semesterferien, Genaueres wird noch bekanntgegeben.

- Qualifizierende Klausurteilleistung: 50 Prozent der regulären Punkte in den Hausaufgaben.

Literatur:

- M. Artin, *Algebra*
- S. Bosch, *Lineare Algebra*
- G. Fischer, *Lineare Algebra*
- F. Lorenz, *Lineare Algebra I*

0.2 Überblick

1. **Ringe und Moduln:** Wiederholung und Verallgemeinerung einiger Grundbegriffe.
2. **Elementarteilertheorie:** Klassifikation von endlich erzeugten Moduln über $\mathbb{Z}$, $K[t]$, allgemeiner über euklidischen Ringen und Hauptidealringen.
3. **Normalformen von Endomorphismen:** Abschluss der Klassifikation von Endomorphismen auf Vektorräumen mithilfe der Elementarteilertheorie.
4. **Bilinearformen:** Definition und Klassifikation von Bilinearformen, euklidische und unitäre Vektorräume, Spektraltheorie.
5. **Multilineare Algebra:** Multilineare Abbildungen und Tensorprodukte, symmetrische und äussere Potenzen.

1 Ringe und Moduln

1.1 Definitionen

Alle betrachteten Ringe seien unitärer Ringe, d. h.

Definition 1.1.

- Ein *Ring* R ist eine Menge mit zwei binären Operatoren $+$, $\cdot$ und zwei ausgezeichneten Elementen $0, 1 \in R$, so dass

  (R1) $(R, +, 0)$ ist kommutative Gruppe,
  (R2) $x(yz) = (xy)z$ für alle $x, y, z \in R$,
  (R3) $x(y + z) = xy + xz$, $(x + y)z = xz + yz$ für alle $x, y, z \in R$,
  (R4) $1x = x1 = x$ für alle $x \in R$.

  Der Ring R heißt kommutativ, falls

  (R5) $xy = yx$ für alle $x, y \in R$.

- Ein *Ringhomomorphismus* $f\colon R \to S$ ist eine Abbildung mit $f(x + y) = f(x) + f(y)$, $f(xy) = f(x)f(y)$ und $f(1) = 1$.
- Eine Untegruppe $R' \subset R$ heißt *Teilring*, wenn R'abgeschlossen unter Multiplikation ist, und $1 \in R'$ gilt.

Beispiele.

- $R = K$ ein Körper,
- $R = \mathbb{Z}$
- $R = S[t]$, der Polynomring über dem Ring S (wobei die Unbestimmte t mit jedem Element aus S kommutiert).
- $R = M_{n,n}(S)$, der Ring der $n \times n$-Matrizen über dem Ring S.

Ein weiteres Beispiel für einen nicht notwendig kommutativen Ring:

Definition 1.2. Sei A ein kommutativer Ring und G eine Gruppe. Der *Gruppenring* $A[G]$ *von* G *mit Koeffizienten in* A ist die abelsche Gruppe

$$\left\{ \sum_{g \in G} a_g g \middle|\ a_g \in A,\ a_g = 0 \text{ für fast alle } g \in G \right\} = A^{(G)}$$

mit der Multiplikation

$$\left(\sum_{g \in G} a_g g \right) \left(\sum_{g \in G} b_g g \right) = \sum_{g \in G} \sum_{h \in G} a_{gh^{-1}} b_h g$$

und $1_{A[G]} = 1_A 1_G$.

Ist G kommutativ, so auch $A[G]$.

Definition 1.3. Ist R ein Ring, so ist der *zu R opposite Ring* R^o der Ring mit derselben unterliegenden abelschen Gruppe und der neuen Multiplikation

$$\cdot^o \colon R \times R \to R, \qquad (x, y) \mapsto y \cdot x.$$

Bemerkung. Die Transponierung

$$M_{n,n}(R^o) \to M_{n,n}(R)^o, \qquad X \mapsto X^t$$

ist ein Ringisomorphismus. Ist R kommutativ, so gilt $R = R^o$ und somit $M_{n,n}(R) \cong M_{n,n}(R)^o$.

Seien R, S Ringe.

Definition 1.4. Ein *(unitärer) R-Linksmodul* M ist eine abelsche Gruppe mit einer Operation

$$R \times M \to M, \quad (r, m) \mapsto rm,$$

so dass für alle $a, b \in R$, $x, y \in M$ gilt

(M1) $a(x + y) = ax + ay$,

(M2) $(a + b)x = ax + bx$,

(M3) $(ab)x = a(bx)$,

(M4) $1x = x$.

Ein *R-Rechtmodul* M ist eine abelsche Gruppe mit einer Operation

$$M \times R \to M, \quad (m, r) \mapsto mr$$

mit den analogen Axiomen, bzw.: ein R-Rechtsmodul ist ein R^o-Linksmodul.
Ein R-S-Bimodul M ist eine abelsche Gruppe mit zwei Operationen

$$R \times M \to M, \quad (r, m) \mapsto rm, \qquad M \times S \to M, \quad (m, s) \mapsto ms$$

so dass M sowohl ein R-Linksmodul als auch ein R-Rechtsmodul ist und

$$(rm)s = r(ms)$$

für alle $r \in R$, $s \in S$, $m \in M$ gilt.

Bemerkung. Mit Modul ist im folgenden immer Linksmodul gemeint.

Beispiele.

- Ist K ein Körper, so ist ein K-Vektorraum nichts anderes als ein K-Modul.

- Jede abelsche Gruppe A ist ein $\mathbb{Z}$-Modul.
- Ist V ein K-Vektorraum und ϕ ein K-linearer Endomorphismus von V. Dann ist V mit der Operation

$$K[t] \times V \to V, \quad (f(t), v) \mapsto f(\phi)(v)$$

  ein $K[t]$-Modul.
- Ist R kommutativ, so ist jeder R-Linksmodul ein R-R-Bimodul.
- R^n ist mit der Matrixmultiplikation von links (rechts) ein $M_{n,n}(R)$-R-Bimodul (R-$M_{n,n}(R)$-Bimodul).
- Ist $\phi\colon R \to S$ ein Ringhomomorphismus, so ist S mit $S \times R \to S, \quad (s, r) \mapsto s\phi(r)$ ein S-R-Bimodul.
- Jeder R-Linksmodul ist ein R-$\mathbb{Z}$-Bimodul.

Definition 1.5. Sei K ein Körper, G eine Gruppe und V ein K-Vektorraum. Eine *lineare Darstellung* von G auf V ist ein Gruppenhomomorphismus $\rho\colon G \to \mathrm{Gl}(V)$.

Bemerkung. Ist ρ eine lineare Darstellung von G auf V, so wird V mit der Operation

$$K[G] \times V \to V, \qquad (\sum a_g g, v) \mapsto \sum a_g \rho(g) v$$

zu einem $K[G]$-Modul. Umgekehrt ist jeder $K[G]$-Modul V auch ein K-Vektorraum und die Zuordnung

$$G \to \mathrm{Gl}(V), \qquad g \mapsto \; V \xrightarrow{g\cdot} V$$

definiert eine lineare Darstellung von G auf V. Beide Konstruktionen sind zueinander invers, d. h. eine lineare Darstellung von G ist nichts weiter als ein $K[G]$-Modul.

Beispiele.

(i) Jeder K-Vektorraum V ist auf natürliche Weise eine lineare $\mathrm{Gl}(V)$-Darstellung.

(ii) Für $\sigma \in S_n$ und $v = (x_1, \ldots, x_n) \in K^n$ sei

$$\rho(\sigma)(v) = (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})$$

, d. h. $\rho(\sigma)$ hat bezüglich der Standardbasis die Darstellungsmatrix $(\delta_{i\sigma(j)})$. Dann ist $\rho\colon S_n \to \mathrm{Gl}(K^n)$ eine Darstellung der S_n auf K^n.

Definition 1.6. Ein *Homomorphismus von R-Linksmoduln (R-lineare Abbildung)* $f\colon M \to N$ ist ein Gruppenhomomorphismus mit $f(rm) = rf(m)$ für alle $r \in R$, $m \in M$. Ein Homomorphismus von R-Rechtsmoduln ist ein Homomorphismus von R^o-Linksmoduln. Ein Homomorphismus von R-S-Bimoduln ist gleichzeitig ein Homomorphismus von R-Linksmoduln und von S-Rechtsmoduln.

Bemerkung. Ist R nicht kommutativ und M, N zwei R-Linksmoduln, so ist die Menge $\mathrm{Hom}_R(M, N)$ der R-linearen Abbildung zwar eine abelsche Gruppe, trägt aber keine natürliche R-Modulstruktur. Ist jedoch M ein R-S-Bimodul, so wird $\mathrm{Hom}_R(M, N)$ durch

$$(s\phi)(m) = \phi(ms) \text{ für } s \in S,\ \phi \in \mathrm{Hom}_R(M, N),\ m \in M$$

zu einem S-Linksmodul: Sei $s, t \in S$.

$$(s(t\phi))(m) = (t\phi)(ms) = \phi(mst) = ((st)\phi)(m).$$

Insbesondere gilt dies, wenn R kommutativ ist und wir M als R-R-Bimodul betrachten. Ist N ein R-S-Bimodul, so wird $\mathrm{Hom}_R(M, N)$ durch

$$(\phi s)(m) = \phi(m)s \text{ für } s \in S,\ \phi \in \mathrm{Hom}_R(M, N),\ m \in M$$

zu einem S-Rechtsmodul.

Lemma 1.7. *Die natürliche Abbildung* $\mathrm{Hom}_R(R, M) \to M$, $\varphi \mapsto \varphi(1)$, *ist ein Isomorphismus von R-Linksmoduln.*

Beweis. Linearität: Standard.
Injektivität: $\varphi(1) = 0 \Rightarrow \varphi(r) = r\varphi(1) = 0$ für alle $r \in R$.
Surjektivität: Sei $m \in M$ beliebig. Definiere $\varphi\colon R \to M$ durch $\varphi(r) = rm$. Dann bildet sich φ auf m ab. □

Definition 1.8. Ein *Untermodul* M' eines R-Linksmoduls M ist eine Untergruppe, die abgeschlossen unter der Multiplikation mit Elementen aus R ist. Die abelsche Gruppe M/M' wird durch $r(m + M') = rm + M'$ zum R-Linksmodul. (*Faktormodul*). Analog für Rechts-, Bimoduln.

Es gibt eine inklusionserhaltende Bijektion:

$$\begin{aligned} \{\text{Untermoduln von } M/M'\} &\xrightarrow{\cong} \{\text{Untermoduln von } M, \text{ die } M' \text{ enthalten}\} \\ M/M' \supset U &\mapsto \bigcup_{u \in U} u \\ V/M' &\hookleftarrow M' \subset V \subset M \end{aligned}$$

Beweis: siehe 1.16.

Ist $f : M \to N$ ein R-Modulhomomorphismus, so sind

$$\ker(f), \quad \mathrm{im}(f) \text{ und } \mathrm{coker}(f) := N/\mathrm{im}(f)$$

wieder R-Moduln. Der Homomorphiesatz (LA I, Satz 3.11) gilt auch hier:

$$M/\ker(f) \cong \mathrm{im}(f).$$

Operationen auf Untermoduln.

Sei M ein R-Linksmodul und $(M_i)_{i\in I}$ eine Familie von Untermoduln. Dann ist $\bigcap_{i\in I} M_i$ ein Untermodul, sowie

$$\sum_{i\in I} M_i = \{\sum_i m_i \mid m_i \in M_i,\ m_i = 0 \text{ für fast alle } i\}.$$

Dies ist der kleinste Untermodul in M, der alle M_i enthält.
Ist $x \in M$, so ist $Rx := \{rx \mid r \in R\}$ ein Untermodul von M.

Satz 1.9.

(i) Sind $L \supset M \supset N$ R-Moduln, so gilt

$$(L/N)/(M/N) \cong L/M$$

(ii) Sind $M_1, M_2 \subset M$ Untermoduln, so gilt $M_1 + M_2/M_1 \cong M_2/M_1 \cap M_2$.

Beweis.
(i) Definiere $\theta\colon L/N \to L/M$ durch $\theta(x + N) = x + M$. θ ist ein wohldefinierter surjektiver R-Modulhomomorphismus und $\ker(\theta) = \{x + N \mid x \in M\} = M/N$. Die Aussage folgt daher aus dem Homomorphiesatz.
(ii) Wir betrachten die zusammengesetzte Abbildung

$$M_2 \longrightarrow M_1 + M_2 \longrightarrow M_1 + M_2/M_1.$$

Dieser R-Modulhomomorphismus ist surjektiv und hat den Kern $M_1 \cap M_2$. Die Aussage folgt daher aus dem Homomorphiesatz. □

Definition 1.10. Sei $(x_i)_{i\in I}$ eine Familie von Elementen von M. Der Untermodul $\sum_{i\in I} Rx_i$ heißt der *von der Familie erzeugte Untermodul*. Es ist der kleinste Untermodul von M der alle x_i enthält. Das System $(x_i)_{i\in I}$ heißt *Erzeugendensystem*, wenn $\sum_{i\in I} Rx_i = M$ gilt. M heißt *endlich erzeugt*, wenn es ein endliches Erzeugendensystem gibt.

Beispiele.

- Für jeden Modul M ist $(m)_{m\in M}$ ein EZS.

- R ist endlich erzeugt: (1) ist ein EZS.
- Ist $M \to N$ ein surjektiver Homomorphismus von R-Moduln und M endlich erzeugt, so ist N endlich erzeugt.
- Untermoduln von endlich erzeugten Moduln sind nicht notwendige endlich erzeugt: Sei $R = \mathbb{Q}[t_n; n \in \mathbb{N}]$ der Polynomring in abzählbar vielen Unbestimmten. Dann ist der R-Modul R endlich erzeugt, der R-Untermodul erzeugt von $(t_n)_{n\in\mathbb{N}}$ ist es nicht.

Definition 1.11. Ein R-Linksmodul M heißt *noethersch*, wenn jede aufsteigende Kette

$$U_1 \subset U_2 \subset \dots$$

von Untermoduln stationär wird, d. h. es gibt ein $i \in \mathbb{N}$, so dass $U_i = U_j$ für alle $j \geq i$.
Der Ring R heißt *(links-)noethersch*, wenn R als R-Linksmodul noethersch ist.

Satz 1.12. *Sei M ein R-Modul und $N \subset M$ ein Untermodul. Dann ist M genau dann noethersch, wenn N und M/N noethersch sind.*

Beweis.
($\Rightarrow$): Jede aufsteigende Kette von Untermoduln in N ist auch eine in M. Die Urbilder einer aufsteigenden Kette von Untermoduln in M/N unter der kanonischen Projektion $M \to M/N$ bilden eine aufsteigende Kette in M, die stationär wird. Damit wird auch die Kette in M/N stationär.
($\Leftarrow$): Sei $(U_n)_{n\in\mathbb{N}}$ eine aufsteigende Kette in M. Dann gibt es ein i mit $U_i \cap N = U_j \cap N$ und $U_i + N/N = U_j + N/N$ für alle $j \geq i$. Sei $x \in U_j$. Dann gibt es $y \in U_i$ mit $x - y \in U_j \cap N = U_i \cap N$, also $x \in U_i$ und $U_i = U_j$. □

Korollar 1.13. *Ein R-Modul ist noethersch genau dann, wenn jeder Untermodul endlich erzeugt ist.*

Beweis.
Jeder noethersche R-Modul M ist endlich erzeugt: Ansonsten gibt es zu jedem endlich erzeugten Untermodul $U_n \subset M$ ein $m \in M - U_n$, d. h. $U_{n+1} = U_n + Rm$ ist endlich erzeugt und $U_n \neq U_{n+1}$. Auf diese Weise erhält man eine nicht stationär werdende aufsteigende Kette. Da jeder Untermodul von M noethersch ist, ist auch jeder Untermodul endlich erzeugt.
Sei jeder Untermodul von M endlich erzeugt und $(U_i)_{i\in\mathbb{N}}$ eine aufsteigende Kette. Dann ist $V = \bigcup_{i\in\mathbb{N}} U_i$ ein Untermodul von M, also endlich erzeugt von $x_1, \dots, x_n \in V$. Dann gibt es ein $i_0 \in \mathbb{N}$, so dass $x_1, \dots, x_n \in U_{i_0}$. Damit gilt aber $V = U_{i_0}$ und somit $U_j = U_{i_0}$ für $j \geq i_0$, d. h. M ist noethersch. □

Korollar 1.14. *Sei R ein noetherscher Ring. Dann ist jeder endlich erzeugte R-Modul M noethersch. Insbesondere ist dann jeder Untermodul von M endlich erzeugt.*

Beweis. Mit R ist auch R^n ein noetherscher Modul (induktiv aus 1.12). Sei $(x_1, \ldots, x_n)$ ein endliches Erzeugendensystem von M. Dann ist

$$R^n \to M, \quad (r_1, \ldots, r_n) \mapsto r_1 x_1 + \ldots + r_n x_n$$

surjektiv. Also ist M noethersch und auch jeder Untermodul von M. □

Beispiele.

- Ein Vektorraum V über einem Körper K ist genau dann noethersch, wenn er endlichdimensional ist. Insbesondere ist K ein noetherscher Ring.
- $\mathbb{Z}$ ist noethersch: Die Untermoduln von $\mathbb{Z}$ sind von der Form $n\mathbb{Z}$ mit $n \in \mathbb{N}_0$ und $m\mathbb{Z} \subset n\mathbb{Z}$ genau dann, wenn $n \mid m$. Ebenso ist $K[t]$ noethersch.
- $M_{n,n}(K)$ ist (links- und rechts-)noethersch: Jeder Untermodul ist gleichzeitig ein endlichdimensionaler K-Vektorraum und die Dimension ist beschränkt durch n^2. Ebenso ist $K[G]$ (links- und rechts-)noethersch, falls G eine endliche Gruppe ist.
- $\mathbb{Q}[t_n; n \in \mathbb{N}]$ ist nicht noethersch. Der Ring $R = \mathbb{Q}^{\mathbb{N}}$ (abzählbares Produkt von Kopien von $\mathbb{Q}$ mit komponentenweiser Multiplikation) ist nicht noethersch, $\mathbb{Q}^{(\mathbb{N})}$ ist ein Ideal in R, das nicht endlich erzeugt ist.

1.2 Ideale

Definition 1.15.
Ein *Linksideal* $\mathfrak{a}$ in R ist ein Untermodul des R-Linksmoduls R.
Ein *Rechtsideal* in R ist ein Untermodul des R-Rechtsmoduls R.
Ein *zweiseitiges Ideal* in R ist ein Unter-Bimodul des R-Bimoduls R.

Beispiele.

- $\mathfrak{a} = R$, $\mathfrak{a} = \{0\}$ sind immer zweiseitige Ideale.
- Ist $f : R \to S$ ein Ringhomomorphismus, so ist $\ker(f) \subset R$ ein zweiseitiges Ideal.
- Ist $\mathfrak{a} \subset R$ ein zweiseitiges Ideal, so ist die Faktorgruppe $R/\mathfrak{a}$ mit repräsentantenweise definierter Multiplikation ein Ring, der Faktorring (auch Restklassenring)
- die Restklassenabbildung $\phi\colon R \to R/\mathfrak{a}$, $r \mapsto r + \mathfrak{a}$, ist ein surjektiver Ringhomomorphismus mit $\ker(\phi) = \mathfrak{a}$.

- Ist K ein Körper, so ist für $1 \leq k \leq n$

$$\{(a_{ij}) \in M_{n,n}(K) |\ a_{ij} = 0 \text{ für } j \neq k\}$$

ein Linksideal in $M_{n,n}(K)$, aber kein zweiseitiges Ideal.

- Die einzigen zweiseitigen Ideale von $R = M_{n,n}(K)$ sind $\{0\}$ und R (Übungsaufgabe).

- Ist $\mathfrak{a} \subset R$ ein Linksideal und M ein R-Linksmodul, so ist

$$\mathfrak{a}M = \{\sum_{i=1}^{n} a_i m_i | a_i \in \mathfrak{a},\ m_i \in M,\ n \in \mathbb{N}\}$$

ein Untermodul von M. Insbesondere sind $\mathfrak{a}^2 = \mathfrak{a}\mathfrak{a}$, $\mathfrak{a}^3$, etc. wieder Linksideale.

Notation:
Sei $\mathfrak{a} \subset R$ ein zweiseitiges Ideal. Wir schreiben $x \equiv y \bmod \mathfrak{a}$ (x ist kongruent y modulo $\mathfrak{a}$), wenn $x - y \in \mathfrak{a}$, d. h. wenn x und y die gleiche Restklasse in $R/\mathfrak{a}$ haben.
Wir schreiben $\mathfrak{a} = (r_1, \ldots, r_n)$ für das von $r_1, \ldots, r_n \in R$ erzeugte Linksideal.

Satz 1.16. *Sei $\mathfrak{a} \subset R$ ein zweiseitiges Ideal. Die Zuordnung*

$$\mathfrak{b} \mapsto \phi^{-1}(\mathfrak{b}) = \bigcup_{b \in \mathfrak{b}} b$$

definiert inklusionserhaltende Bijektionen

$$\left\{ \begin{array}{c} \textit{Links-/Rechts-/zweiseitige Ideale} \\ \textit{in } R/\mathfrak{a} \end{array} \right\} \xrightarrow{\cong} \left\{ \begin{array}{c} \textit{Links-/Rechts-/zweiseitige Ideale} \\ \textit{in } R, \textit{ die } \mathfrak{a} \textit{ enthalten} \end{array} \right\}$$

Beweis. für Linksideale; Rechts- und zweiseitige Ideale geht analog.

- Wohldefiniertheit: $\mathfrak{a} = \ker(\phi) = \phi^{-1}(0)$ und $0 \in \mathfrak{b}$, also $\phi^{-1}(\mathfrak{b}) \supseteq \mathfrak{a}$.

- Inklusionen werden erhalten: $\mathfrak{b}_1 \supseteq \mathfrak{b}_2 \Rightarrow \phi^{-1}(\mathfrak{b}_1) \supseteq \phi^{-1}(\mathfrak{b}_2)$.

- Surjektivität: Zu gegebenem Ideal $\mathfrak{c} \subset R$ mit $\mathfrak{a} \subset \mathfrak{c}$ setze $\mathfrak{b} = \phi(\mathfrak{c})$.
  $\mathfrak{b}$ ist Linksideal, weil ϕ surjektiv ist. Genauer:
  - $b_1, b_2 \in \mathfrak{b} \Rightarrow \exists\, c_1, c_2 \in \mathfrak{c}$ mit $\phi(c_i) = b_i,\ i = 1, 2$, also $b_1 + b_2 = \phi(c_1 + c_2) \in \mathfrak{b}$.
  - $r \in R/\mathfrak{a},\ b \in \mathfrak{b} \Rightarrow \exists\, s \in R,\ c \in \mathfrak{c}$ mit $\phi(s) = r,\ \phi(c) = b \Rightarrow rb = \phi(sc) \in \mathfrak{b}$.

Es gilt $\mathfrak{c} = \phi^{-1}(\mathfrak{b})$: Die Inklusion $\mathfrak{c} \subset \phi^{-1}(\mathfrak{b}) = \phi^{-1}(\phi(\mathfrak{c}))$ ist trivial. Sei nun $\phi(x) = y \in \mathfrak{b}$. Nach Definition existiert $x_0 \in \mathfrak{c}$ mit $\phi(x_0) = y$. Daher gilt $\phi(x - x_0) = y - y = 0$, also $x - x_0 \in \ker(\phi) = \mathfrak{a} \subset \mathfrak{c}$ und damit $x \in \mathfrak{c}$.

- Injektivität: Gilt $\phi^{-1}(\mathfrak{b}_1) = \phi^{-1}(\mathfrak{b}_2)$, so gilt wegen der Surjektivität von ϕ:

$$\mathfrak{b}_1 = \phi(\phi^{-1}(\mathfrak{b}_1)) = \phi(\phi^{-1}(\mathfrak{b}_2)) = \mathfrak{b}_2.$$

□

Satz 1.17. *Sei A ein kommutativer Ring $\neq \{0\}$. Dann sind äquivalent*

(i) *A ist ein Körper.*
(ii) *(0) und (1) sind die einzigen Ideale in A.*
(iii) *jeder Homomorphismus $f\colon A \to S$ in einem Ring $S \neq \{0\}$ ist injektiv.*

Beweis. (i) $\Rightarrow$ (ii). Sei $\mathfrak{a} \subset A$ ein Ideal $\neq \{0\}$. Dann existiert ein $0 \neq x \in \mathfrak{a}$. Daher gilt $1 = x^{-1}x \in \mathfrak{a}$, folglich $A = (1) \subseteq \mathfrak{a} \subseteq A$.
(ii) $\Rightarrow$ (iii). Sei $f\colon A \to S$ ein Ringhomomorphismus mit $S \neq \{0\}$. Wegen $0 \neq 1$ in S ist $\ker(f) \subset A$ ein Ideal $\neq A \Rightarrow \ker(f) = 0$.
(iii) $\Rightarrow$ (i). Sei $x \in A$ keine Einheit. Dann ist $(x) \neq A$, also $S = A/(x)$ nicht der Nullring. Es gilt $x \in \ker(\phi\colon A \to A/(x))$, also $x = 0$. Daher ist A Körper. □

Definition 1.18. Ein Linksideal $\mathfrak{m} \subset R$ heißt *maximal*, wenn $\mathfrak{m} \neq R$ und es kein Linksideal $\mathfrak{a}$ mit $\mathfrak{m} \subsetneq \mathfrak{a} \subsetneq R$ gibt.

Beispiele.

- Die maximalen Ideale von $\mathbb{Z}$ sind von der Form (p) mit p Primzahl.
- (0) ist das einzige maximale Ideal eines Körpers K.
- Die maximalen Ideale von $K[t]$ sind von der Form (f) mit $0 \neq f \in K[t]$ normiert und irreduzibel.
- Sei $0 \neq v \in K^n$. Betrachte K^n als $M_{n,n}(K)$-Linksmodul. Dann ist der Kern der $M_{n,n}(K)$-linearen Abbildung

$$M_{n,n}(K) \to K^n, \quad A \mapsto Av$$

ein maximales Ideal. Auf diese Art erhält man alle maximalen Ideale von $M_{n,n}(K)$. (Übungsaufgabe)

Satz 1.19. *Sei A ein kommutativer Ring und $\mathfrak{m} \subset A$ ein maximales Ideal. Dann ist $A/\mathfrak{m}$ ein Körper.*

Beweis. Nach 1.16 entsprechen die Ideale $\mathfrak{a}$ mit $\mathfrak{m} \subsetneq \mathfrak{a} \subsetneq A$ den Idealen $\neq (0), (1)$ in $A/\mathfrak{m}$. Nach 1.17 ist $A/\mathfrak{m}$ genau dann ein Körper, wenn es solche Ideale nicht gibt. □

Beispiele.

- $\mathbb{C} = \mathbb{R}[t]/(t^2+1)$.
- Sei K ein Körper, $f = \sum a_k t^k \in K[t]$ irreduzibel und $\alpha = t+(f) \in K[t]/(f)$. Dann ist $K[\alpha] := K[t]/(f)$ ein Körper, der K als Teilkörper enthält und

  $$f(\alpha) = \sum a_k \alpha^k = f + (f) = 0;$$

  d. h. $K[\alpha]$ ist eine Erweiterung von K, in der f eine Nullstelle besitzt.
- $\mathbb{Q}[i] = \mathbb{Q}[t]/(t^2+1)$, $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}[t]/(t^2-2)$, etc.
- Sei $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$ der Körper mit 3 Elementen. Dann ist

  $$\mathbb{F}_9 = \mathbb{Z}/3\mathbb{Z}[t]/(t^2+\bar{1})$$

  ein Körper mit 9 Elementen.

Hat jeder Ring maximale Linksideale?

Zwischenbemerkung aus der Mengentheorie

Definition 1.20. Eine *Halbordnung* auf einer Menge M ist eine (binäre) Relation $\leq$, so dass

Transitivität: $\forall x, y, z \in M : x \leq y \wedge y \leq z \Rightarrow x \leq z$,

Reflexivität: $\forall x \in M : x \leq x$,

Antisymmetrie: $\forall x, y \in M : x \leq y \wedge y \leq x \Rightarrow x = y$.

Eine *vollständige Ordnung (Totalordnung)* ist eine Halbordnung, so dass

Totalität: $\forall x, y \in M : x \leq y \vee y \leq x$.

Eine *halbgeordnete* Menge $M = (M, \leq)$ ist eine Menge M zusammen mit einer Halbordnung $\leq$.
Eine Teilmenge T einer halbgeordneten Menge $(M, \leq)$ heißt *Kette*, wenn $(T, \leq)$ vollständig geordnet ist.
Ein $m \in M$ heißt *obere Schranke* für eine Teilmenge $T \subset M$ wenn $t \leq m$ für alle $t \in T$ gilt.
Ein Element $m \in M$ heißt *maximal*, wenn aus $m \leq x$ folgt, dass $m = x$.

Zorn'sches Lemma: *Sei $(M, \leq)$ eine halbgeordnete nichtleere Menge. Besitzt jede Kette in M eine obere Schranke, so enthält M mindestens ein maximales Element.*

Äquivalent dazu (siehe z.B. S. Lang: *Algebra*):

Auswahlaxiom: *Sei $(M_i)_{i\in I}$ eine Familie von nichtleeren Mengen. Dann gilt*

$$\prod_{i\in I} M_i \neq \emptyset$$

d. h. für jedes $i \in I$ kann man ein Element $m_i \in M_i$ auswählen.

Bemerkung. Für endliche Indexmengen I kann man eine eine solche Auswahlfunktion direkt angeben. Das Auswahlaxiom ist daher nur für nicht endliche Indexmengen interessant. In diesem Fall haben wir in der Regel aber auch keine Möglichkeit mehr, eine konkrete Auswahlfunktion anzugeben. Das Auswahlaxiom kann nicht aus den grundlegenden Axiomen der Mengentheorie (ZF-Axiomensystem) hergeleitet werden.

Satz 1.21. *Sei $R \neq \{0\}$ ein Ring und $\mathfrak{a} \subsetneq R$ ein Linksideal. Dann existiert ein maximales Linksideal $\mathfrak{m}$ von R mit $\mathfrak{a} \subset \mathfrak{m}$. Insbesondere besitzt jeder Ring $R \neq \{0\}$ ein maximales Linksideal.*

Beweis. Sei Σ die Menge der Linksideale $\neq (1)$ in R, die $\mathfrak{a}$ enthalten. Wegen $\mathfrak{a} \in \Sigma$ ist $\Sigma \neq \varnothing$. Wir ordnen Σ durch Inklusion, d.h. $\mathfrak{b} \leq \mathfrak{c} \Leftrightarrow \mathfrak{b} \subset \mathfrak{c}$.
Sei nun $(\mathfrak{b}_\alpha)$ eine Kette in Σ. Für α, β haben wir $\mathfrak{b}_\alpha \subset \mathfrak{b}_\beta$ oder $\mathfrak{b}_\beta \subset \mathfrak{b}_\alpha$. Setze $\mathfrak{b} = \bigcup_\alpha \mathfrak{b}_\alpha$. Dann ist $\mathfrak{b}$ ein Linksideal: $r \in R$, $a \in \mathfrak{b} \Rightarrow ra \in \mathfrak{b}$ weil $a \in \mathfrak{b}_\alpha$ für ein α und deshalb $ra \in \mathfrak{b}_\alpha$ $a \in \mathfrak{b}_\alpha$, $b \in \mathfrak{b}_\beta$. Gilt $\mathfrak{b}_\alpha \subset \mathfrak{b}_\beta$ so folgt $a + b \in \mathfrak{b}_\beta \subset \mathfrak{b}$, ansonsten gilt $\mathfrak{b}_\beta \subset \mathfrak{b}_\alpha$ und $a + b \in \mathfrak{b}_\alpha \subset \mathfrak{b}$.
Nun ist $\mathfrak{b} \in \Sigma$ wegen $1 \notin \mathfrak{b} = \bigcup \mathfrak{b}_\alpha$ und $\mathfrak{a} \subset \mathfrak{b}$. Ferner ist $\mathfrak{a}$ obere Schranke für die Kette $(\mathfrak{a}_\alpha)$.
Zorn'sches Lemma $\Rightarrow \Sigma$ besitzt mindestens ein maximales Element. □

Bemerkung. Weitere Anwendung des Zorn'schen Lemmas: Jeder Vektorraum besitzt eine Basis.

1.3 Freie Moduln

Definition 1.22. Ein System $(x_i)_{i\in I}$ von Elementen eines R-Linksmoduls M heißt *linear unabhängig*, wenn für jedes endliche System von Elementen $(r_i)_{i\in I}$ (d.h. $r_i = 0$ f.f.a. $i \in I$) die Implikation $\sum r_i x_i = 0 \Rightarrow r_i = 0$ für alle i gilt. Ein linear unabhängiges Erzeugendensystem heißt *Basis* des R-Moduls M. M heißt *freier R-Modul*, wenn eine Basis von M existiert.

Beispiele.

- Ist $R = K$ ein Körper, so ist jeder R-Modul frei.
- $\{0\}$ ist ein freier R-Modul mit dem leeren System als Basis.
- R selbst ist ein freier R-Modul mit Basis $1 \in R$. ($r = r \cdot 1$ und aus $r \cdot 1 = 0$ folgt $r = 0$).
- Sind M und N freie Moduln mit Basen $(x_i)_{i\in I}$ und $(y_j)_{j\in J}$, so ist $M \oplus N$ ein freier R-Modul mit Basis $((x_i, 0), (0, y_j))_{i\in I, j\in J}$ (Indexmenge $I \dot{\bigcup} J$). Insbesondere ist $R^n = \underbrace{R \oplus \cdots \oplus R}_{n\text{-mal}}$ frei mit der kanonischen Basis $(e_1, \ldots, e_n)$ wobei $e_i = (0, \ldots, 0, 1, 0 \ldots 0)$ (die 1 an der i-ten Stelle).
- Ist M ein freier R-Modul mit Basis $(x_i)_{i\in I}$, so ist die Abbildung
$$\phi\colon R^{(I)} \to M, \quad (r_i)_{i\in I} \longmapsto \sum_{i\in I} r_i x_i,$$
ein R-Modulisomorphismus. D.h.: Ein Modul ist genau dann frei, wenn er isomorph zu einem Modul der Form $R^{(I)}$ ist.
- Ein Modul der Form R^I ist im allgemeinen nicht frei.
Ausnahmen: I endlich, oder R Körper.
- Ist $\mathfrak{a} \subsetneq R$ ein von (0) verschiedenes Ideal, so ist $R/\mathfrak{a}$ kein freier R-Modul.
Grund: Ist $a \in \mathfrak{a}$, $a \neq 0$, so gilt für jedes $x \in R/\mathfrak{a}$: $ax = 0$. Daher gibt es kein nichtleeres l.u. System von Elementen in $R/\mathfrak{a}$. Wegen $R/\mathfrak{a} \neq 0$ kann es keine Basis geben.
(Andererseits ist $R/\mathfrak{a}$ frei als $R/\mathfrak{a}$-Modul.)
- Sei $V \neq \{0\}$ ein endlich-dimensionaler K-Vektorraum und $\varphi \in \mathrm{End}_K(V)$. Das Paar (V, φ) als $K[t]$-Modul ist nicht frei.
Grund: es gilt $\chi_\varphi(t) \cdot v = 0$ für alle $v \in V$ (Cayley-Hamilton). Alternatives Argument: Ein freier $K[t]$-Modul $\neq 0$ ist als K-Vektorraum unendlich-dimensional.

Satz 1.23 (Universaleigenschaft freier Moduln)**.** *Sei M ein freier R-Modul mit Basis $(x_i)_{i\in I}$ und N ein weiterer R-Modul. Dann ist*
$$\mathrm{Hom}_R(M, N) \to N^I = \mathrm{Abb}(I, N), \quad \phi \mapsto (\phi(x_i))_{i\in I}$$
ein Isomorphismus abelscher Gruppen. Mit anderen Worten:
Zu jeder Vorgabe $(y_i)_{i\in I}$ von Elementen in N gibt es genau einen R-Modulhomomorphismus $\phi\colon M \to N$ mit $\phi(x_i) = y_i \quad \forall\, i \in I$.

Beweis. Für $(y_i)_{i\in I} \in N^I$ setze

$$\phi(\sum r_i x_i) = \sum r_i y_i \quad (r_i = 0 \text{ f. f. a. } i)$$

□

Hat jede Basis eines freien R-Moduls die gleiche Kardinalität?

Beispiel. Sei $R = \mathrm{End}_{\mathbb{C}}(\mathbb{C}[t])$. Für $f = \sum a_k t^k$ setze

$$p_1(f) = \sum a_{2k} t^k, \qquad i_1(f) = f(t^2),$$
$$p_2(f) = \sum a_{2k+1} t^k, \qquad i_2(f) = tf(t^2).$$

Dann ist (p_1, p_2) eine Basis von R: Wegen $\mathrm{id} = i_1 p_1 + i_2 p_2$ ist es EZS. Sei $\alpha, \beta \in R$ und $\alpha p_1 + \beta p_2 = 0$. Dann gilt

$$0 = (\alpha p_1 + \beta p_2) i_1 = \alpha.$$

Analog: $\beta = 0$. (id) ist aber ebenfalls eine Basis, d. h. es gibt Basen unterschiedlicher Kardinalität.

Definition 1.24. Der Ring R hat *invariante Basiszahl*, wenn für alle $n, m \in \mathbb{N}$ gilt: $R^m \cong R^n \Rightarrow n = m$

Satz 1.25. *Jeder kommutative Ring $R \neq \{0\}$ hat invariante Basiszahl.*

Beweis. Sei $\mathfrak{m} \subset R$ ein maximales Ideal und $k = R/\mathfrak{m}$. Angenommen, $\phi\colon R^m \to R^n$ ist ein Isomorphismus. Für $x \in R^s$ sei $\bar{x}$ das Bild von x in k^s. Dann ist

$$\widetilde{\phi}\colon k^m \to k^n, \quad \bar{x} \mapsto \overline{\phi(x)}$$

ein wohldefinierter k-linearer Isomorphismus (die Inverse ist $\widetilde{\phi^{-1}}$). Für Vektorräume wissen wir bereits, dass dann $m = n$ gelten muss (LA I, Korollar 3.27). □

Satz 1.26. *Jeder noethersche Ring $R \neq \{0\}$ hat invariante Basiszahl.*

Beweis. Sei $\phi\colon R^m \to R^n$ ein Isomorphismus mit $n < m$. Setze

$$i\colon R^n \to R^m, \quad (r_1, \ldots, r_n) \mapsto (r_1, \ldots, r_n, \underbrace{0, \ldots, 0}_{m-n})$$
$$R^{m-n} \cong M_0 = \{(\underbrace{0, \ldots, 0}_{n}, r_{n+1}, \ldots, r_m) | r_i \in R\} \subset R^m,$$

so dass $R^m = i(R^n) + M_0$. Setze induktiv $M_k = M_0 + (i\phi)(M_{k-1})$ Dann ist $M_0 \subset M_1 \subset \ldots$ eine aufsteigende Kette, die nicht stationär wird. □

Korollar 1.27. *Der Ring R habe invariante Basizahl. Zwei beliebige Basen eines endlich erzeugten freien R-Moduls M haben die gleiche Kardinalität.*

Beweis. Sind $(x_1, \ldots, x_n)$ und $(y_1, \ldots, y_m)$ Basen von M, so gilt $R^n \cong M \cong R^m$ und also $m = n$ nach 1.25. □

Definition 1.28. Der Ring R habe invariante Basiszahl. Die Kardinalität einer (jeder) Basis eines endlich erzeugten freien R-Moduls M heißt sein *Rang*. Notation: $r(M)$.

Bemerkung. Ist $R = K$ ein Körper, so ist Rang = Dimension.

Seien M und N endlich erzeugte, freie R-Moduln mit Basen $x = (x_1, \ldots, x_m)$ und $y = (y_1, \ldots, y_n)$. Zu $f \in \mathrm{Hom}_R(M, N)$ bilden wir die *Darstellungsmatrix* $M_y^x(f) = (a_{ij})$ mit

$$f(x_j) = \sum_{i=1}^{n} a_{ij} y_i.$$

Die Matrix $M_y^x(f)$ fassen wir als ein Element von $M_{n,m}(R^o)$ auf (!). Es gilt dann $M_z^x(g \circ f) = M_z^y(g) M_y^x(f)$ (Multiplikation von Matrizen mit Einträgen in R^o), falls z eine Basis des freien Moduls P mit Basis z ist und $g \in \mathrm{Hom}_R(N, P)$.

Für eine feste Matrix $A = (a_{ij}) \in M_{n,m}(R^o)$ setzen wir

$$F_y^x(A) \colon M \to N, \quad \sum_{j=1}^{m} r_j x_j \mapsto \sum_{j=1}^{m} \sum_{i=1}^{n} r_j a_{ij} y_i = \sum_{i=1}^{m} s_i y_i$$

(Multiplikation in R), wobei

$$s_i = \sum_{j=1}^{m} r_j a_{ij} = \sum_{j=1}^{m} a_{ij} \cdot^o r_j,$$

d. h. $s = Ar$ (Multiplikation von Matrizen mit Einträgen in R^o). Die Zuordnung $A \mapsto F_y^x(A)$ liefert eine Abbildung $F_y^x \colon M_{m,n}(R) \to \mathrm{Hom}_R(M, N)$.

Satz 1.29. *Die so definierte Abbildung $F_y^x \colon M_{n,m}(R^o) \to \mathrm{Hom}_R(N, M)$ ist ein Isomorphismus von abelschen Gruppen.*

Beweis. Wörtlich der gleiche wie im Vektorraum-Fall. □

Definition 1.30. Sind $x = (x_1, \ldots, x_n)$ und $x' = (x'_1, \ldots, x'_m)$ zwei Basen desselben endlich erzeugten freien R-Moduls M, so heißt die Matrix $T = M_{x'}^x(\mathrm{id}_M)$ die *Transformationsmatrix* von x nach x'.

Bemerkung. Es gilt $M_{x'}^x(\mathrm{id}_M) M_x^{x'}(\mathrm{id}_M) = E_m$, $M_x^{x'}(\mathrm{id}_M) M_{x'}^x(\mathrm{id}_M) = E_n$. Insbesondere ist T im Fall $n = m$ invertierbar mit inverser Matrix $T^{-1} = M_x^{x'}(\mathrm{id}_M)$.

Satz 1.31. *(Basiswechsel). Seien M, N endlich erzeugte freie R-Moduln und $f\colon M \to N$ eine R-lineare Abbildung. Seien $x = (x_1, \dots, x_n)$ und $x' = (x'_1, \dots, x'_m)$ zwei Basen von M und $y = (y_1, \dots, y_k)$ und $y' = (y'_1, \dots, y'_\ell)$ zwei Basen von N. Dann gilt*

$$M_{y'}^{x'}(f) = M_y^{y'}(\mathrm{id}_N) \cdot M_y^x(f) \cdot M_x^{x'}(\mathrm{id}_M)$$

Beweis. Wie bei Vektorräumen. Siehe LA I, Satz 4.15. □

Definition 1.32. Ein R-Modul M heißt *endlich präsentierbar*, wenn es eine lineare Abbildung $f\colon F_1 \to F_0$ zwischen endlich erzeugten, freien R-Moduln F_i gibt, so dass $M \cong \operatorname{coker} f$.

Bemerkung. Endlich präsentierbare Moduln lassen sich also im Wesentlichen (nicht eindeutig) durch die Matrix von f beschreiben.

Satz 1.33. *Sei R ein noetherscher Ring. Dann ist jeder endlich erzeugte R-Modul M auch endlich präsentierbar.*

Beweis. Sei $(x_1, \dots, x_n)$ ein Erzeugendensystem von M und $F_0 = R^n$. Dann ist

$$g\colon R^n \to M, \qquad (r_1, \dots, r_n) \mapsto \sum_{i=1}^n r_i x_i$$

eine surjektive lineare Abbildung festgelegt. Der Untermodul $\ker g$ von F_0 ist wieder endlich erzeugt, da R noethersch ist. Durch Wiederholung der Konstruktion erhalten wir einen endlich erzeugten, freien R-Modul F_1 und eine lineare Abbildung $f\colon F_1 \to F_0$ mit $\operatorname{im} f = \ker g$. Nach dem Homomorphiesatz gilt $\operatorname{coker} f = F_0/\ker g \cong M$. □

2 Elementarteilertheorie

2.1 Integritätsringe

Sei R ein kommutativer Ring.

Definition 2.1. $x \in R$ heißt *Nullteiler*, wenn es ein $y \in R$, $y \neq 0$, gibt mit $xy = 0$. R heißt *nullteilerfrei* (oder Integritätsring) wenn $R \neq \{0\}$ und $0 \in R$ der einzige Nullteiler ist.

Beispiele.

- $\overline{2} \in \mathbb{Z}/6\mathbb{Z}$ ist Nullteiler wegen $\overline{2} \cdot \overline{3} = 0$ in $\mathbb{Z}/6\mathbb{Z}$, aber beide $\neq 0$.
- Körper sind nullteilerfrei.
- $\mathbb{Z}$ ist nullteilerfrei, allgemeiner: jeder Teilring eines Körpers ist nullteilerfrei.

- R nullteilerfrei $\Rightarrow R[t]$ ist nullteilerfrei (LA I, Kor. 6.34).

Wir betrachten (wie für $R = \mathbb{Z}$ in der Schule und für $R = K[t]$ in LA I gemacht) die folgende Relation auf der Menge $R \times (R \setminus \{0\})$

$$(x_1, y_1) \sim (x_2, y_2) \iff x_1 y_2 = x_2 y_1.$$

Lemma 2.2. *Die Relation $\sim$ ist eine Äquivalenzrelation auf $R \times (R \setminus \{0\})$.*

Beweis. Symmetrie und Reflexivität sind klar. Es verbleibt, die Transitivität zu zeigen. Es gelte $(x_1, y_1) \sim (x_2, y_2)$ und $(x_2, y_2) \sim (x_3, y_3)$. Dann gilt nach Definition $x_1 y_2 = x_2 y_1$ und $x_2 y_3 = x_3 y_2$. Dies impliziert

$$y_2(x_1 y_3 - x_3 y_1) = x_1 y_2 y_3 - y_1 y_2 x_3 = x_2 y_1 y_3 - y_1 x_3 y_2$$

$$= y_1(x_2 y_3 - x_2 y_3) = 0.$$

Wegen $y_2 \neq 0$ und der Nullteilerfreiheit von R folgt $x_1 y_3 - x_3 y_1 = 0$, also $(x_1, y_1) \sim (x_3, y_3)$. □

Wir bezeichnen die Äquivalenzklasse von (x, y) mit

$$\frac{x}{y}$$

und die Menge aller Äquivalenzklassen mit $Q(R)$. Wir führen auf $Q(R)$ die folgenden Operationen ein

$$\frac{x_1}{y_1} + \frac{x_2}{y_2} = \frac{x_1 y_2 + x_2 y_1}{y_1 y_2} \qquad \frac{x_1}{y_1} \cdot \frac{x_2}{y_2} = \frac{x_1 x_2}{y_1 y_2}.$$

Lemma 2.3. *Diese Operationen auf $Q(R)$ sind wohldefiniert und machen $Q(R)$ zu einem Körper mit $\frac{0}{1}$ als Null- und $\frac{1}{1}$ als Einselement.*

Beweis. Die Wohldefiniertheit lassen wir als Übungsaufgabe. Dass $\frac{0}{1}$ und $\frac{1}{1}$ das Null- bzw. Einselement sind, sieht man direkt an der Definition der Operationen. Nach Definition von $\sim$ gilt

$$\frac{x}{y} = \frac{0}{1} \iff x = 0.$$

Gilt also $\frac{x}{y} \neq 0$ in $Q(R)$, so ist $x \neq 0$ und $\frac{y}{x}$ das inverse Element zu $\frac{x}{y}$. □

Definition 2.4. $Q(R)$ heißt der *Quotientenkörper* von R.

Beispiel.

- $Q(\mathbb{Z}) = \mathbb{Q}$ (Körper der rationalen Zahlen),

- $Q(K[t]) = K(t)$ (Körper der rationalen Funktionen über dem Körper K).
- $Q(\mathbb{Z}[t]) = \mathbb{Q}(t)$.

Wir betrachten die natürliche Abbildung

$$R \longrightarrow Q(R), \quad r \mapsto \frac{r}{1}.$$

Diese ist ein injektiver Ringhomomorphismus, so dass wir R als Teilring von $Q(R)$ und $Q(R)$ als R-Modul auffassen können.

Definition 2.5. Für $x \in R$ heißt das Ideal $(x) := Rx = \{ax \mid a \in A\}$ das von x erzeugte *Hauptideal*. Ein Ideal $\mathfrak{a} \subset R$ heißt Hauptideal, wenn $\mathfrak{a} = (x)$ für ein $x \in R$.

Bemerkung. $x \in R$ ist Einheit $\iff (x) = R = (1)$.

Sei jetzt R kommutativ und nullteilerfrei.

Definition 2.6. Man sagt $a|b$ wenn ein $c \in R$ mit $b = ac$ existiert. Zwei Elemente $a, b \in R$ heißen *assoziiert*, wenn $a|b$ und $b|a$ gilt. Notation $a \hat{=} b$.

Lemma 2.7. *(R nullteilerfrei) Für Elemente $a, b \in R$ sind äquivalent:*
(i) $a \hat{=} b$,
(ii) $(a) = (b)$,
(iii) *es existiert eine Einheit $e \in R^\times$ mit $b = ea$.*

Beweis. Ist a oder b gleich Null, so sagen (i), (ii) und (iii), dass das jeweils andere Element auch gleich 0 ist. Seien im Folgenden a und b von 0 verschieden.
(i)$\Leftrightarrow$(ii) $a|b$ ist äquivalent zu $(b) \subset (a)$, also $a \hat{=} b$ zu $(a) = (b)$.
(i)$\Rightarrow$(iii) Sei $b = ac$ und $a = bd$. Dann folgt $b = bcd$, also $b(1 - cd) = 0$. Wegen $b \neq 0$ und der Nullteilerfreiheit von R folgt $cd = 1$, also ist c eine Einheit.
(iii)$\Rightarrow$(i). Aus $b = ae$ folgt $a = be^{-1}$, also $a|b$ und $b|a$. □

Definition 2.8. Ein Element $\pi \in R \setminus (R^\times \cup \{0\})$ (R nullteilerfrei wie immer) heißt *Primelement*, falls gilt $\pi|ab \Rightarrow \pi|a$ oder $\pi|b$.

Ein Element $\pi \in R \setminus (R^\times \cup \{0\})$ heißt *irreduzibel*, falls gilt: aus $ab = \pi$ folgt $a \in R^\times$ oder $b \in R^\times$.

Lemma 2.9. *Primelemente sind irreduzibel.*

Beweis. Sei π prim und und $\pi = ab$. Dann gilt $\pi \mid a$ oder $\pi \mid b$. Sei OE $a = a'\pi$, $a' \in R$. Dann gilt $\pi = ab = \pi a'b \Rightarrow \pi(a'b - 1) = 0 \overset{\pi \neq 0}{\Longrightarrow} a'b = 1 \Rightarrow b \in R^\times$. □

Definition/Lemma 2.10. *Sei M ein R-Modul. Ein Element $x \in M$ heißt* Torsionselement, *wenn es ein $0 \neq s \in R$ gibt mit $sx = 0$. Die Menge der Torsionselemente in M bildet einen Untermodul. Dieser heißt der* Torsionsuntermodul *und wird mit $T(M)$ bezeichnet.*

Beweis. Klar gilt $0 \in T(M)$, d. h. $T(M) \neq \emptyset$. Seien $x, y \in T(M)$, $r \in R$. Dann existieren $s, t \in R - \backslash\{0\}$ mit $sx = ty = 0$. Da R nullteilerfrei ist gilt $st \neq 0$. Nun gilt

$$st(x + ry) = t(sx) + rs(ty) = 0,$$

also $x + ry \in T(M)$. Damit ist $T(M)$ ein Untermodul. □

Definition 2.11. M heißt *Torsionsmodul* $\iff M = T(M)$.
M heißt *torsionsfrei* $\iff T(M) = 0$

Beispiele.

(i) Jeder Untermodul N eines freien R-Moduls M ist torsionsfrei: Sei $(m_i)_{i\in I}$ ein Erzeugendensystem von M und $n = \sum_i r_i m_i \in N$, $r \in R$. Dann gilt

$$(r(\sum r_i m_i) = 0) \Rightarrow \sum (rr_i)m_i = 0 \Rightarrow rr_i = 0 \quad \forall\, i \Rightarrow r_i = 0 \quad \forall\, i.$$

(ii) Ist $R = K$ ein Körper, so ist jeder Modul torsionsfrei (weil frei).

(iii) $\mathbb{Z}/n\mathbb{Z}$ ist ein $\mathbb{Z}$-Torsionsmodul, wegen $n \cdot x = 0$ für alle $x \in \mathbb{Z}/n\mathbb{Z}$.

(v) Der Modul (0) ist der einzige Modul, der sowohl Torsionsmodul als auch frei ist.

(iv) Sei S ein kommutativer Ring mit nichtrivialen Nullteilern, M ein S-Modul. Dann besitzt jeder freie Modul auch Torsionselemente und die Menge $T(M)$ ist in der Regel kein Untermodul.

Lemma 2.12. *Der Faktormodul $M/T(M)$ ist torsionsfrei.*

Beweis. Sei $m+T(M) \in M/T(M)$ ein Torsionselement. Dann existiert $0 \neq r \in R$ mit $r(m + T(M)) = 0$, also $rm \in T(M)$. Daher existiert ein $s \in R$ mit $srm = 0$. Wegen $sr \neq 0$ folgt $m \in T(M)$, also $m + T(M) = 0 + T(M) \in M/T(M)$. □

Lemma 2.13. *Sei $f\colon M \to N$ ein R-Homomorphismus. Dann bildet f $T(M)$ auf $T(N)$ ab. Insbesondere gilt $T(M) \cong T(N)$, falls $M \cong N$.*

Beweis. Sei $x \in T(M)$. Dann gibt es ein $r \in R$ mit $rx = 0$. Also $rf(x) = f(rx) = 0$ und $f(x) \in T(N)$. □

2.2 Hauptidealringe

Definition 2.14. Ein *Hauptidealring* ist ein nullteilerfreier kommutativer Ring, in dem jedes Ideal Hauptideal ist.

Beispiel. $\mathbb{Z}$ und $K[t]$ (K Körper) sind Hauptidealringe.

Lemma 2.15. *Jeder Hauptidealring ist noethersch.*

Beweis. Jedes Ideal ist endlich erzeugt (von einem Element). □

Satz 2.16. *In einem Hauptidealring ist jedes irreduzible Element prim.*

Beweis. Sei π irreduzibel und es gelte $\pi|ab$. Z.z.: $\pi|a$ oder $\pi|b$. Wir betrachten das Ideal $(a)+(\pi) \overset{\text{Hauptidealring}}{=} (c)$. Es gilt $\pi \in (c) \Rightarrow \pi = ce$ für ein $e \in R$. Da π irreduzibel ist, muss einer der beiden folgenden Fälle auftreten:
1. Fall: e Einheit $\Rightarrow (c) = (\pi)$, also $a \in (c) = (\pi) \Rightarrow \pi|a$.
2. Fall: c Einheit $\Rightarrow 1 \in (c)$, also existieren $x, y \in R$ mit $ax + \pi y = 1$. Daraus folgt

$$b = b \cdot 1 = abx + b\pi y \in (\pi)$$

also $\pi|b$. □

Lemma 2.17. *Sei R ein Hauptidealring und $a \in R \setminus (R^\times \cup \{0\})$. Gilt*

$$a = p_1 \cdots p_n = q_1 \cdots q_m$$

mit irreduziblen Elementen p_i, q_i, so gilt $n = m$ und, nach Umnummerierung, $p_i \hat{=} q_i$, $i = 1, \ldots, n$.

Beweis. Ohne Einschränkung gelte $n \leq m$. Es ist p_n irreduzibel, daher prim $\Rightarrow p_n|q_1 \cdots q_m \Rightarrow$ (nach Umnummerierung) $p_n|q_m \Rightarrow q_m = p_n \cdot e$, für ein $e \in R$. Da q_m irreduzibel und p_n keine Einheit ist, folgt $e \in R^\times$. Wir erhalten

$$p_1 \cdots p_n = q_1 \cdots q_{m-1} \cdot p_n \cdot e$$

und somit $p_1 \cdots p_{n-1} = q_1 \cdots q_{m-1} \cdot e$. Wir führen diesen Prozeß weiter und kommen schließlich zu

$$1 = q_1 \cdots q_{m-n} \cdot \text{Einheit}.$$

Hieraus folgt $m - n = 0$, weil die q_i keine Einheiten sind. □

Satz 2.18. *Sei R ein Hauptidealring. Dann hat jedes $a \in R \setminus (R^\times \cup \{0\})$ eine bis auf Reihenfolge und Assoziiertheit eindeutige Zerlegung*

$$a = p_1 \cdots p_n$$

in irreduzible Elemente p_i.

Bemerkung. Ein Ring mit dieser Eigenschaft heißt *faktoriell*. Der Polynomring $\mathbb{Z}[x]$ ist faktoriell, aber kein Hauptidealring.

Beweis. Es genügt nach 2.17 die Existenz einer Zerlegung in Irreduzible zu zeigen. Angenommen $a \in R \setminus (R^\times \cup \{0\})$ hat keine Zerlegung in Irreduzible. Dann ist insbesondere a selbst nicht irreduzibel und es existieren daher $a_2, a_2' \in R \setminus (R^\times \cup \{0\})$ mit $a = a_2 \cdot a_2'$. Haben a_2 und a_2' beide eine Zerlegung in Irreduzible, so auch a, also habe ohne Enschränkung a_2 keine Zerlegung in Irreduzible. Setze $a_1 = a$. Wegen $a_2' \notin R^\times$ gilt $(a_1) \subsetneqq (a_2)$. Sukzessive erhalten wir eine Folge von Idealen $(a_1) \subsetneqq (a_2) \subsetneqq (a_3) \ldots$. Dies steht im Widerspruch zu Lemma 2.15. □

Definition 2.19. Sei R ein faktorieller Ring, P ein Repräsentantensystem der irreduziblen Elemente von R modulo Assoziiertheit, $a, b \in R$ mit Zerlegungen

$$a = u \prod_{p \in P} p^{n_p}, \qquad b = v \prod_{p \in P} p^{m_p}$$

($u, v \in R^\times$) Dann heißt

$$\mathrm{ggT}(a, b) = \prod_{p \in P} p^{\min(n_p, m_p)}$$

grösster gemeinsamer Teiler von a und b.

Bemerkung. Das Hauptideal $(\mathrm{ggT}(a, b))$ ist von der Wahl des Repräsentantensystems P unabhängig, d. h. $\mathrm{ggT}(a, b)$ ist bis auf Assoziiertheit wohlbestimmt.

Lemma 2.20 (Lemma von Bezout)**.** *Sei R ein Hauptidealring, $a, b \in R$. Dann gilt*

$$(\mathrm{ggT}(a, b)) = (a, b) = Ra + Rb$$

Insbesondere gibt es $x, y \in R$ mit

$$\mathrm{ggT}(a, b) = xa + yb$$

Beweis. Sei d ein Erzeuger des Hauptideals (a, b). Dann gilt $d \mid a$ und $d \mid b$, also

$$d = w \prod_{p \in P} p^{k_p}$$

mit $w \in R^\times$, $k_p \leq \min(n_p, m_p)$ und somit $d \mid \mathrm{ggT}(a, b)$. Andererseits gibt es $x, y \in R$ mit $d = xa + yb$ und somit $\mathrm{ggT}(a, b) \mid d$. Also

$$(a, b) = (d) = (\mathrm{ggT}(a, b)).$$

□

Korollar 2.21 (Chinesischer Restsatz)**.** *Sei R ein Hauptidealring, $a, b \in R$ mit* $\mathrm{ggT}(a, b) = 1$*. Die R-lineare Abbildung*

$$\varphi \colon R \to R/(a) \oplus R/(b), \quad r \mapsto (r + (a), r + (b))$$

induziert einen Isomorphismus $R/(ab) \cong R/(a) \oplus R/(b)$.

Beweis. Es gilt

$$\ker \varphi = \{r \in R \mid a \mid r, b \mid r\} \overset{\mathrm{ggT}(a,b)=1}{=} \{r \in R; \mid ab \mid r\} = (ab)$$

Seien $x, y \in R$, so dass $1 = \mathrm{ggT}(a, b) = xa + yb$ und $r_1 + (a) \in R/(a)$, $r_2 + (b) \in R/(b)$. Setze $r = r_1 yb + r_2 xa$. Dann gilt

$$r + (a) = r_1 yb + (a) = r_1 yb + r_1 xa + (a) = r_1 + (a).$$

Analog gilt $r + (b) = r_2 + (b)$. Also ist φ surjektiv. Nach dem Homomorphiesatz erhalten wir einen$R$-linearen Isomorphismus

$$\bar{\phi}\colon R/(ab) \to R/(a) \oplus R/(b), \qquad r + (ab) \mapsto (r + (a), r + (b)).$$

□

Korollar 2.22. *Sei R ein Hauptidealring. Das Ideal (π) ist maximal in R genau dann, wenn π ein Primelement ist.*

Beweis.
($\Rightarrow$): Zu zeigen: $R/(\pi)$ ist Körper. Sei $0 \neq \overline{a} \in R/(\pi)$ und $a \in R$ ein Vertreter. Dann gilt $\pi \nmid a$, also $\mathrm{ggT}(a, \pi) = 1$. Wähle $x, y \in R$ mit $xa + y\pi = 1$. Dann gilt $\overline{x} \cdot \overline{a} = 1$ in $R/(\pi)$, also $\overline{a}$ hat ein multiplikatives Inverses. Daher ist $R/(\pi)$ ein Körper und nach 1.19 folgt die Maximalität von (π).
($\Leftarrow$): Sei (π) maximal und $a, b \in R$ mit $\pi \mid ab$, $\pi \nmid a$. Dann gilt $\overline{ab} = 0$ im Körper $R/(\pi)$, aber $\overline{a} \neq 0$, also $\pi \mid b$. Daher ist π Primelement. □

2.3 Euklidische Ringe

Problem:

Sei R ein Hauptidealring, $a, b \in R$. Wie können wir $x, y \in R$ mit

$$\mathrm{ggT}(a, b) = xa + yb$$

bestimmen? In $\mathbb{Z}$ und $K[t]$ geht das, weil wir Division mit Rest ausführen können.

Definition 2.23. Ein Ring R heißt *euklidisch*, wenn er nullteilerfrei ist und es eine Abbildung $N\colon R \setminus \{0\} \to \mathbb{N}_0$ gibt mit

Zu $a, b \in R$, $b \neq 0$ gibt es $q, r \in R$ mit $a = bq + r$ und $r = 0$ oder $N(r) < N(b)$.

Man nennt dann N eine *euklidische Normfunktion* von R.

Bemerkung. Ein euklidischer Ring kann verschiedene euklidische Normfunktionen besitzen.

Der erweiterte euklidische Algorithmus

Gegeben: $a_0 \neq 0, a_1 \neq 0$ in R euklidisch mit Normfunktion N, $N(a_0) \geq N(a_1)$.

Gesucht: $\mathrm{ggT}(a_0, a_1)$, $x, y \in R$ mit $\mathrm{ggT}(a_0, a_1) = xa_0 + ya_1$.

Setze $k := 0$, $x_0 := 1$, $x_1 := 0$
Wiederhole:
Erhöhe k um 1
Bestimme a_{k+1} und q_k mit $a_{k-1} = a_k q_k + a_{k+1}$

und $a_{k+1} = 0$ oder $N(a_{k+1}) < N(a_k)$
(i. A. nicht effektiv)
Setze $x_{k+1} := x_{k-1} - q_k x_k$
bis $a_{k+1} = 0$.
Rückgabe $\mathrm{ggT}(a_0, a_1) := a_k$, $x := x_k$, $y := \frac{a_k - x_k a_0}{a_1}$.

Beispiele.

- $R = \mathbb{Z}$ und $N(a) = |a|$ (alternativ: $N(a) = a^2$)
- $R = K[t]$, K Körper und $N(f) = \deg(f)$
- $R = \mathbb{C}\{t\} = \left\{ \begin{array}{c} \text{Potenzreihen } \sum_{i=0}^{\infty} a_i t^i \text{ mit } a_i \in \mathbb{C}, \\ \text{die in einer offenen Umgebung von 0 konvergieren.} \end{array} \right\}$ und $N(f) = \min\{i | a_i \neq 0\}$. Es gilt $a = t^{N(a)}u$, $b = t^{N(b)}v$ mit $u, v \in R^\times$ und somit $b \mid a$ für $N(a) \geq N(b)$ und $a = 0 \cdot b + a$ für $N(a) < N(b)$.
- Analog: $R = \mathbb{R}\{t\}$,

$$R = K[[t]] = \{\text{formale Potenzreihen } \sum_{i=0}^{\infty} a_i t^i \text{ mit } a_i \in K\},$$

K Körper und $N(f) = \min\{i | a_i \neq 0\}$.

Satz 2.24. *Jeder euklidische Ring ist ein Hauptidealring.*

Beweis. Sei R euklidisch, insbesondere nullteilerfrei, und $\mathfrak{a} \subset R$ ein Ideal. (0) ist Hauptideal, also sei ohne Einschränkung $\mathfrak{a} \neq (0)$. Dann gibt es in $\mathfrak{a}$ ein Element $a_0 \neq 0$ mit $N(a_0) = \min_{a \in \mathfrak{a}} N(a)$.

Behauptung: $\mathfrak{a} = (a_0)$.
Grund: Die Inklusion $(a_0) \subset \mathfrak{a}$ ist klar. Sei $a \in \mathfrak{a}$ beliebig. Dann gibt es $q, r \in R$ mit $a = qa_0 + r$, insbesondere $r \in \mathfrak{a}$. Da $N(r) < N(a_0)$ nicht möglich ist, gilt $r = 0$, also $a \in (a_0)$. □

Korollar 2.25. *$\mathbb{Z}$ und $K[t]$ sind Hauptidealringe, ebenso $\mathbb{C}\{t\}$, $\mathbb{R}\{t\}$, $K[[t]]$.*

Weitere Beispiele:

Sei $d \in \mathbb{Z}$ quadratfrei, d. h. durch keine Quadratzahl außer 1 teilbar. Setze

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{d} & \text{falls } d \equiv 2, 3 \mod 4 \\ \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2} & \text{falls } d \equiv 1 \mod 4 \end{cases}$$

($\mathcal{O}_{\mathbb{Q}(\sqrt{d})} \subset \mathbb{Q}(\sqrt{d}) = \mathbb{Q}[x]/(x^2 - d)$ ist der Ganzheitsring des Körpers $\mathbb{Q}(\sqrt{d})$.)

$$N \colon \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}, \qquad a + b\sqrt{d} \mapsto |a^2 - db^2|$$

Dann gilt $N(\mathcal{O}_{\mathbb{Q}(\sqrt{d})}) \subset \mathbb{N}$.

Theorem 2.26.

- $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ *ist euklidisch mit der Normfunktion* N *genau dann, wenn*

  $$d \in \{-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}$$

  (Chatland & Davenport, Inkeri, 1950)

- *Für*

  $$d \in \{-19, -43, -67, -163\}$$

  ist $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ *Hauptidealring, aber nicht euklidisch. Für alle übrigen* $d < 0$ *ist* $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ *kein Hauptidealring.*

- $\mathcal{O}_{\mathbb{Q}(\sqrt{69})}$ *ist euklidisch, aber mit einer anderen Normfunktion (Clark, 1994).*

- *Offene Vermutung (Gauß):* $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ *ist für unendlich viele* $d > 0$ *ein Hauptidealring.*

- *Von diesen sind alle bis auf höchstens* 2 *euklidisch (Narkiewicz, 2007) (alle, wenn die verallgemeinerte riemannsche Vermutung gilt).*

Beispiele.

$d = -1$: $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i] = \mathbb{Z}[x]/(x^2 - 1)$ ist normeuklidisch (Ring der Gauß-Zahlen)

$d = -3$: $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})} = \mathbb{Z}[\zeta_3]$, $\zeta_3 = \frac{-1+i\sqrt{3}}{2} = e^{\frac{2\pi i}{3}}$, $x^3 - 1 = (x-1)(x-\zeta_3)(x-\zeta_3^2)$, ist normeuklidisch (Eisenstein-Zahlen).

$d = -5$: $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}]$ ist kein Hauptidealring und auch nicht faktoriell.

2.4 Äquivalente Matrizen und Determinantenideale

Sei R ein kommutativer Ring.

Definition 2.27. Matrizen $M, N \in M_{m,n}(R)$ heißen *äquivalent* ($M \sim N$) wenn invertierbare Matrizen $C \in M_{n,n}(R)$, $D \in M_{m,m}(R)$ mit

$$D \cdot M = N \cdot C$$

existieren.
Im Fall $n = m$ heißen M und N *ähnlich*, wenn $C = D$ gewählt werden kann ($M \approx N$).

Satz 2.28. *Sei* K *ein Körper,* $M, N \in M_{m,n}(K)$*. Dann gilt* $M \sim N$ *genau dann, wenn* $\mathrm{Rg}(M) = \mathrm{Rg}(N)$.

Beweis.
LA I, Kor. 4.23: $M \sim N \Rightarrow \operatorname{Rg}(M) = \operatorname{Rg}(N)$.
LA I, Kor. 4.25: Für jede Matrix $M \in M_{m,n}(K)$ gilt

$$M \sim \begin{pmatrix} E_{\operatorname{Rg} M} & 0 \\ 0 & 0 \end{pmatrix}$$

($E_r \in M_{r,r}(K)$ Einheitsmatrix). □

Bemerkung. Die entsprechende Frage für $\approx$ konnte in der LA I noch nicht beantwortet werden.

Wie kann man allgemein feststellen, ob zwei Matrizen äquivalent sind?

Definition 2.29. Sei $A = (a_{ij}) \in M_{m,n}(R)$, $I \subset \{1, \ldots, m\}$, $J \subset \{1, \ldots, n\}$ r-elementige Teilmengen mit der natürlichen Ordnung. Dann sei $\det_{I,J}(A) \in R$ die Determinante der Matrix $(a_{ij})_{i \in I, j \in J} \in M_{r,r}(R)$. Die $\det_{I,J}(A)$ heißen die Minoren der Ordnung r von A.

Theorem 2.30 (Cauchy-Binet-Formel)**.** *Sei $A \in M_{m,n}(R)$, $B \in M_{n,k}(R)$, $I \subset \{1, \ldots, m\}$, $J \subset \{1, \ldots, k\}$ r-elementige Teilmengen. Dann gilt*

$$\det_{I,J}(AB) = \sum_{\substack{K \subset \{1,\ldots,n\} \\ \sharp K = r}} \det_{I,K}(A) \det_{K,J}(B).$$

Beweis. Ist deutlich einfacher mit etwas multilinearer Algebra, siehe später. □

Definition 2.31. Sei $A \in M_{m,n}(R)$. Für $r \in \mathbb{N}_0$ heißt das von den Minoren der Ordnung r erzeugte Ideal $I_r(A)$ das *r-te Determinantenideal von A.*

Beispiel. Sei

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \in M_{2,3}(\mathbb{Z}).$$

Dann gilt

$$\begin{aligned} I_0(A) &= (1) \qquad \text{(Die Determinante der leeren Matrix ist 1.)} \\ I_1(A) &= (1, 2, 3, 4, 5, 6) = (1) \\ I_2(A) &= (-3, -6, -3) = (3) \\ I_r(A) &= (0), \qquad r > 2 \end{aligned}$$

Lemma 2.32. *Sei $A \in M_{m,n}(R)$.Dann gilt*

(i) $I_r(A) = I_r(A^t)$.

(ii) $I_{r+1}(A) \subset I_r(A)$

(iii) $I_r(AB) \subset I_r(A)I_r(B)$ *für* $B \in M_{n,k}(R)$.

(iv) $I_r(A) = I_{r+k}\left(\begin{pmatrix} A & 0 \\ 0 & E_k \end{pmatrix}\right)$.

(iv) Sei $\phi\colon R \to S$ *ein Homomorphismus kommutativer Ringe. Dann gilt*

$$I_r(\phi(A)) = I_r(A)S.$$

Dabei wird für ein Ideal $\mathfrak{a} \subset R$ *das von* $\mathfrak{a}$ *in* S *erzeugte Ideal mit*

$$\mathfrak{a}S = \{\sum_i \phi(a_i)s_i | a_i \in \mathfrak{a}, s_i \in S\}$$

bezeichnet.

Beweis.
(i) C ist genau dann $r \times r$-Untermatrix von A, wenn C^t $r \times r$-Untermatrix von A^t ist und es gilt $\det_R C^t = \det_R C$. Also gilt $I_r(A) = I_r(A^t)$.
(ii) Sei $C = (c_{ij})$ eine $(r+1)\times(r+1)$-Untermatrix von A und C_{ij} die Untermatrix von C, die aus C durch Streichen von i-ter Zeile und j-ter Spalte entsteht. Nach dem Entwicklungssatz von Laplace (LA I, Kor 6.18) gilt:

$$\det C = \sum_{i=1}^{n} (-1)^{i+j} c_{ij} \det(C_{ij}).$$

Insbesondere ist $\det(C)$ eine R-Linearkombination von Minoren der Ordnung r von A.
(iii) folgt aus der Cauchy-Binet-Formel.
(iv) Es reicht, $k = 1$ zu betrachten. Ist C eine $r\times r$-Untermatrix von A, so ist $\left(\begin{smallmatrix} C & 0 \\ 0 & 1 \end{smallmatrix}\right)$ eine $(r+1) \times (r+1)$-Untermatrix von $B = \left(\begin{smallmatrix} A & 0 \\ 0 & 1 \end{smallmatrix}\right)$ mit derselben Determinante. Also gilt $I_r(A) \subset I_{r+1}(B)$. Ist C' eine Untermatrix von B, die die letze Spalte, aber nicht die letze Zeile enthält oder umgekehrt, so gilt $\det C' = 0$. Enthält C' weder die letzte Spalte noch die letzte Zeile, ist C' eine Untermatrix von A und $\det C' \in I_{r+1}(A) \subset I_r(A)$. Damit gilt $I_{r+1}(B) \subset I_r(A)$.
(v) folgt aus $\det_S \phi(C) = \phi(\det_R C)$ (LA I, Bemerkung nach 6.8). □

Satz 2.33. *Sei* $A \sim B \in M_{m,n}(R)$. *Dann gilt* $I_r(A) = I_r(B)$.

Beweis. Wegen $I_r(A) = I_r(A^t)$ reicht es, $I_r(CA) = I_r(A)$ für $C \in \mathrm{Gl}_m(R)$ zu zeigen. Nach dem Lemma gilt

$$I_r(CA) \subset I_r(C)I_r(A) \subset I_r(A).$$

Andererseits gilt $A = C^{-1}CA$, also auch

$$I_r(A) \subset I_r(CA).$$

□

Beispiel. Sei

$$B = \begin{pmatrix} 3 & 2 & 1 \\ 4 & 5 & 6 \end{pmatrix} \in M_{2,3}(\mathbb{Z}).$$

Dann gilt $I_0(B) = I_0(A)$, $I_1(B) = I_1(A)$, aber

$$I_2(B) = (7, 14, 7) = (7) \neq I_2(A),$$

Also $A \not\sim B$.

Andersherum gilt das i. A. nicht:

Beispiel. Sei $R = \mathbb{Q}[x, y, z]$,

$$A = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}, \quad B = \begin{pmatrix} x & 0 \\ y & z \end{pmatrix} = A^t \in M_{2,2}(R)$$

Dann gilt $I_r(A) = I_r(B)$ für alle r, aber $A \not\sim B$. (Übungsaufgabe)

2.5 Smith-Normalform

Definition 2.34. Sei $r = \min(m, n)$. Wir nennen eine nicht notwendig quadratische Matrix der Form $\operatorname{diag}(a_1, \ldots, a_r) = (a_{ij}) \in M_{m,n}(R)$ mit

$$a_{ij} = \begin{cases} a_i & \text{falls } i = j \\ 0 & \text{falls } i \neq j \end{cases}$$

Diagonalmatrix.

Theorem 2.35 (Elementarteilersatz für Matrizen)**.** *Jede $m \times n$-Matrix A über einem Hauptidealring ist äquivalent zu einer Diagonalmatrix der Form*

$$\operatorname{diag}(a_1, \ldots, a_r)$$

mit $r = \min(m, n)$, $a_1 \mid a_2 \mid \cdots \mid a_r$. Die Folge der Ideale $(a_1), \ldots, (a_r)$ ist eindeutig bestimmt.

Definition 2.36. $a_1, \ldots, a_r$ heißen die *Elementarteiler* (auch *invariante Faktoren*) der Matrix A. Die Matrix $\operatorname{diag}(a_1, \ldots, a_r)$ heißt *Smith*-Normalform von A.

Beispiele. Sei R ein Hauptidealring.

(i) Sei

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2,2}(R)$$

mit $a \neq 0$. Dann existieren $x, y \in R$ mit $e = \mathrm{ggT}(a, c) = xa + yc$. Die Matrix

$$C = \begin{pmatrix} x & y \\ -\frac{c}{e} & \frac{a}{e} \end{pmatrix}$$

hat Determinante $\frac{xa+yb}{e} = 1$, ist also invertierbar (LA I, Kor. 6.22) und es gilt

$$CA = \begin{pmatrix} e & xb + yd \\ 0 & \frac{\det A}{e} \end{pmatrix}$$

Falls $a = e$ wählen wir $x = 1$, $y = 0$. Falls $b = 0$ ist dann CA eine Diagonalmatrix.

(ii) Analog existieren $w, z \in R$ mit $f = \mathrm{ggT}(a, b) = wa + zb$ und

$$A \begin{pmatrix} w & -\frac{b}{f} \\ z & \frac{a}{f} \end{pmatrix} = \begin{pmatrix} f & 0 \\ cw + dz & \frac{\det A}{f} \end{pmatrix}.$$

(iii) Ist $A = \mathrm{diag}(a, d) \in M_{2,2}(R)$ und $e = \mathrm{ggT}(a, d) = xa + yd$, so gilt

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & d \\ 0 & d \end{pmatrix},$$
$$\begin{pmatrix} 1 & 0 \\ -\frac{yd}{e} & 1 \end{pmatrix} \begin{pmatrix} a & d \\ 0 & d \end{pmatrix} \begin{pmatrix} x & -\frac{d}{e} \\ y & \frac{a}{e} \end{pmatrix} = \begin{pmatrix} e & 0 \\ 0 & \frac{ad}{e} \end{pmatrix}$$

und $e \mid \frac{ad}{e}$.

(iv) Sei

$$A = \begin{pmatrix} 8 & 12 & 0 \\ 9 & 15 & 0 \\ 12 & 24 & 20 \end{pmatrix} \in M_{3,3}(\mathbb{Z}).$$

Dann gilt

$$
\begin{aligned}
A &\sim A \begin{pmatrix} -1 & -3 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 4 & 0 & 0 \\ 6 & 3 & 0 \\ 12 & 12 & 20 \end{pmatrix} = A_1 \\
&\sim \begin{pmatrix} -1 & 1 & 0 \\ -3 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} A_1 = \begin{pmatrix} 2 & 3 & 0 \\ 0 & 6 & 0 \\ 12 & 12 & 20 \end{pmatrix} = A_2 \\
&\sim A_2 \begin{pmatrix} -1 & -3 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 6 & 12 & 0 \\ 0 & -12 & 20 \end{pmatrix} = A_3 \\
&\sim \begin{pmatrix} 1 & 0 & 0 \\ -6 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} A_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 12 & 0 \\ 0 & -12 & 20 \end{pmatrix} = A_4 \\
&\sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} A_4 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 12 & 0 \\ 0 & 0 & 20 \end{pmatrix} = A_5 \\
&\sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} A_5 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 12 & 20 \\ 0 & 0 & 20 \end{pmatrix} = A_6 \\
&\sim A_6 \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & -5 \\ 0 & -1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & -20 & 60 \end{pmatrix} = A_7 \\
&\sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 5 & 1 \end{pmatrix} A_7 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 60 \end{pmatrix}
\end{aligned}
$$

Sei R ein Hauptidealring.

Definition 2.37. Sei $a \in R$. Die Zahl

$$
\ell(a) = \begin{cases} \infty & \text{falls } a = 0. \\ 0 & \text{falls } a \in R^\times \\ \text{Anzahl der Primfaktoren von } a & \text{sonst.} \end{cases}
$$

heißt *Länge von a*.

Existenz der Smith-Normalform:

Algorithmus SNF

Gegeben: $A = (a_{ij})$
Gesucht: Smith-Normalform $D = \mathrm{SNF}(A)$ (und invertierbare Matrizen X, Y mit

$D = XAY$).

Falls A die Nullmatrix: fertig.
Sonst tausche Zeilen und Spalten in A bis $a_{11} \neq 0$.
Solange es in der ersten Zeile oder Spalte Einträge b gibt,
    die nicht durch a_{11} teilbar sind:
        Multipliziere A mit einer invertierbaren Matrix,
            so dass a_{11} durch $\mathrm{ggT}(a_{11}, b)$ ersetzt wird.
(Die Schleife bricht ab, weil $\ell(\mathrm{ggT}(a_{11}, b)) < \ell(a_{11}) < \infty$,
    d. h. in jedem Durchgang wird $\ell(a_{11})$ kleiner.)
Räume die erste Zeile und Spalte von A aus.
Sei A' die Matrix, die aus A durch Streichen
    der ersten Zeile und Spalte entsteht.
Wende Algorithmus SNF auf A' an mit Ergebnis
    $\mathrm{diag}(a_2, \dots, a_r)$, $a_2 \mid a_3 \mid \cdots \mid a_r$
Setze $a_1 := a_{11}$, $D := \mathrm{diag}(a_1, a_2, \dots, a_r)$
Von $i := 1$ bis $r - 1$:
    Setze $e := \mathrm{ggT}(a_i, a_{i+1})$.
    Durch Rechts- und Linksmultiplikation mit geeigneten Matrizen:
    Ersetze a_{i+1} durch $\frac{a_i a_{i+1}}{e}$ und a_i durch e.
    (Danach gilt $a_1 \mid \cdots \mid a_i \mid a_{i+1}$ und $a_i \mid a_{i+2} \mid \cdots \mid a_r$)
    (Insbesondere gilt $a_i \mid \mathrm{ggT}(a_{i+1}, a_{i+2})$)
Rückgabe von D.

Eindeutigkeit der Smith-Normalform:

Satz 2.38. *Sei $A \in M_{m,n}(R)$ und $D = \mathrm{diag}(a_1, \dots, a_r)$, $r = \min(m, n)$, eine Smith-Normalform von A und b_k ein Erzeuger des Hauptideals $I_k(A)$. Dann gilt*

$$b_k \mathrel{\hat{=}} \prod_{i=1}^{k} a_i.$$

Insbesondere gilt für $k > 0$

$$a_k \mathrel{\hat{=}} \frac{b_k}{b_{k-1}}$$

Beweis. Nach Satz 2.33 gilt

$$I_k(A) = I_k(D) = (\det_{I,J} D \colon I \subset \{1, \dots, m\}, J \subset \{1, \dots, n\}, \sharp I = \sharp J = k)$$

Falls I oder J nicht in $\{1, \dots, r\}$ enthalten sind, ist $\det_{I,J} D$ die Determinante einer Matrix mit einer Nullzeile oder -spalte, also gleich 0, ebenso, falls $I \neq J$. Also gilt

$$I_k(D) = (\det_{I,I} D = \prod_{i \in I} a_i \colon I \subset \{1, \dots, r\}, \sharp I = k).$$

Sei $I = \{i_1 < i_2 < \cdots < i_k\}$. Dann gilt $a_j \mid a_{i_j}$ und somit

$$\prod_{j=1}^{k} a_j \mid \prod_{i \in I} a_i.$$

Damit gilt

$$(b_k) = I_k(A) = (\prod_{j=1}^{k} a_j),$$

also auch

$$b_k \mathrel{\hat{=}} \prod_{j=1}^{k} a_j.$$

□

Da die b_k bis auf Assoziiertheit eindeutig bestimmt sind, gilt dies nun auch für die a_k. Damit ist der Beweis von Theorem 2.35 vollständig.

Korollar 2.39. *Sei $A \in M_{n,n}(R)$. Dann gilt:*

$$\det(A) \mathrel{\hat{=}} a_1 \cdots a_n,$$

wobei $a_1, \ldots, a_n$ die Elementarteiler von A sind.

Beweis.

$$(\det(A)) = I_n(A) = (\prod_{i=1}^{n} a_i)$$

□

Korollar 2.40. *Sei S ein weiterer Hauptidealring und $\phi\colon R \to S$ ein Ringhomomorphismus. Sind $a_1, \ldots, a_r$ die Elementarteiler von $A \in M_{m,n}(R)$, so sind $\phi(a_1), \ldots, \phi(a_r)$ die Elementarteiler von $\phi(A) \in M_{m,n}(S)$.*

Beweis. Klar, weil $I_k(A)S = I_k(\phi(A))$. □

Korollar 2.41. *Sei $A \in M_{m,n}(R)$ mit Elementarteilern $a_1, \ldots, a_r \in R$. Betrachte A mittels der kanonischen Einbettung $R \subset Q(R)$ als ein Element von $M_{m,n}(Q(R))$. Dann gilt*

$$\mathrm{Rg}_{Q(R)}(A) = \max\{i\colon a_i \neq 0\}$$

Beweis. Die Aussage folgt mit 2.40 und 2.28. Beachte: In $Q(R)$ ist jedes Element $a \neq 0$ assoziiert zu 1. □

2.6 Endlich erzeugte Moduln über Hauptidealringen

Sei R ein kommutativer Ring. Für $A \in M_{m,n}(R)$ sei $\operatorname{coker}(A)$ der R-Modul $\operatorname{coker}(R^n \xrightarrow{A\cdot} R^m) = R^m/\operatorname{im}(A)$.
Erinnerung: Jeder endlich präsentierbare R-Modul ist von dieser Gestalt.

Definition 2.42. Sei $M \cong \operatorname{coker}(A)$ endlich präsentierbar.

$$\operatorname{Fitt}_r(M) = \begin{cases} (1) & \text{falls } r \geq m \\ I_{m-r}(A) & \text{sonst} \end{cases}$$

heißt das r-te Fitting-Ideal von M.

Bis auf die Verschiebung um m und die umgekehrte Nummerierung unterscheiden sich Fitting-Ideale und Determinantenideale nicht. Durch die Verschiebung um m erreichen wir, dass die Fitting-Ideale nur von M und nicht von der Wahl der Präsentation abhängen. Die umgekehrte Nummerierung ist reine Konventionsfrage.

Satz 2.43. $\operatorname{Fitt}_r(M)$ *ist von der Wahl der Präsentation unabhängig: Gilt*

$$\operatorname{coker}(A) \cong M \cong \operatorname{coker}(B)$$

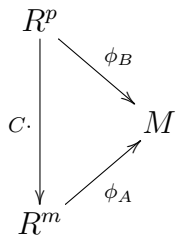
für $A \in M_{m,n}(R)$, $B \in M_{p,q}(R)$, *so gilt*

$$\operatorname{Fitt}_r(\operatorname{coker}(A)) = \operatorname{Fitt}_r(\operatorname{coker}(B)).$$

Beweis. Sei $\phi_A \colon R^m \to \operatorname{coker}(A) \to M$ die Zusammensetzung des Isomorphismus mit der natürlichen Projektion und $x_1, \ldots, x_m \in M$ die Bilder der Standardbasis von R^m. Analog konstruieren wir $\phi_B \colon R^p \to \operatorname{coker}(B) \to M$ und $y_1, \ldots, y_p \in M$. Da $(x_1, \ldots, x_m)$ ein Erzeugendensystem von M ist, finden wir $c_{ij} \in R$ so dass

$$y_j = \sum_{i=1}^{m} c_{ij} x_i,$$

d. h. $C = (c_{ij}) \in M_{m,p}$ ist so gewählt, dass das Diagramm



kommutiert.

Setze

$$\phi\colon R^{m+p} = R^m \oplus R^p \to M, \qquad \left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) \mapsto \phi_A(x) + \phi_B(y).$$

und

$$A' = \begin{pmatrix} A & -C \\ 0 & E_p \end{pmatrix} = \begin{pmatrix} E_m & -C \\ 0 & E_p \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & E_p \end{pmatrix} \in M_{m+p,n+p}(R).$$

Dann gilt $\mathrm{im}(A') = \ker(\phi)$ und somit $M \cong \mathrm{coker}(A')$:
Sei $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) \in \ker(\phi)$. Dann gilt

$$0 = \phi_A(x) + \phi_B(y) = \phi_A(x + Cy),$$

also gibt es ein $z \in R^n$ mit $Az = x + Cy$ und es gilt

$$A' \left(\begin{smallmatrix} z \\ y \end{smallmatrix}\right) = \left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right).$$

und somit $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) \in \mathrm{im}(A')$.
Andersherum gilt

$$\phi(A' \left(\begin{smallmatrix} z \\ y \end{smallmatrix}\right)) = \phi_A(Az - Cy) + \phi_B(y) = \phi_A(Az) = 0.$$

Nun gilt

$$\mathrm{Fitt}_r(\mathrm{coker}(A)) = I_{m-r}(A) = I_{m+p-r}\left(\left(\begin{smallmatrix} A & 0 \\ 0 & E_p \end{smallmatrix}\right)\right) = I_{m+p-r}(A') = \mathrm{Fitt}_r(\mathrm{coker}(A')).$$

Dieselbe Konstruktion mit A und B vertauscht liefert $B' \in M_{m+p,m+q}(R)$ mit $\mathrm{Fitt}_r(\mathrm{coker}(B)) = \mathrm{Fitt}_r(\mathrm{coker}(B'))$ und $\mathrm{im}(B') = \ker(\phi) = \mathrm{im}(A')$.

Wir drücken jetzt wieder die Bilder der Standardbasis unter der Abbildung $R^{n+p} \to \ker(\phi)$, $x \mapsto B'x$ durch die Bilder der Standardbasis unter $R^{m+q} \to \ker(\phi)$, $x \mapsto A'x$ aus und erhalten eine Matrix $X \in M_{n+p,m+q}(R)$ mit $A'X = B'$. Analog erhalten wir eine Matrix $Y \in M_{m+q,n+p}(R)$ mit $B'Y = A'$. Nun gilt

$$I_{m+p-r}(B') \subset I_{m+p-r}(A')I_{m+p-r}(X) \subset I_{m+p-r}(A')$$

und analog $I_{m+p-r}(B') \subset I_{m+p-r}(A')$, also

$$\mathrm{Fitt}_r(\mathrm{coker}(A)) = \mathrm{Fitt}_r(\mathrm{coker}(B)).$$

□

Bemerkung. Ist $\phi\colon M \to N$ ein Isomorphismus, so ist jede endliche Präsentation von M auch eine von N und umgekehrt. Insbesondere gilt $\mathrm{Fitt}_r(M) = \mathrm{Fitt}_r(N)$. Die Fitting-Ideale hängen also nur von der Isomorphieklasse von M ab.

Korollar 2.44. *Sei R ein Hauptidealring. Für Matrizen $A, B \in M_{m,n}(R)$ sind äquivalent:*

(i) $A \sim B$,

(ii) A *und* B *haben dieselben Elementarteiler,*

(iii) $I_r(A) = I_r(B)$ *für alle* r.

(iv) $\operatorname{coker}(A) \cong \operatorname{coker}(B)$

(v) $\operatorname{Fitt}_r(\operatorname{coker}(A)) = \operatorname{Fitt}_r(\operatorname{coker}(B))$ *für alle* r.

Beweis.
(i) $\Leftrightarrow$ (ii): A und B sind beide äquivalent zu ihrer Smith-Normalform.
(i) $\Rightarrow$ (iii): Satz 2.33.
(iii) $\Rightarrow$ (ii): Satz 2.38
(iii) $\Leftrightarrow$ (v): klar wegen $\operatorname{Fitt}_r = I_{m-r}$.
(iv) $\Rightarrow$ (v): Satz 2.43.
(i) $\Rightarrow$ (iv): Ist $A \sim B$, so existieren invertierbare C, D mit $DA = BC$. Das bedeutet, dass das Diagramm von R-Moduln

$$\begin{array}{ccc} R^n & \xrightarrow{A} & R^m \\ \downarrow{\scriptstyle C} & & \downarrow{\scriptstyle D} \\ R^n & \xrightarrow{B} & R^m \end{array}$$

kommutativ ist. Da die Linksmultiplikationen mit C und D Isomorphismen sind, ist auch der auf den Kokernen induzierte Homomorphismus

$$\operatorname{coker}(A) \to \operatorname{coker}(B), x + \operatorname{im}(A) \mapsto Dx + \operatorname{im}(B)$$

ein Isomorphismus. □

Theorem 2.45 (Struktursatz für endlich erzeugte Moduln über einem Hauptidealring)**.** *Sei* M *ein endlich erzeugter Modul über einem Hauptidealring* R*. Dann existieren von Null verschiedene Ideale* $(a_1) \supseteq (a_2) \cdots \supseteq (a_n)$ *und ein* $r \geq 0$ *so dass*

$$M \cong R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_n).$$

Die Zahlen r *und* n*, und die Ideale* $(a_1), \ldots, (a_n)$ *sind eindeutig bestimmt. Die Zahl* r *ist die kleinste Zahl, so dass*

$$\operatorname{Fitt}_r(M) \neq (0).$$

Die Zahl n *ist die kleinste Zahl, so dass*

$$\operatorname{Fitt}_{r+n}(M) = (1).$$

Definition 2.46. Die Elemente $a_1, \cdots, a_n$ heißen die *Elementarteiler* von M und sind bis auf Assoziiertheit wohlbestimmt. Die Zahl $r = r(M)$ wird als *Rang* des Moduls M bezeichnet.

Beweis. Da R noethersch ist, finden wir eine endliche Präsentation $M \cong \operatorname{coker}(A)$ mit $A \in M_{p,q}(R)$. Wir dürfen annehmen, dass $A = \operatorname{diag}(x_1, \ldots, x_s)$, $s = \min(p, q)$, in Smith-Normalform ist. Dann gilt

$$M \cong \operatorname{coker}(A) = \bigoplus_{i=1}^{s} R/(x_i) \oplus R^t$$

mit $s + t = p$. Einige dieser Faktoren können allerdings trivial oder gleich R sein: Seien $x_1, \ldots, x_v$ Einheiten und $x_{v+n+1} = \cdots = x_s = 0$. Setze $r = p - v - n$ und $a_i = x_{i+v}$. Dann gilt

$$M \cong \bigoplus_{i=1}^{n} R/(a_i) \oplus R^r.$$

Es gilt

$$\operatorname{Fitt}_i(M) = I_{p-i}(A) = (\prod_{j=1}^{p-i} x_j) = \begin{cases} (1) & \text{falls } i \geq p - v = r + n \\ (0) & \text{falls } i \leq p - v - n - 1 = r - 1 \\ (\prod_{j=1}^{r+n-i} a_j) & \text{sonst.} \end{cases}$$

Insbesondere sind die a_i durch die Fitting-Ideale bis auf Assoziiertheit eindeutig bestimmt. □

Korollar 2.47. *Sei $A \in M_{p,q}(R)$. Dann gilt $r(\operatorname{coker} A) = p - \operatorname{Rg}_{Q(R)} A$.*

Beweis. Sei wie eben $A = \operatorname{diag}(x_1, \ldots, x_s)$ in Smith-Normalform. Dann gilt $\operatorname{Rg}_{Q(R)} A = v + n$ und somit $r(\operatorname{coker} A) = p - \operatorname{Rg}_{Q(R)} A$. □

Korollar 2.48. *Seien M und N endlich erzeugte Moduln über einem Hauptidealring. Dann gilt $M \cong N$ genau dann, wenn $r(M) = r(N)$ und M und N dieselben Elementarteiler haben.*

Beweis. Klar haben isomorphe Moduln denselben Rang und dieselben Elementarteiler. Umgekehrt gilt

$$M \cong R^{r(M)} \oplus R/(a_1) \oplus \cdots \oplus R/(a_n) \cong N.$$

□

Korollar 2.49. *Sei M ein endlich erzeugter Modul über einem Hauptidealring mit Elementarteilern $a_1, \ldots, a_n$. Dann gilt*

$$T(M) \cong R/(a_1) \oplus \cdots \oplus R/(a_n).$$

Beweis. Sei $r = r(M)$,

$$x = (y_1, \ldots, y_r, x_1 + (a_1), \ldots, x_n + (a_n)) \in R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_n) =: X \cong M.$$

und $r \in R$. Dann gilt

$$rx = 0 \Leftrightarrow y_1 = \cdots = y_r = 0 \text{ und } rx_i \in (a_i) \text{ für } i = 1, \ldots, n.$$

Also

$$R/(a_1) \oplus \ldots R/(a_n) \cong T(X) \overset{2.13}{\cong} T(M).$$

□

Korollar 2.50. *Sei M endlich erzeugter Modul über einem Hauptidealring. Dann ist M genau dann frei, wenn er torsionfrei ist. Insbesondere ist jeder endlich erzeugte Untermodul eines freien Moduls frei.*

Beweis. Da der Hauptidealring R nullteilerfrei ist, wissen wir bereits, dass freie Moduln und ihre Untermoduln torsionsfrei sind. Sei M torsionsfrei und endlich erzeugt. Da $T(M) = 0$ folgt, dass die Folge der Elementarteiler leer ist und dass $M \cong R^{r(M)}$. □

Bemerkung. $R = \mathbb{Z}$, $M = \mathbb{Q}$ ist torsionsfrei aber nicht frei (keine zwei Elemente sind linear unabhängig). Daher ist der erste Teil von 2.50 falsch für nicht endlich erzeugte Moduln. Man kann jedoch (mit dem Zorn'schen Lemma) zeigen, dass jeder Untermodul (endlich erzeugt oder nicht) eines freien Moduls über einem Hauptidealring wieder frei ist.

Korollar 2.51. *Sei M ein endlich erzeugter Torsionsmodul über einem Hauptidealring R und a_n der größte Elementarteiler. Dann gilt*

$$(a_n) = \{x \in R | xm = 0 \text{ für alle } m \in M\} =: \mathrm{Ann}_R(M)$$

*(*Annullator von M*)*

Beweis. Ohne Einschränkung

$$M = \bigoplus_{i=1}^{n} R/(a_i)$$

mit $a_1 \mid \cdots \mid a_n$. Klar gilt $a_n m = 0$ für alle $m \in M$ und somit $(a_n) \subset \mathrm{Ann}_R(M)$. Sei umgekehrt $x \in R$ und

$$e_n = (\underbrace{0, \ldots, 0}_{n-1}, 1) \in M$$

Dann gilt $xe_n = 0$ genau dann, wenn $x \in (a_n)$. Also $\mathrm{Ann}_R(M) \subset (a_n)$. □

Korollar 2.52. *Sei R ein Hauptidealring und M ein endlich erzeugter R-Torsionsmodul. Dann existieren eindeutig bestimmte maximale Ideale $(p_1), \ldots, (p_n)$, für jedes $i = 1, \ldots, n$ eindeutig bestimmte Zahlen $v_{i_1} \leq v_{i_2} \leq \cdots \leq v_{i,m_i}$ und ein Isomorphismus von R-Moduln*

$$M \cong \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{m_i} R/(p_i^{v_{ij}}).$$

Beweis. Für $a = p_1^{e_1} \cdots p_r^{e_r}$ mit p_i prim und paarweise verschieden gilt nach dem chinesischen Restsatz:

$$R/(a) \cong R/(p_1^{e_1}) \oplus \cdots \oplus R/(p_r^{e_r}).$$

Daher kann man die Existenz der Zerlegung aus dem Hauptsatz über endlich erzeugte Moduln ableiten. Sei nun eine Zerlegung

$$M \cong \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{m_i} R/(p_i^{v_{ij}})$$

gegeben. Setze $m = \max\{m_1, \ldots, m_n\}$ und für $j = 1, \ldots, m$

$$a_j = \prod_{i=1}^{n} p_i^{v_{i,j+m_i-m}}$$

(mit $v_{ik} = 0$ für $k < 1$). Dann gilt $a_j \mid a_{j+1}$ und

$$M \cong \bigoplus_{j=1}^{m} R/(a_j),$$

wieder nach dem chinesischen Restsatz. Also sind die a_j die Elementarteiler von M. Ist

$$M \cong \bigoplus_{i=1}^{n'} \bigoplus_{j=1}^{m'_i} R/(q_i^{v'_{ij}})$$

eine weitere Zerlegung, so folgt aus der Eindeutigkeit der Elementarteiler $m = \max\{m'_1, \ldots, m'_{n'}\}$ und

$$a_j \mathrel{\hat{=}} \prod_{i=1}^{n'} q_i^{v'_{i,j+m'_i-m}}.$$

Aus der Eindeutigkeit der Primfaktorzerlegung folgt nach Umnummerierung der q_i, dass $m'_i = m_i$, $n' = n$, $v_{ij} = v'_{ij}$ und $(p_i) = (q_i)$. □

Bemerkung. Die Ideale $(p_i^{v_{ij}})$ werden *invariante Faktoren* (manchmal auch *Elementarteiler*) genannt.

Korollar 2.53 (*Elementarteilersatz*)**.** *Sei R ein Hauptidealring, F ein freier R-Modul vom Rang n und $M \subset F$ ein Untermodul. Dann existiert eine Basis $(e_1, \ldots, e_n)$ von F, eine Zahl m, $0 \leq m \leq n$ und von 0 verschiedene Elemente $a_1, \ldots, a_m \in R$ so dass*

(i) $(a_1 e_1, \ldots, a_m e_m)$ *ist eine Basis von* M.

(ii) $a_i \mid a_{i+1}$ *für* $i = 1, \ldots, m-1$.

Die Zahl m und die Folge von Idealen $(a_1) \supseteq (a_2) \supseteq \cdots \supseteq (a_m)$ sind eindeutig bestimmt.

Beweis. M ist als Untermodul des endlich erzeugten, freien Moduls F frei und endlich erzeugt. Wähle nun eine Basis $(f_1, \ldots, f_m)$ von M und eine Basis $(e_1, \ldots, e_n)$ von F so, dass die Darstellungsmatrix der Inklusion $M \subset F$ in Smith-Normalform $\operatorname{diag}(a_1, \ldots, a_r)$ ist. Es gilt dann $a_i e_i = f_i$. Da die Inklusionsabbildung injektiv ist, ist $a_i = 0$ nicht möglich und $m = r = \min(m, n)$. □

Anwendung:

Korollar 2.54 (Klassifikation endlicher abelscher Gruppen)**.** *Jede endliche abelsche Gruppe ist bis auf Isomorphie von der Form*

$$\mathbb{Z}/(a_1) \oplus \cdots \oplus \mathbb{Z}/(a_n)$$

mit $a_i \in \mathbb{Z} \setminus \{0\}$, $a_1 \mid \cdots \mid a_n$.

Beweis. Fasse die Gruppe als $\mathbb{Z}$-Modul auf und wende 2.45 an. Beachte, dass der Rang 0 sein muss, ansonsten gäbe es unendlich viele Elemente. □

Beispiel. Wieviele abelsche Gruppenstrukturen bis auf Isomorphie gibt es auf einer Menge mit 36 Elementen? Das Produkt der invarianten Faktoren einer solchen Gruppe muss $36 = 2 \cdot 2 \cdot 3 \cdot 3$ ergeben. Ausprobieren aller möglichen invarianten Faktoren liefert folgende vollständige Liste:

invariante Faktoren	Elementarteiler
$\mathbb{Z}/(4) \oplus \mathbb{Z}/(9)$	$= \mathbb{Z}/(36)$,
$\mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(9)$	$= \mathbb{Z}/(2) \oplus \mathbb{Z}/(18)$,
$\mathbb{Z}/(4) \oplus \mathbb{Z}/(3) \oplus \mathbb{Z}(3)$	$= \mathbb{Z}/(3) \oplus \mathbb{Z}(12)$,
$\mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(3) \oplus \mathbb{Z}/(3)$	$= \mathbb{Z}/(6) \oplus \mathbb{Z}/(6)$.

3 Normalformen von Endomorphismen

3.1 k-Endomorphismen und $k[t]$-Torsionsmoduln

Sei k ein Körper. Wir betrachten als Objekte Paare (V, α) mit V ein endlichdimensionaler k-Vektorraum und $\alpha \in \operatorname{End}_k(V)$. Für zwei solche Paare (V, α), (W, β) definieren wir die Menge der Morphismen

$$\operatorname{Hom}((V, \alpha), (W, \beta)) = \{f \in \operatorname{Hom}_k(V, W) | \beta \circ f = f \circ \alpha\}.$$

Die Objekte und Morphismen bilden eine Kategorie (siehe LA I, Seite 28), die *Kategorie der Endomorphismen endlichdimensionaler k-Vektorräume*. Ziel ist es, die Objekte dieser Kategorie bis auf Isomorphie zu klassifizieren.

(Ein Isomorphismus ist ein Morphismus $f \in \mathrm{Hom}((V,\alpha),(W,\beta))$ mit einem Inversen $g \in \mathrm{Hom}((W,\beta),(V,\alpha))$, so dass

$$f \circ g = \mathrm{id}_W, g \circ f = \mathrm{id}_V.$$

Hier reicht es, dass f bijektiv ist; dann gilt für $g = f^{-1}$ automatisch

$$\alpha \circ g = g \circ f \circ \alpha \circ g = g \circ \beta \circ f \circ g = g \circ \beta.$$

)
Indem wir eine Basis $v = (v_1, \ldots, v_n)$ von V wählen, erhalten wir einen Isomorphismus $(k^n, M_v^v(\alpha)) \cong (V,\alpha)$. Andererseits sind (k^n, A) und (k^m, B) mit $A \in M_{n,n}(k)$, $B \in M_{m,m}(k)$ genau dann isomorph, wenn $n = m$ und es ein $C \in \mathrm{Gl}_n(k)$ gibt, so dass $CA = BC$ gilt. Letzteres bedeutet, dass A und B zueinander ähnlich sind. Damit ist unser Problem äquivalent dazu, $n \times n$-Matrizen bis auf Ähnlichkeit zu klassifizieren.
Wir führen unser Problem noch auf eine weitere äquivalente Formulierung zurück.

Definition 3.1. Sei V ein n-dimensionaler k-Vektorraum und $\alpha \in \mathrm{End}_k(V)$. Wir definieren wie folgt einen $k[t]$-Modul V_α:
Als k-Vektorraum ist V_α mit V identisch.
Für $f \in k[t]$, $v \in V$ setzen wir

$$f \cdot v = f(\alpha)(v).$$

Folgendes Lemma ist aus der 1. Klausur LA I bekannt:

Lemma 3.2. *Sei $a \in k[t]$ mit $a \neq 0$. Dann ist $k[t]/(a)$ ein k-Vektorraum der Dimension $d = \dim_k k[t]/(a) = \deg(a) < \infty$. Gilt $d > 0$, so ist das System der Restklassen $(1 + (a), t + (a), \ldots, t^{d-1} + (a))$ eine k-Vektorraum-Basis.*

Beweis. Falls $d = \deg(a) = 0$, so gilt $a \in k^\times = k[t]^\times$, $k[t]/(a) = 0$ mit der Dimension $\dim_k k[t]/(a) = 0 = d$. Ansonsten setze $x_i = t^i + (a) \in k[t]/(a)$.
k-lineare Unabhängigkeit: Seien $\alpha_i \in k$ mit

$$\sum_{i=0}^{d-1} \alpha_i x_i = 0.$$

Dann gilt

$$b = \sum_{i=0}^{d-1} \alpha_i t^i \in (a).$$

und somit $a \mid b$. Wegen $\deg(b) < \deg(a)$ geht das nur, wenn $b = 0$, also $\alpha_i = 0$ für alle i.
Erzeugendensystem über k: Sei $f + (a) \in k[t]/(a)$ mit $f = \sum_i \alpha_i t^i \in k[t]$. Da $k[t]$

euklidisch mit Normfunktion deg ist, gibt es $u, r = \sum_{i=0}^{d-1} \beta_i t^i \in k[t]$ mit $f = ua + r$ und es gilt

$$f + (a) = r + (a) = \sum_{i=0}^{d-1} \beta_i x_i.$$

□

Satz 3.3.

(i) Für jedes Paar (V, α) mit V endlichdimensionaler k-Vektorraum und $\alpha \in \mathrm{End}_k(V)$ ist V_α ein endlich erzeugter $k[t]$-Torsionsmodul.

(ii) Sind (V, α) und (W, β) zwei Paare wie in (i) so gilt

$$\mathrm{Hom}_{k[t]}(V_\alpha, W_\beta) = \{\phi \in \mathrm{Hom}_k(V, W) | \phi \circ \alpha = \beta \circ \phi\} = \mathrm{Hom}((V, \alpha), (W, \beta))$$

als k-Unterräume von $\mathrm{Hom}_k(V, W)$.

(iii) Ist M ein endlich erzeugter $k[t]$-Torsionsmodul so ist M ein endlichdimensionaler k-Vektorraum und Multiplikation mit t definiert einen Endomorphismus $\mu_t \in \mathrm{End}_k(M)$, sodass $M_{\mu_t} = M$.

Bemerkung. Man sagt: Die Kategorie der Endomorphismen von endlichdimensionalen k-Vektorräumen ist äquivalent zu der Kategorie der endlich erzeugten $k[t]$-Torsionsmoduln. Insbesondere gilt: Die Paare (V, α) und (W, β) sind genau dann isomorph, wenn die $k[t]$-Torsionsmoduln V_α und W_β isomorph sind.

Beweis.
Zu (i): Für $V = 0$ ist die Aussage offensichtlich richtig. Sei also $V \neq 0$. Dann ist V_α schon als k-Vektorraum endlich erzeugt. Nach Definition wirkt $f \in k[t]$ auf V_α wie $f(\alpha)$. Nach dem Satz von Cayley-Hamilton (LA I, 6.45) gilt

$$\chi_\alpha(\alpha) = 0$$

für das charakteristische Polynom χ_α von α. Der Grad von χ_α ist $\dim_k V$, insbesondere $\chi_\alpha \neq 0$ und somit ist jedes Element von V_α ein Torsionselement.
Zu (ii): Jedes $\phi \in \mathrm{Hom}_{k[t]}(V_\alpha, V_\beta)$ ist auch k-linear. Ferner gilt für $v \in V$:

$$\phi(\alpha(v)) = \phi(t \cdot v) = t \cdot \phi(v) = \beta(\phi(v)).$$

Andersrum folgt für $\phi \in \mathrm{Hom}_k(V, W)$ mit $\phi \circ \alpha = \beta \circ \phi$, $f = \sum_n a_n t^n \in k[t]$ und $v \in V$:

$$\phi(f \cdot v) = \sum_n a_n \phi(\alpha^n(v)) = \sum_n a_n \beta^n(\phi(v)) = f \cdot \phi(v).$$

Zu (iii): Als $k[t]$-Modul und damit auch als k-Vektorraum ist M isomorph zu einer endlichen direkten Summe von $k[t]$-Moduln der Form $k[t]/(a)$ (Korollar 2.52). Da

$k[t]/(a)$ als k-Vektorraum endlichdimensional ist (Lemma 3.2), gilt dies auch für M. Klar ist

$$\mu_t \colon M \to M, \qquad m \mapsto tm.$$

ein k-linearer Endomorphismus und für $f \in k[t]$, $m \in M$ gilt $f(\mu_t)(m) = f(t)m$, also stimmt M mit M_{μ_t} überein. □

Definition 3.4. Sei V ein k-Vektorraum der Dimension d und $\alpha \in \mathrm{End}_k(V)$.

(i) Ein Untervektorraum $W \subset V$ heißt α-invariant, falls $\alpha(w) \in W$ für alle $w \in W$.

(ii) V heißt α-zyklisch, falls es ein $v \in V$ gibt, so dass

$$(v, \alpha(v), \ldots, \alpha^{d-1}(v))$$

eine Basis von V ist.

Korollar 3.5. *Sei V ein k-Vektorraum der Dimension d und $\alpha \in \mathrm{End}_k(V)$.*

(i) Die α-invarianten Unterräume von V entsprechen gerade den $k[t]$-Untermoduln von V_α.

(ii) V ist genau dann α-zyklisch, wenn $V_\alpha \cong k[t]/(g)$ mit $0 \neq g \in k[t]$ (vom Grad d).

(iii) V zerfällt in eine direkte Summe $V = W_1 \oplus \cdots \oplus W_k$ von α-zyklischen, α-invarianten Unterräumen $W_i \subset V$.

Beweis.
(i): klar.
(ii): Sei V α-zyklisch mit Basis $(v, \alpha(v), \ldots, \alpha^{d-1}(v))$. Dann gilt

$$\alpha^d(v) = \sum_{i=0}^{d-1} c_i \alpha^i(v)$$

für eindeutig bestimmte $c_i \in k$. Setze $g = \sum c_i t^i \in k[t]$. Dann liegt (g) im Kern der surjektiven (!) k-linearen Abbildung

$$k[t] \to V, \qquad f \mapsto f(\alpha)(v)$$

Wegen $d = \dim_k k[t]/(g) = \dim_k V$ und dem Homomorphiesatz folgt $k[t]/(g) \cong V$. Andersrum zeigt Lemma 3.2, dass $V \cong k[t]/(g)$ für $g \neq 0$ α-zyklisch ist.
(iii): Folgt sofort aus dem Struktursatz 2.45. □

Definition 3.6. Die Elementarteiler des $k[t]$-Moduls V_α nennen wir kurz die (charakteristischen) Elementarteiler von α.

Bemerkungen.

(i) In der Literatur gibt es keinen feststehenden Begriff für die charakteristischen Elementarteiler.

(ii) Die charakteristischen Elementarteiler von $k^n \xrightarrow{A\cdot} k^n$ sollten nicht mit den Elementarteilern der Matrix A über dem Körper (und damit Hauptidealring) k verwechselt werden. Diese sind (nach Normierung) entweder 0 oder 1 (vgl. Satz 2.28) und deshalb nicht so interessant.

(iii) In $k[t]$ ist jedes Hauptideal $\neq (0)$ von der Form (f) mit f normiert. Wir wählen die charakteristischen Elementarteiler immer als normierte Polynome.

3.2 Die charakteristische Matrix

Sei ab jetzt V ein k-Vektorraum der Dimension n und $\alpha \in \mathrm{End}_k(V)$. Nach Wahl einer Basis $x = (x_1, \ldots, x_n)$ von V können wir α durch eine Matrix $A = M_x^x(\alpha) \in M_{n,n}(k)$ darstellen.

Definition 3.7. $tE_n - A \in M_{n,n}(k[t])$ heißt die *charakteristische Matrix* von A.

Bemerkung. Insbesondere gilt

$$\chi_\alpha(t) = \det(tE_n - A) \in k[t].$$

Wir betrachten nun die Abbildung

$$\pi_x \colon k[t]^n \to V_\alpha, \qquad \pi_x(e_i) = x_i$$

Satz 3.8. *Die Folge*

$$0 \longrightarrow k[t]^n \xrightarrow{tE_n - A} k[t]^n \xrightarrow{\pi_x} V_\alpha \longrightarrow 0$$

ist exakt, d. h. Linksmultiplikation mit $tE_n - A$ ist injektiv, π_x ist surjektiv und

$$\mathrm{im}(tE_n - A) = ker(\pi_x)$$

Insbesondere gilt $\mathrm{coker}(tE_n - A) \cong V_\alpha$, *d. h.* $k[t]^n \xrightarrow{tE_n - A} k[t]^n$ *ist eine endliche Präsentation von* V_α.

Beweis. Da x eine Basis des k-Vektorraums V ist, ist x auch ein Erzeugendensystem des $k[t]$-Moduls V_α und π_x ist surjektiv.
Es gilt $\pi_x \circ (tE_n - A) = 0$ weil

$$\pi_x((tE_n - A)e_i) = \alpha \circ \pi(e_i) - \sum_j a_{ji}\pi(e_j) = \alpha(x_i) - \alpha(x_i) = 0.$$

Also gilt $\mathrm{im}(tE_n - A) \subset \ker(\pi_x)$. Um Gleichheit zu zeigen, müssen wir zeigen, dass die induzierte Abbildung

$$\overline{\pi}\colon k[t]^n/\mathrm{im}(tE_n - A) \longrightarrow V_\alpha$$

ein Isomorphismus ist. $\overline{\pi}$ ist surjektiv und $\dim_k V_\alpha = n$. Damit genügt es zu zeigen: $k[t]^n/\mathrm{im}(tE_n - A)$ ist als k-Vektorraum von dem System $(e_1 + \mathrm{im}(tE_n - A), \ldots, e_n + \mathrm{im}(tE_n - A))$ erzeugt.

Für $f \in k[t]^n$ gilt $te_i = Ae_i - (tE_n - A)e_i$, also

$$te_i + \mathrm{im}(tE_n - A) = Ae_i + \mathrm{im}(tE_n - A).$$

Induktiv folgt $t^j e_i + \mathrm{im}(tE_n - A) = A^j e_i + \mathrm{im}(tE_n - A)$. Da das System

$$(t^j e_i)_{j\in\mathbb{N}_0, i\in\{1,\ldots,n\}}$$

eine k-Vektorraum-Basis von $k[t]^n$ ist und $A^i e_j$ als k-Linearkombination von $e_1, \ldots, e_n$ darstellbar ist, folgt, dass jedes Element von $k[t]/\mathrm{im}(tE_n - A)$ als k-Linearkombination der $e_1 + \mathrm{im}(tE_n - A), \ldots, e_n + \mathrm{im}(tE_n - A)$ darstellbar ist, was zu zeigen war.

Es bleibt zu zeigen, dass $k[t]^n \xrightarrow{tE_n - A} k[t]^n$ injektiv ist. Das kommutative Diagramm

$$\begin{array}{ccc} k[t]^n & \xrightarrow{tE_n - A} & k[t]^n \\ \downarrow & & \downarrow \\ k(t)^n & \xrightarrow{tE_n - A} & k(t)^n, \end{array}$$

wobei die nach unten zeigenden Pfeile die kanonischen Inklusionen sind, zeigt, dass es reicht, die Injektivität der unteren Abbildung zu zeigen. Nun gilt

$$\mathrm{Rg}_{k(t)}(tE_n - A) = n - r(\mathrm{coker}(tE_n - A))$$

nach 2.47. Da $\mathrm{coker}(tE_n - A) \cong V_\alpha$ ein $k[t]$-Torsionsmodul ist, folgt $r(tE_n - A) = 0$. Die Matrix $tE_n - A$ hat also vollen Rang und ist somit sogar invertierbar in $M_{n,n}(k(t))$. □

Korollar 3.9. *Die charakteristischen Elementarteiler von α sind gleich den Elementarteilern von $tE_n - A$ von positiven Grad.*

Beweis. Die Elementarteiler von $\mathrm{coker}(tE_n - A) \cong V_\alpha$ sind gerade die Elementarteiler von $tE_n - A$, die weder Einheiten in $k[t]$ noch gleich 0 sind (siehe Beweis des Strukturatzes). Letzteres kommt gar nicht vor, weil Multiplikation mit $tE_n - A$ injektiv ist. Die Einheiten in $k[t]$ haben alle Grad 0. □

Korollar 3.10 (Charakterisierung ähnlicher Matrizen)**.** *Sei k ein Körper, $A, B \in M_{n,n}(k)$. Dann sind äquivalent:*

(i) $A \approx B$

(ii) *Die $k[t]$-Torsionsmoduln $(k^n)_A$ und $(k^n)_B$ sind isomorph*

(iii) $(tE_n - A) \sim (tE_n - B)$

(iv) *A und B haben die gleichen charakteristischen Elementarteiler.*

Beweis.
$(i) \Leftrightarrow (ii)$: Nach Satz 3.3 sind die $k[t]$-Isomorphismen $(k^n)_A \to (k_n)_B$ gerade die k-Automorphismen α von k^n mit $\alpha(Av) = B\alpha(v)$ für alle $v \in k^n$. Die Darstellungsmatrix C von α bezüglich der Standardbasis erfüllt dann $CA = BC$ und $C \in \mathrm{Gl}_n(k)$. Andersrum beschreibt jede solche Matrix einen $k[t]$-Isomorphismus $(k^n)_A \to (k_n)_B$.
$(ii) \Leftrightarrow (iii) \Leftrightarrow (iv)$: 2.44 □

Lemma 3.11. *$\chi_\alpha(t)$ ist das Produkt der charakteristischen Elementarteiler von α.*

Beweis.

$$\begin{aligned}\chi_\alpha(t) &= \det(tE_n - A)\\ &\overset{2.39}{=} \text{Produkt der Elementarteiler von } tE_n - A\\ &= \text{Produkt der charakteristischen Elementarteiler von } \alpha.\end{aligned}$$

Beachte, dass wir die Elementarteiler als normierte Polynome wählen, d. h. Einheiten als Elementarteiler spielen in dem Produkt keine Rolle. □

Korollar 3.12. *Das Minimalpolynom von α ist gleich dem größten charakteristischen Elementarteiler von α.*

Beweis. Sei a_n der größte charakteristische Elementarteiler. Nach Definition des Minimalpolynoms und 2.51 gilt

$$\begin{aligned}(\chi_\alpha^{\min}) &= \{f \in k[t] | f(\alpha) = 0\}\\ &= \{f \in k[t] | fv = 0 \text{ für alle } v \in V_\alpha\}\\ &= \mathrm{Ann}_{k[t]} V_\alpha = (a_n).\end{aligned}$$

Da wir die Polynome $\chi_\alpha^{\min}$ und a_n als normiert annehmen, folgt $a_n = \chi_\alpha^{\min}$. □

Beispiele. Wir betrachten die Matrizen

$$A_1 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},\ A_2 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},\ A_3 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$tE - A_1 = \begin{pmatrix} t-1 & 0 & -1 \\ -1 & t-1 & 0 \\ 0 & 0 & t-1 \end{pmatrix}$$

Zyklische Vertauschung der Spalten.

$$\rightsquigarrow \begin{pmatrix} -1 & t-1 & 0 \\ 0 & -1 & t-1 \\ t-1 & 0 & 0 \end{pmatrix}$$

rechts ausräumen $\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & t-1 \\ t-1 & (t-1)^2 & 0 \end{pmatrix}$

unten ausräumen $\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & t-1 \\ 0 & (t-1)^2 & 0 \end{pmatrix}$

rechts ausräumen $\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & (t-1)^2 & (t-1)^3 \end{pmatrix} \overset{\text{unten ausr.}}{\rightsquigarrow} \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & (t-1)^3 \end{pmatrix}$

Also charakteristische Elementarteiler von A_1: $\chi_{A_1} = \chi_{A_1}^{\min} = (t-1)^3$.

Ebenso: Charakteristische Elementarteiler von A_2: $\chi_{A_2} = \chi_{A_2}^{\min} = (t-1)^3$
$A_1 \approx A_2$.
Charakteristische Elementarteiler von A_3: $(t-1), \chi_{A_3}^{\min} = (t-1)^2$.
Charakteristisches Polynom: $\chi_{A_3} = (t-1)^3$
$A_3 \not\approx A_1$.

Sei nun K ein Körper, der k umfaßt, $k \subset K$ (z.B. $k = \mathbb{R}$, $K = \mathbb{C}$).

Korollar 3.13. *Sei $A \in M_{n,n}(k)$. Die charakteristischen Elementarteiler von A aufgefasst als Element von $M_{n,n}(K)$ liegen schon in $k[t] \subset K[t]$ und sind genau die charakteristischen Elementarteiler von $A \in M_{n,n}(k)$.*

Beweis. Wende 2.40 auf die Inklusion von Hauptidealringen $k[t] \subset K[t]$ an. □

Korollar 3.14. *Das Minimalpolynom einer Matrix A über k bleibt dasselbe, wenn man A als Matrix über K auffasst.*

Beweis. $\chi^{\min}(A)$ ist der letzte charakteristische Elementarteiler. □

Korollar 3.15. *Seien $A, B \in M_{n,n}(k)$. Dann sind äquivalent:*

(i) $A \approx B$ *in* $M_{n,n}(k)$.

(ii) $A \approx B$ *in* $M_{n,n}(K)$.

Beweis. Klar nach 3.10 und 3.13. □

3.3 Frobenius- und Weierstraß-Normalformen

Sei k ein Körper, V ein endlich-dimensionaler k-Vektorraum und $\alpha \in \mathrm{End}_k(V)$. Unser Ziel ist es, eine Basis von V zu finden, bezüglich derer α eine möglichst einfache Darstellungsmatrix hat.
Ist $V = V_1 \oplus \cdots \oplus V_s$ eine Zerlegung in α-invariante Unterräume, und wählen wir für jedes V_i eine Basis $(v_{i,1}, \ldots, v_{i,r_i})$, $r_i = \dim_k V_i$, so wird α bezüglich $(v_{i,1}, \ldots, v_{i,r_i})$ durch die Matrix $A_i \in M_{r_i,r_i}(k)$ dargestellt und α bezüglich der Basis $(v_{1,1}, \ldots, v_{1,r_1}, \ldots, v_{s,1}, \ldots, v_{s,r_s})$ durch die Matrix

$$A = \left(\begin{array}{c|c|c|c} A_1 & & & \\ \hline & A_2 & & \\ \hline & & & \\ \hline & & & A_s \end{array}\right)$$

dargestellt. Wir nennen die A_i *Blöcke*.

Definition 3.16. Sei $g(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0$ ein normiertes Polynom vom Grad $n \geq 1$. Die Matrix

$$B_g = \begin{pmatrix} 0 & & & -a_0 \\ 1 & \ddots & & -a_1 \\ & \ddots & & \vdots \\ & & 0 & -a_{n-2} \\ & & 1 & -a_{n-1} \end{pmatrix}$$

heißt die *Begleitmatrix von* g. (Für $n = 1$ ist B_g die 1×1-Matrix $(-a_0)$.)

Bemerkung. Die Begleitmatrix B_g ist die Darstellungsmatrix des k-linearen Endomorphismus

$$k[t]/(g) \xrightarrow{t\cdot} k[t]/(g)$$

bezüglich der Basis $(1 + (g), t + (g), \ldots, t^{n-1} + (g))$.

Satz 3.17. *Sei $A \in M_{n,n}(k)$ eine beliebige Matrix. Dann existieren normierte Polynome $g_1 \mid \cdots \mid g_r \in k[t]$ vom Grad ≥ 1, so dass*

$$A \approx \left(\begin{array}{c|c|c|c} B_{g_1} & & & \\ \hline & B_{g_2} & & \\ \hline & & & \\ \hline & & & B_{g_r} \end{array}\right)$$

Diese Darstellung ist eindeutig und heißt Frobenius-Normalform *von A. Die $g_1, \ldots, g_r$ sind die charakteristischen Elementarteiler von A.*

Beweis.
Existenz: Seien $g_1, \ldots, g_r$ die charakteristischen Elementarteiler der Matrix A. Bezeichne $(k^n)_A$ den Vektorraum k^n mit $k[t]$-Modulstruktur durch $f \cdot x = f(A) \cdot x$. Nach dem Struktursatz gilt

$$(k^n)_A \cong k[t]/(g_1) \oplus \cdots \oplus k[t]/(g_r).$$

Bezüglich der wie oben gewählten Basen von $k[t]/(g_i)$, $i = 1, \ldots, r$, hat A daher die gewünschte Form.
Eindeutigkeit: Sei

$$A \approx \left(\begin{array}{c|c|c} B_{g_1} & & \\ \hline & & \\ \hline & & B_{g_r} \end{array}\right)$$

mit Begleitmatrizen B_{g_i}, $g_1|g_2|\ldots|g_r$. Der $k[t]$-Modul $(k^n)_A$ ist dann isomorph zu

$$k[t]/(g_1) \oplus \cdots \oplus k[t]/(g_r).$$

Wegen der Eindeutigkeit im Struktursatz sind $g_1, \ldots, g_r$ die charakteristischen Elementarteiler von A. □

Bemerkung. Da sich die Elementarteiler beim Übergang zu einem größeren Körper nicht ändern, gilt das gleiche auch für die Frobenius-Normalform.

Beispiel. Wir erinnern uns an

$$A_1 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} A_2 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} A_3 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$A_1 \approx A_2$ haben die Frobenius-Normalform $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -3 \\ 0 & 1 & 3 \end{pmatrix}$

(die charakteristischen Elementarteiler sind $(t-1)^3 = t^3 - 3t^2 + 3t - 1$).
A_3 hat die charakteristischen Elementarteiler $(t-1), (t-1)^2 = t^2 - 2t + 1$ und die Normalform

$$\left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & 0 & -1 \\ 0 & 1 & 2 \end{array}\right)$$

Satz 3.18. *Sei $A \in M_{n,n}(k)$. Dann existieren normierte Polynome $h_1, \ldots, h_r$, alle Potenzen von Primpolynomen, so dass*

$$A \approx \left(\begin{array}{c|c|c} B_{h_1} & & \\ \hline & & \\ \hline & & B_{h_r} \end{array}\right)$$

ist. Die Darstellung ist bis auf die Reihenfolge der h_i eindeutig und heißt Weierstraß-Normalform *von A.*

Beweis. Nach Folgerung 2.52 gilt

$$(k^n)_A \cong \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{m_i} k[t]/(p_i^{v_{ij}}).$$

Sind nun $h_1, \ldots, h_r$ die in der obigen Zerlegung auftauchenden Primpolynompotenzen so erhält man die Basis bezüglich derer A die gewünschte Form hat wie im letzten Beweis. Ist nun $A \approx \begin{pmatrix} B_{h_1} & & \\ & \ddots & \\ & & B_{h_r} \end{pmatrix}$, so gilt

$$(k^n)_A \cong k[t]/(h_1) \oplus \cdots \oplus k[t]/(h_r),$$

und die Eindeutigkeitsaussage in 2.52 sagt uns, dass die einzige Freiheit in der Wahl der Reihenfolge der h_i liegt. □

Bemerkung. Ein Primpolynom $p \in k[t]$ braucht in $K[t]$ ($K \supset k$ ein Oberkörper) nicht prim zu bleiben (Bsp.: $k = \mathbb{R}$, $K = \mathbb{C}$, $p = x^2 + 1$). Daher bleibt die Weierstraß-Normalform beim Übergang zu einem größeren Körper nicht notwendig erhalten. Die Blöcke sind aber im Vergleich zur Frobenius-Normalform in der Regel kleiner.

Beispiel. Wir betrachten die reelle Matrix $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

Charakteristische Elementarteiler: $t^2 + 1$

$$\begin{pmatrix} t & 1 \\ -1 & t \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & t \\ t & -1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & t \\ 0 & -1-t^2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 0 & -1-t^2 \end{pmatrix}$$

Also ist A schon in Frobenius-Normalform und weil $t^2 + 1$ über $\mathbb{R}$ irreduzibel ist, ist dies auch die reelle Weierstraß-Normalform. Über $\mathbb{C}$ zerfällt $t^2+1 = (t+i)(t-i)$ und die Weierstraß-Normalform von A über $\mathbb{C}$ ist $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$.

3.4 Die Jordan-Normalform

Voraussetzung in diesem Abschnitt: $A \in M_{n,n}(k)$ und χ_A zerfällt in lineare Polynome (z.B. immer, wenn $k = \mathbb{C}$). In dieser Situation kann man jede Matrix in eine besonders einfache Form bringen.

Definition 3.19. Sei $\lambda \in k$. Ein *Jordan-Kästchen zu λ der Breite n* ist eine untere $n \times n$-Dreieckmatrix mit

(i) Auf der Diagonale steht überall λ.

(ii) auf der ersten unteren Nebendiagonale stehen Einsen.

(iii) auf den anderen unteren Nebendiagonalen stehen Nullen.

Beispiel. (λ), $\begin{pmatrix} \lambda & 0 & 0 & 0 \\ 1 & \lambda & 0 & 0 \\ 0 & 1 & \lambda & 0 \\ 0 & 0 & 1 & \lambda \end{pmatrix}$ sind Jordankästchen (der Breiten 1 bzw. 4).

Bemerkung. Bei manchen Autoren ist ein Jordankästchen eine *obere* Dreiecksmatrix, wobei die Einsen nicht auf der ersten unteren, sondern auf der ersten oberen Nebendiagonale stehen. Das macht für die Theorie keinen Unterschied.

Satz 3.20 (Jordan-Normalform)**.** *Unter den Voraussetzungen dieses Abschnitts ist A ähnlich zu einer Matrix der Form*

$$\left(\begin{array}{c|c|c|c|c} J_1 & & & & \\ \hline & J_2 & & & \\ \hline & & & & \\ \hline & & & & \\ \hline & & & & J_r \end{array}\right)$$

wobei die J_i's Jordan-Kästchen sind. Die Darstellung ist bis auf die Reihenfolge der Jordan-Kästchen eindeutig.

Beweis. Wir betrachten den $k[t]$-Modul $(k^n)_A$. Dieser zerfällt in die direkte Summe von Moduln der Form $k[t]/(p^i)$, wobei $p \in k[t]$ prim und normiert ist. Da χ_A in das Produkt von linearen Polynomen zerfällt gilt $p(t) = t - \lambda$ für ein $\lambda \in k$, λ Eigenwert von A. Nun betrachten wir als k-Vektorraum-Basis die Bilder von $1, t-\lambda, \ldots, (t-\lambda)^{i-1}$ in $k[t]/(t-\lambda)^i$. Es gilt $t \cdot (t-\lambda)^j = (t-\lambda)^{j+1} + \lambda(t-\lambda)^j$ für $j = 0, \ldots, i-2$ und

$$\begin{aligned} t \cdot (t-\lambda)^{i-1} &= (t-\lambda)^i + \lambda(t-\lambda)^{i-1} \\ &= \lambda(t-\lambda)^{i-1}. \end{aligned}$$

Also hat A auf diesem direkten Summanden und bezüglich dieser Basis die gewünschte Matrixdarstellung. Die direkte Summe gibt Blockform für A. □

Beispiel. Wir betrachten die Matrix

$$A = \begin{pmatrix} 2 & 0 & -1 \\ 1 & 2 & 1 \\ 0 & 0 & 3 \end{pmatrix}$$

mit dem einzigen Elementarteiler

$$\chi_A(t) = \chi_A^{\min}(t) = (t-2)^2(t-3) = (t^2 - 4t + 4)(t-3) = t^3 - 7t^2 + 16t - 12$$

Also

Frobenius-Normalform: $\begin{pmatrix} 0 & 0 & 12 \\ 1 & 0 & -16 \\ 0 & 1 & 7 \end{pmatrix}$

Weierstraß-Normalform: $\left(\begin{array}{cc|c} 0 & -4 & 0 \\ 1 & 4 & 0 \\ \hline 0 & 0 & 3 \end{array}\right)$

Jordan-Normalform: $\begin{pmatrix} 2 & 0 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}$

3.5 Verallgemeinerte Eigenräume

Voraussetzung in diesem Abschnitt: V ein endlichdimensionaler k-Vektorraum, $\alpha \in \mathrm{End}_k V$ ein Endomorphismus, so dass χ_α in lineare Polynome zerfällt (z.B. immer, wenn $k = \mathbb{C}$).

Ziel: Algorithmus zur effizienten Berechnung der Jordan-Normalform von α und einer Basis von V, bezüglich der α Jordan-Normalform annimmt.

Erinnerung: Ist λ Eigenwert von α, so ist der Eigenraum zu λ definiert als

$$V(\lambda) = \ker(\lambda \mathrm{id}_V - \alpha) \neq 0$$

Definition 3.21. Der Raum $V^{(i)}(\lambda) = \ker((\lambda \mathrm{id} - \alpha)^i)$ heißt *der i-te verallgemeinerte Eigenraum* zu λ.

Bemerkungen.

(i) $V^1(\lambda)$ ist der gewöhnliche Eigenraum. Wir setzen $V^0(\lambda) = 0$.

(ii) Ist $V^1(\lambda) = 0$, also λ kein Eigenwert, so ist $\lambda \mathrm{id}_V - \alpha$ invertierbar. Somit ist für jedes i auch $(\lambda \mathrm{id}_V - \alpha)^i$ invertierbar, d.h. $V^i(\lambda) = 0$ für alle $i \in \mathbb{N}$.

(iii) Da V endlich-dimensional ist, wird die Kette von Unterräumen $V^{(1)}(\lambda) \subseteq V^{(2)}(\lambda) \subseteq \dots$ stationär.

(iv) $V^{(i)}(\lambda)$ ist ein α-invarianter Unterraum von V: Gilt $(\lambda \mathrm{id}_V - \alpha)^i(x) = 0$, so auch

$$(\lambda \mathrm{id}_V - \alpha)^i(\alpha(x)) = \alpha((\lambda \mathrm{id}_V - \alpha)^i)(x) = 0.$$

Lemma 3.22.

(i) Gilt $V^i(\lambda) = V^{i+1}(\lambda)$ für ein $i \in \mathbb{N}$, so folgt

$$V^i(\lambda) = V^{i+1}(\lambda) = V^{i+2}(\lambda) = \cdots .$$

(ii) *Sei $i \in \mathbb{N}$. Das Urbild von $V^{i-1}(\lambda)$ unter $\lambda\mathrm{id}_V - \alpha$ ist $V^i(\lambda)$. Insbesondere gilt*

$$(\lambda\mathrm{id}_V - \alpha)(V^i(\lambda)) = V^{i-1}(\lambda).$$

(iii) *Ist $W \subset V$ ein Unterraum mit $W \cap V^i(\lambda) = 0$ für ein $i \in \mathbb{N}$, so ist*

$$(\lambda\mathrm{id}_V - \alpha)|_W \colon W \to V$$

injektiv.

Beweis. Setze $\beta = (\alpha - \lambda\mathrm{id}_V)$.
Zu (i): Nach Voraussetzung gilt $\ker(\beta^i) = \ker(\beta^{i+1})$. Für $v \in V^{(i+2)}(\lambda) = \ker(\beta^{i+2})$ folgt $\beta^{i+1}(\beta(v)) = 0$, also $\beta(v) \in \ker(\beta^{i+1}) = \ker(\beta^i)$. Es folgt $\beta^{i+1}(v) = \beta^i(\beta(v)) = 0$, also $v \in V^{(i+1)}(\lambda)$. Nun schließt man per Induktion über i.
Zu (ii): Sei $\beta(v) \in V^{i-1}(\lambda) = \ker(\beta^{i-1})$. Dann gilt $\beta^i(v) = 0$, also $v \in \ker(\beta^i) = V^i(\lambda)$.
Zu (iii): Für $0 \neq w \in W$ gilt $\beta^i(w) \neq 0$, also auch $\beta(w) \neq 0$. □

Definition 3.23.

$$V_{\text{allg.}}(\lambda) = \bigcup_{i=1}^{\infty} V^{(i)}(\lambda) = \{v \in V | \exists i \colon (\lambda\mathrm{id}_V - \alpha)^i(v) = 0\}$$

heißt *der verallgemeinerte Eigenraum* zu λ.

Wähle nun einen $k[t]$-Isomorphismus

$$\phi \colon V_\alpha \xrightarrow{\cong} \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{m_i} k[t]/(t-\lambda_i)^{v_{ij}} = X$$

mit $v_{i1} \leq v_{i2} \leq \cdots \leq v_{im_i}$ und paarweise verschiedenen $\lambda_i \in k$ (Zerlegung in invariante Faktoren, siehe 2.52). Es gilt

$$\chi_\alpha(t) = \prod_{i=1}^{n} \prod_{j=1}^{m_i} (t-\lambda_i)^{v_{ij}}.$$

(siehe 3.11). Insbesondere sind die λ_i gerade die Nullstellen des charakteristischen Polynoms und somit die Eigenwerte von α (LA I, Satz 6.44).

Lemma 3.24. *Unter dem Isomorphismus ϕ identifiziert sich $V_{\text{allg.}}(\lambda_\ell)$ mit dem Summanden*

$$\bigoplus_{j=1}^{m_\ell} k[t]/(t-\lambda_\ell)^{v_{\ell j}} \subset X$$

und $V^{(s)}(\lambda_\ell)$ mit dessen Untermodul

$$\bigoplus_{j=1}^{m_\ell} (t-\lambda_\ell)^{\max(v_{\ell j}-s,0)} k[t]/(t-\lambda_\ell)^{v_{\ell j}}.$$

Beweis. Für $v \in V$ gilt

$$\phi((\lambda_\ell \mathrm{id}_V - \alpha)(v)) = \phi((\lambda_\ell - t)v) = (\lambda_\ell - t)\phi(v).$$

Also identifiziert sich $V^{(s)}(\lambda_\ell)$ mit $X^{(s)}(\lambda_\ell) = \ker(X \xrightarrow{(\lambda_\ell - t)^s \cdot} X)$. Sei nun

$$x = (x_{ij} + ((t-\lambda_i)^{v_{ij}})) \in X$$

Dann gilt $x \in X^{(s)}(\lambda_\ell)$ genau dann, wenn $(t-\lambda_i)^{v_{ij}} | (t-\lambda_\ell)^s x_{ij}$ für alle i und j. Für $i \neq \ell$ bedeutet dies, dass $x_{ij} \in ((t-\lambda_i)^{v_{ij}})$, für $i = \ell$, dass $(t-\lambda_\ell)^{\max(v_{ij}-s,0)} | x_{ij}$. Damit gilt

$$X^{(s)}(\lambda_\ell) = \bigoplus_{j=1}^{m_\ell} (t-\lambda_\ell)^{\max(v_{\ell j}-s,0)} k[t]/(t-\lambda_\ell)^{v_{\ell j}}.$$

Wähle nun $s \geq v_{\ell m_\ell}$. Dann gilt

$$\bigoplus_{j=1}^{m_\ell} k[t]/(t-\lambda_\ell)^{v_{\ell j}} \cong V^{(s)}(\lambda_\ell) = V_{\text{allg.}}(\lambda_\ell).$$

□

Korollar 3.25.

$$V = \bigoplus_{\lambda \text{ EW}} V_{allg}(\lambda)$$

Beweis. Folgt sofort aus dem Lemma und der Struktur von X. □

Korollar 3.26. *Seien $J_1, \ldots, J_r$ die Jordan-Kästchen zum Eigenwert λ in der Jordan-Normalform von α und n_i die Breite von J_i. Dann gilt*

$$\dim V^{(i)}(\lambda) = \sum_{j=1}^{r} \min(i, n_j).$$

Insbesondere gilt

$$\dim V_{allg}(\lambda) = \sum_{j=1}^{r} n_j.$$

Beweis. Jedes der Jordankästchen J_j entspricht einem Summanden $k[t]/(t-\lambda)^{n_j}$ von X mit den Bildern von $1, (t-\lambda), \ldots, (t-\lambda)^{n_j-1}$ als K-Basis. Der Untermodul $(t-\lambda)^{\max(n_j-i,0)} k[t]/(t-\lambda)^{n_j}$ hat dann die Bilder von $(t-\lambda)^{\max(n_j-i,0)}, \ldots, (t-\lambda)^{n_j-1}$ als K-Basis und damit die Dimension

$$n_j - \max(n_j - i, 0) = \min(i, n_j).$$

über K. □

Gegeben: $V = k^n$ und ein Endomorphismus $\alpha \in \mathrm{End}_k(V)$, der bezüglich der Standardbasis die Darstellungsmatrix A hat.

Gesucht: Eine Jordan-Normalform J von α und eine Basis von V, so dass J die Darstellungsmatrix von α bezüglich dieser Basis hat, d. h. eine Matrix $C \in \mathrm{Gl}_n(k)$ mit $C^{-1}AC = J$. (Die gesuchte Basis ist dann durch die Spalten von C gegeben.)

Algorithmus:

1. Berechne die Eigenwerte von A, d. h. die Nullstellen des charakteristischen Polynoms
$$\chi_A(t) = (t - \lambda_1)^{e_1} \cdots (t - \lambda_r)^{e_r}$$
mit λ_i paarweise verschieden.

2. Wegen der Zerlegung $V = \bigoplus V_{\text{allg.}}(\lambda_i)$ in α-invariante Unterräume reicht es, für jeden Eigenwert λ von α eine geeignete Basis von $V_{\text{allg.}}(\lambda)$ zu bestimmen. Wir bestimmen dazu zunächst beliebige Basen $v^{(j)} = (v_1^{(j)}, \ldots, v_{d_j}^{(j)})$ der $V_j = V^{(j)}(\lambda)$, $d_j = \dim_k V_j$ für $j = 1, 2, \ldots$, bis wir die kleinste Zahl k mit $d_k = d_{k+1}$ erreichen. (k ist auf jeden Fall kleiner gleich der Ordnung von λ als Nullstelle von $\chi_A(t)$). Es gilt dann $V_{\text{allg.}}(\lambda) = V_k$ nach 3.22. Konkret können wir mittels Gauß-Elimination die strengen Zeilenstufenformen D_j von $(\lambda E_n - A)^j$ bestimmen. Aus diesen kann man Basen v_j direkt ablesen (siehe LA I, §5.3). Etwas schneller geht es, wenn man ausnutzt, dass D_{j+1} gleich der strengen Zeilenstufenform von $D_j(\lambda E_n - A)$ ist (siehe LA I, Satz 5.4).

3. Setze $\beta = \alpha - \mathrm{id}_V\lambda$, $V_0 = V_{-1} = 0$. Wir konstruieren nun für
$$i = k, k-1, \ldots, 1$$
Unterräume $W_i \subset V_i$ und Systeme $(w_j^{(i)})_{j \in J_i}$ von Vektoren in V_i so dass

   (i) $\beta(W_i) \subset V_{i-1}$,

   (ii) $\beta(W_i) \cap V_{i-2} = 0$,

   (iii) $(\beta^{t-i}(w_j^{(t)}))_{t=i,\ldots,k;j\in J_t}$ ist eine Basis von W_i.

   (Schritt 1) Wähle eine Basis $\left(w_j^{(k)}\right)_{j\in J_k}$ eines zu V_{k-1} komplementären Unterraums W_k in V_k, z. B. durch Anwenden des Basisergänzungsverfahrens aus (LA I, 5.1) auf die Basen $v^{(k-1)}$ von $V^{(k-1)}$ und $v^{(k)}$ von V_k. Dann ist $\beta(W_k) \subset \beta(V_k) = V_{k-1}$ nach 3.22.(ii). Sei $v \in W_k$ Dann gilt
$$\beta(v) \in V_{k-2} \overset{3.22.(ii)}{\Longleftrightarrow} v \in V_{k-1} \Longleftrightarrow v = 0,$$
   also $\beta(W_k) \cap V_{k-2} = 0$. Also sind (i),(ii),(iii) erfüllt.

(Schritt $k-i$) Seien jetzt W_r und $(w_j^{(r)})_{j\in J_r}$ für $i+1 \le r \le k$ bereits konstruiert. Wähle eine Basis $(w_j^{(i)})_{j\in J_i}$ eines zu $\beta(W_{i+1}) \oplus V_{i-1}$ komplementären Unterraums in V_i und setze

$$W_i = \beta(W_{i+1}) + \operatorname{Lin}((w_j^{(i)})_{j\in J_i}.$$

Nach (ii) und 3.22.(iii) ist $\beta\colon W_{i+1} \to V_i$ injektiv, also ist nach (iii)

$$\left(\beta^{t-i}(w_j^{(t)})\right)_{t=i+1,\dots,k,j\in J_t} \text{ eine Basis von } \beta(W_{i+1})$$
$$\left(\beta^{t-i}(w_j^{(t)}\right)_{t=i,\dots,k,j\in J_t} \text{ eine Basis von } W_i.$$

Also gilt (iii) für W_i. Wie oben zeigt man, dass auch (i) und (ii) gilt.

4. Nach Konstruktion gilt

$$V_k = V_{k-1} \oplus W_k = V_{k-2} \oplus W_{k-1} \oplus W_k = \ldots = W_1 \oplus \ldots \oplus W_k$$

und $w_\lambda = \left(\beta^s(w_j^{(t)})\right)_{s=0,\dots,k-1;t=s+1,\dots,k;j\in J_t}$ (mit $s = t-i$) ist eine Basis von V_k. Es gilt

$$\alpha(\beta^s(w_j^{(t)})) = \begin{cases} \beta^{s+1}(w_j^{(t)}) + \lambda\beta^s(w_j^{(t)}) & \text{falls } s < t-1, \\ \lambda\beta^{t-1}(w_j^{(t)}) & \text{falls } s = t-1 \end{cases}$$

(beachte, dass $w_j^{(t)} \in V_t = \ker\beta^t$). Damit ist die Darstellungsmatrix von $\alpha|_{V_k}$ bezüglich w_λ in Jordan-Normalform.

5. Füge alle Basen w_λ der Räume $V_{\text{allg.}}(\lambda)$ zu einer Basis w von V zusammen und bilde die Matrix $C = M_e^w(\mathrm{id})$, in deren Spalten die Basisvektoren aus w stehen. Dann ist $C^{-1}AC$ die Jordan-Normalform von A.

Beispiel. Sei

$$A = \begin{pmatrix} 3 & -1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix}$$

1. Charakteristisches Polynom

$$\chi_A(t) = \det(tE-A) = ((t-3)(t-1)+1)(t-2) = (t^2-4t+4)(t-2) = (t-2)^3.$$

Eigenwert 2.

2. Setze

$$B = A - 2E = \begin{pmatrix} 1 & -1 & 1 \\ 1 & -1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

Strikte obere Zeilenstufenform:

$$D_1 = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad \Rightarrow \quad V_1 = \ker(B) = \operatorname{Lin}\left(\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix} \right)$$

Es gilt $D_1 B = 0$, was schon in strikter oberer Zeilenstufenform ist.

$$V_2 = \ker(B^2) = \ker(D_1 B) = \operatorname{Lin}\left(\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right)$$

3. Setze

$$w_1^{(2)} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad W_2 = \mathbb{R} w_1^{(2)} \quad \Longrightarrow \quad V_2 = V_1 \oplus W_2, \quad B w_1^{(2)} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}.$$

Setze

$$w_1^{(1)} = \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}, \quad W_1 = \mathbb{R} B w_1^{(2)} + \mathbb{R} w_1^{(1)} \quad \Longrightarrow V_1 = W_1.$$

4. Bilde die Matrix mit den Spalten $w_1^{(1)}, w_1^{(2)}, B w_1^{(2)}$:

$$C = \begin{pmatrix} -1 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

5. Entfällt, weil 2 der einzige Eigenwert ist.

Probe:

$$C^{-1} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & -1 & 1 \\ 0 & 1 & 0 \end{pmatrix} \qquad \text{(mittels Gauss-Algorithmus)}$$

$$C^{-1} A C = \begin{pmatrix} 0 & 0 & 2 \\ 2 & -2 & 2 \\ 1 & 1 & 1 \end{pmatrix} C = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 1 & 2 \end{pmatrix}$$

3.6 Die Jordan-Chevalley-Zerlegung

Sei V ein n-dimensionaler k-Vektorraum und $\alpha \in \operatorname{End}_k V$.

Definition 3.27. Der Endomorphismus α heißt

(i) *nilpotent*, wenn $\alpha^r = 0$ für ein $r \geq 1$ gilt,

(ii) *unipotent*, wenn $\alpha - \mathrm{id}_V$ nilpotent ist,

(iii) *potentiell unipotent*, wenn α^r für ein $r \geq 1$ unipotent ist,

(iv) *halbeinfach*, wenn

$$V_\alpha \cong \bigoplus_{i=1}^{r} k[t]/(p_i)$$

mit irreduziblen Polynomen p_i (d. h. V_α ist endliche direkte Summe einfacher $k[t]$-Moduln).

Entsprechend für Matrizen.

Beispiele. Eine obere Dreieckmatrix-Matrix

$$\begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

ist nilpotent, wenn $\lambda_i = 0$, unipotent, wenn $\lambda_i = 1$, potentiell unipotent, wenn λ_i Einheitswurzeln sind und halbeinfach, wenn sie eine Diagonalmatrix ist.

Lemma 3.28. *Seien $\alpha, \beta \in \mathrm{End}_k(V)$ mit $\alpha\beta = \beta\alpha$.*

(i) Sind α, β nilpotent so auch $\alpha + \beta$ und $\alpha\beta$.

(ii) Sind α, β (potentiell) unipotent, so auch $\alpha\beta$.

Beweis.
(i): Sei $\alpha^k = 0$, $\beta^\ell = 0$. Weil α und β kommutieren, gilt nach der binomischen Formel

$$(\alpha + \beta)^{k+\ell} = \sum_{r=0}^{k+\ell} \binom{k+\ell}{r} \alpha^r \beta^{k+\ell-r} = 0$$

da $r \geq k$ oder $k + \ell - r \geq \ell$. Ferner gilt $(\alpha\beta)^{k+\ell} = \alpha^{k+\ell}\beta^{k+\ell} = 0$.
(ii): Seien α, β unipotent. Dann ist

$$(\alpha\beta - \mathrm{id}) = (\alpha - \mathrm{id})(\beta - \mathrm{id}) + (\alpha - \mathrm{id}) + (\beta - \mathrm{id})$$

als Summe kommutierender nilpotenter Endomorphismen wieder nilpotent, also $\alpha\beta$ unipotent.
Seien nun erst α^k und β^ℓ unipotent. Dann ist auch $\alpha^{k\ell} = (\alpha^k)^\ell$ unipotent, ebenso $\beta^{k\ell}$ und $(\alpha\beta)^{k\ell}$, also $\alpha\beta$ potentiell unipotent. □

Lemma 3.29. *α ist nilpotent $\iff \chi_\alpha = t^n \iff \chi_\alpha^{\min} = t^r$ für ein $r > 0$.*

Beweis. χ_α und $\chi_\alpha^{\min}$ haben dieselben Primteiler. Ist $\chi_\alpha = t^n$, so folgt nach Cayley-Hamilton $\alpha^n = 0$. Ist andersrum $\alpha^s = 0$ für ein $s > 0$, so folgt $\chi^{\min} \mid t^s$. □

Satz 3.30. *Die folgenden Bedingungen sind äquivalent.*

(i) *α ist halbeinfach.*

(ii) *$\chi_\alpha^{\min}$ hat keine doppelten Primfaktoren.*

Ist k algebraisch abgeschlossen, so ist (i) zusätzlich äquivalent zu

(iii) *α ist diagonalisierbar.*

Beweis.
$(i) \Leftrightarrow (ii)$: Sei

$$V_\alpha \cong \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{m_i} k[t]/(p_i^{v_{ij}}), \qquad p_i \text{ prim und paarweise verschieden}$$

die Zerlegung in invariante Faktoren, siehe 2.52. Dann gilt

$$\chi_\alpha^{\min}(t) = \prod_{i=1}^{n} p_i^{\max(v_{i1},\ldots,v_{im_i})}.$$

Es gilt

$$\alpha \text{ halbeinfach} \quad \Leftrightarrow \quad \forall i,j\colon v_{ij} = 1 \quad \Leftrightarrow \quad \chi_\alpha^{\min} = \prod_{i=1}^{n} p_i.$$

$(ii) \Leftrightarrow (iii)$: Ist k algebraisch abgeschlossen, so sind alle irreduziblen Polynome linear und die Äquivalenz folgt aus LA I, 6.72. □

Korollar 3.31. *Sei $\alpha \in \mathrm{End}_k(V)$ halbeinfach und $W \subset V$ ein α-invarianter Untermodul. Dann ist auch $\alpha|_W$ halbeinfach.*

Beweis. Es gilt $\chi_\alpha^{\min}(\alpha|_W)(w) = \chi_\alpha^{\min}(\alpha)(w) = 0$ für alle $w \in W$. Also gilt $\chi_{\alpha|_W}^{\min} \mid \chi_\alpha^{\min}$. Somit kommt auch in $\chi_{\alpha|_W}^{\min}$ jeder Primfaktor nur einfach vor. □

Lemma 3.32. *Ist α sowohl halbeinfach, als auch nilpotent, so gilt $\alpha = 0$.*

Beweis. Da α nilpotent, gilt $\chi_\alpha^{\min}(t) = t^r$, da α halbeinfach, gilt $r = 1$, also $\alpha = 0$. □

Von jetzt an sei der Einfachheit halber k algebraisch abgeschlossen, z.B. $k = \mathbb{C}$.

Satz 3.33 (Simultane Diagonalisierbarkeit)**.** *Sind α und β halbeinfach und gilt $\alpha\beta = \beta\alpha$, so existiert eine Basis bezüglich derer α und β Diagonalgestalt haben.*

Beweis. Es gilt $V = \bigoplus_\lambda V(\lambda, \alpha)$, wobei λ die Eigenwerte von α durchläuft und $V(\lambda, \alpha)$ der Eigenraum bezüglich α zu λ ist. Nun gilt für $v \in V(\lambda, \alpha)$

$$\lambda\beta(v) = \beta(\lambda v) = \beta\alpha(v) = \alpha(\beta(v)),$$

also gilt $\beta(v) \in V(\lambda, \alpha)$, d. h. $V(\lambda, \alpha)$ ist β-invariant. Wegen 3.31 ist $\beta|_{V(\lambda,\alpha)}$ halbeinfach.
Nun wählen wir für jedes $V(\lambda, \alpha)$ eine Basis aus Eigenvektoren zu β und fügen die Basen zu einer Basis von V zusammen. Bzgl. dieser Basis haben α und β Diagonalform. □

Korollar 3.34. *Sind α, β halbeinfach und gilt $\alpha\beta = \beta\alpha$, so sind auch $\alpha + \beta$ und $\alpha\beta$ halbeinfach.*

Theorem 3.35 (additive Jordan-Chevalley-Zerlegung)**.** *Sei k algebraisch abgeschlossen. Zu jedem $\alpha \in \mathrm{End}_k V$ gibt es $\alpha_s, \alpha_n \in \mathrm{End}_k(V)$ mit α_s halbeinfach und α_n nilpotent so dass*

$$\alpha = \alpha_s + \alpha_n \quad \textit{und} \quad \alpha_s\alpha_n = \alpha_n\alpha_s.$$

Diese Zerlegung ist eindeutig. Ferner gibt es Polynome $p_s, p_n \in k[t]$ ohne konstanten Term mit

$$\alpha_s = p_s(\alpha), \qquad \alpha_n = p_n(\alpha).$$

Kommutiert $\beta \in \mathrm{End}_k(V)$ mit α, so auch mit α_s und α_n.

Beweis.
Existenz: Sei

$$\chi_\alpha^{\min}(t) = \prod_{i=1}^{r} (t - \lambda_i)^{m_i}, \qquad \lambda_i \text{ paarweise verschieden}$$

das Minimalpolynom von α und

$$\epsilon = \begin{cases} 0 & \text{falls } \lambda_i = 0 \text{ für ein } i, \\ 1 & \text{sonst.} \end{cases}$$

Nach dem chinesischen Restsatz 2.21 ist

$$k[t]/(t^\epsilon \chi_\alpha^{\min}(t)) \to k[t]/(t^\epsilon) \oplus k[t]/(t - \lambda_1)^{m_1} \oplus \ldots \oplus k[t]/(t - \lambda_r)^{m_r}$$

ein Isomorphismus. Es gibt also ein $p_s \in k[t]$ mit

$$p_s \equiv 0 \mod t^\epsilon, \qquad p_s \equiv \lambda_i \mod (t - \lambda_i)^{m_i}.$$

Setze $p_n(t) = t - p_s(t)$. Nach Konstruktion gilt $p_s(0) = p_n(0) = 0$ und $\alpha_s = p_s(\alpha), \alpha_n = p_n(\alpha)$ kommutieren mit α und allen β, die mit α kommutieren. Insbesondere $\alpha_s\alpha_n = \alpha_n\alpha_s$. Setze

$$f = (t - \lambda_1) \cdots (t - \lambda_r), \quad g = f(p_s(t))$$

Dann gilt

$$g \equiv f(\lambda_i) \equiv 0 \mod (t - \lambda_i)^{m_i},$$

nach dem chinesischen Restsatz angewandt auf $k[t]/(\chi_\alpha^{\min})$ also $g = a\chi_\alpha^{\min}$ für ein $a \in k[t]$. Insbesondere gilt

$$f(\alpha_s) = g(\alpha) = a(\alpha)\chi_\alpha^{\min}(\alpha) = 0$$

und somit $\chi_{\alpha_s}^{\min} \mid f$. Da in f jeder Primfaktor nur einfach vorkommt, gilt dies auch für $\chi_{\alpha_s}^{\min}$, d. h. α_s ist halbeinfach. Sei $m = \max(m_1, \ldots, m_r)$. Dann gilt

$$p_n(t)^m \equiv (t - \lambda_i)^m \equiv 0 \mod (t - \lambda_i)^{m_i}.$$

Also $p_n(t)^m \in (\chi_\alpha^{\min})$ und $\alpha_n^m = p_n(\alpha)^m = 0$, d. h. α_n ist nilpotent.
Eindeutigkeit: Sei $\alpha = \beta + \gamma$ eine andere Zerlegung mit β halbeinfach, γ nilpotent und $\beta\gamma = \gamma\beta$. Dann gilt

$$\alpha\beta = (\beta + \gamma)\beta = \beta(\beta + \gamma) = \beta\alpha,$$

also auch $\alpha_s\beta = \beta\alpha_s$. Damit ist $\alpha_s - \beta$ wieder halbeinfach. Analog gilt $\alpha_n\gamma = \gamma\alpha_n$, d. h. $\alpha_s - \beta = \gamma - \alpha_n$ ist halbeinfach und nilpotent, also gleich 0. □

Korollar 3.36. *Sei die Darstellungsmatrix J von α bezüglich der Basis v von V in Jordan-Normalform,*

$$J = \begin{pmatrix} \lambda_1 E_{j_1} + N_{j_1} & & & 0 \\ & \lambda_2 E_{j_2} + N_{j_2} & & \\ & & \ddots & \\ 0 & & & \lambda_r E_{j_r} + N_{j_r} \end{pmatrix},$$

$$N_j = \begin{pmatrix} 0 & & & 0 \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ 0 & & 1 & 0 \end{pmatrix} \in M_{j,j}(k)$$

mit λ_i nicht notwendig paarweise verschiedene Eigenwerte von α. Dann haben α_s und α_n die Darstellungsmatrizen

$$J_s = \begin{pmatrix} \lambda_1 E_{j_1} & & 0 \\ & \ddots & \\ 0 & & \lambda_r E_{j_r} \end{pmatrix}, \qquad J_n = \begin{pmatrix} N_{j_1} & & 0 \\ & \ddots & \\ 0 & & N_{j_r} \end{pmatrix}$$

Insbesondere hat α_s dieselben Eigenwerte wie α.

Beweis. J_s ist diagonal, J_n ist nilpotent und $J_sJ_n = J_nJ_s$. Aus der Eindeutigkeit der Jordan-Chevalley-Zerlegung folgt die Behauptung. □

Korollar 3.37 (multiplikative Jordan-Chevalley-Zerlegung)**.** *Sei k algebraisch abgeschlossen und $\alpha \in \mathrm{Aut}_k(V)$. Dann gibt es eine eindeutige Zerlegung $\alpha = \alpha_s\alpha_u$ mit $\alpha_s \in \mathrm{Aut}_k(V)$ halbeinfach, $\alpha_u \in \mathrm{Aut}_k(V)$ unipotent und $\alpha_s\alpha_u = \alpha_u\alpha_s$.*

Beweis. Schreibe $\alpha = \alpha_s + \alpha_n$. Da α_s dieselben Eigenwerte wie α hat und die Determinante das Produkt der Eigenwerte ist, folgt $\det\alpha_s = \det\alpha \neq 0$, d. h. $\alpha_s \in \mathrm{Aut}_k(V)$. Setze $\alpha_u = \mathrm{id}+\alpha_s^{-1}\alpha_n$. Da α_s und α_n kommutieren, gilt $(\alpha_s^{-1}\alpha_n)^k = \alpha_s^{-k}\alpha_n^k = 0$ für genügend großes k. Also ist α_u unipotent und somit invertierbar:

$$\alpha_u^{-1} = \sum_{i=0}^{k} \alpha_s^{-i}\alpha_n^i.$$

Ferner gilt $\alpha_s\alpha_u = \alpha_u\alpha_s = \alpha$. Ist $\alpha = \beta_s\beta_u$ eine zweite Zerlegung mit den obigen Eigenschaften, so ist $\beta_n = \beta_s(\beta_u - \mathrm{id})$ nilpotent und $\alpha = \beta_s + \beta_u$. Wegen der Eindeutigkeit der additiven Jordan-Chevalley-Zerlegung folgt $\alpha_s = \beta_s$ und $\alpha_u = \beta_u$. □

Bemerkungen.

1. Die Jordan-Chevalley-Zerlegung spielt eine wichtige Rolle in der Theorie der Lie-Gruppen und Lie-Algebren.

2. Allgemeiner existiert eine Jordan-Chevalley-Zerlegung falls k *perfekt* ist, d. h. wenn irreduzible Polynome in $k[t]$ keine mehrfachen Nullstellen im algebraischen Abschluss von k haben. Insbesondere gilt dies für alle Körper der Charakteristik 0 und alle endlichen Körper. Zum Beweis braucht man Galois-Theorie.

3. Sei $k = \mathbb{Z}/p\mathbb{Z}(x)$ der Körper der rationalen Funktionen über $\mathbb{Z}/p\mathbb{Z}$ mit p prim und $\chi_\alpha(t) = \chi_\alpha^{\min}(t) = (t^p - x)^2$. Dann hat α keine Jordan-Chevalley-Zerlegung.

3.7 Computeralgebra-Systeme

Explizite Rechnungen mit Matrizen muss heute kein Mathematiker mehr mit der Hand ausführen. Einfache Matrizenrechnung beherrscht heute schon jeder halbwegs fortschrittliche Taschenrechner. Für den Computer gibt es aber noch potentere Werkzeuge, sogenannte *Computeralgebrasysteme*. Diese beherrschen auch das symbolische Rechnen.

Wichtige Computeralgebrasysteme:

General-Purpose-Systeme:

- Mathematica (kommerziell)
- Maple (kommerziell)
- Magma (lizenzpflichtig)
- Mathcad (kommerziell, eher für den ingenieurtechnischen Bereich)
- MuPAD (an der Uni Paderborn entwickelt, heute Teil von MATLAB, kommerziell)
- Axiom (open source)
- Sage (open source, Integration mehrerer spezialisierter Systeme)
- Maxima (open source)

Spezialisierte Systeme:

- kommutative Algebra: CoCoA-5, Macauley2, SINGULAR
- Zahlentheorie: PARI/GP, KANT/KASH
- Gruppentheorie, Kombinatorik: GAP

Beispiel. Matrizenrechnung mit Maple:

`with(LinearAlgebra)` $\to$ Laden des Lineare-Algebra-Pakets
`A:=Matrix([[x,0],[0,-x]])` $\to$ Ausgabe der Matrix, interpretiert als Element von $M_{2,2}(\mathbb{C}(x))$
`Determinant(A)` $\to$ Ausgabe x^3
`Minimalpolynomial(A,t)` $\to$ Ausgabe $-x^2 + t^2$
`x:=0` $\to$ Spezialisiere x zu 0
`Minimalpolynomial(A,t)` $\to$ Ausgabe t
`A` $\to$ Ausgabe $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$
`?Eigenvalues` $\to$ Aufruf der Hilfeseiten zu dem Befehl.

4 Bilinearformen und Skalarprodukte

4.1 Bilinearformen

Sei K ein Körper.

Definition 4.1. Sei V ein K-Vektorraum. Eine *Bilinearform auf V* ist eine Abbildung

$$\gamma\colon V \times V \to K,$$

so dass γ in jedem Argument linear ist, d. h. für $\alpha, \beta \in K$, $u, v, w \in V$ gilt

$$\gamma(\alpha u + \beta v, w) = \alpha\gamma(u, w) + \beta\gamma(v, w),$$
$$\gamma(u, \alpha v + \beta w) = \alpha\gamma(u, v) + \beta\gamma(v, w).$$

Beispiele.

(i) Sei $\phi\colon V \to V^*$ eine lineare Abbildung. Dann ist

$$\gamma_\phi\colon V \times V \to K, \quad (v, w) \mapsto (\phi(w))(v)$$

eine Bilinearform.

(ii) Ist $\gamma\colon V \times V \to K$ eine Bilinearform, so ist auch

$$\gamma^*\colon V \times V \to K, \quad (v, w) \mapsto \gamma(w, v)$$

eine Bilinearform.

(iii) Sei $V = K^n$ und $A \in M_{n,n}(K)$. Dann ist

$$\gamma_A\colon K^n \times K^n \to K, \quad (v, w) \mapsto v^t A w$$

eine Bilinearform.

(iv) Speziell für $K = \mathbb{R}$, $A = E_n$ erhält man so das *Standardskalarprodukt*

$$\langle \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}, \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \rangle_{\mathbb{R}^n} = a_1 b_1 + \cdots + a_n b_n.$$

Definition 4.2. Sei V ein endlich-dimensionaler Vektorraum mit Basis $(v_1, \ldots, v_n)$ und

$$\gamma\colon V \times V \longrightarrow K$$

eine Bilinearform. Die Matrix

$$G = (g_{ij}) = (\gamma(v_i, v_j))$$

heißt die *Fundamentalmatrix* von γ bzgl. dieser Basis.

Die Menge aller Bilinearformen auf V wird zum Vektorraum $\mathrm{Bil}(V)$ durch

$$(\alpha\gamma_1 + \beta\gamma_2)(v,w) := \alpha\gamma_1(v,w) + \beta\gamma_2(v,w), \quad \alpha,\beta \in K.$$

Lemma 4.3. *Sei V ein n-dimensionaler K-Vektorraum und sei $(v_1,\ldots,v_n)$ eine Basis von V. Dann gibt es einen Isomorphismus von Vektorräumen*

$$\begin{array}{rccc} \varphi_{v_1,\ldots,v_n}\colon \mathrm{Bil}(V) & \longrightarrow & M_{n,n}(K) \\ \gamma & \longmapsto & G \quad . \end{array}$$

Beweis. Da γ bilinear ist, gilt für Vektoren $v = \sum a_i v_i$ und $w = \sum b_i v_i$

$$(*) \qquad \gamma(v,w) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_i\gamma(v_i,v_j)b_j = (a_1,\ldots,a_n)G\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = a^tGb \in K,$$

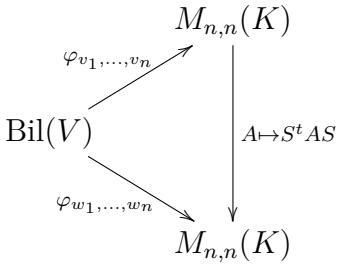
weshalb die Bilinearform γ durch ihre Fundamentalmatrix G schon eindeutig bestimmt ist. Umgekehrt definiert jede Matrix $G \in M_{n,n}(K)$ mit Hilfe der Gleichung $(*)$ eine Bilinearform $\gamma : V \times V \to K$ mit Fundamentalmatrix G.
Linearität von $\varphi_{v_1,\ldots,v_n}$: Sind G_1 und G_2 die Fundamentalmatrizen zu γ_1 und γ_2, so ist $\alpha G_1 + \beta G_2$ die Fundamentalmatrix zu $\alpha\gamma_1 + \beta\gamma_2$. □

Wie ändert sich die Fundamentalmatrix G bei Basiswechsel?

Satz 4.4 (Transformationssatz für Bilinearformen)**.** *Sei V ein n-dimensionaler K-Vektorraum und seien $(v_1,\ldots,v_n)$ und $(w_1,\ldots,w_n)$ Basen von V. Ist $S = M^{w_1,\ldots,w_n}_{v_1,\ldots,v_n}(\mathrm{id}_V)$, so gilt*

$$\varphi_{w_1,\ldots,w_n}(\gamma) = S^t\varphi_{v_1,\ldots,v_n}(\gamma)S,$$

d.h. es kommutiert das Diagramm



Beweis. Die Fundamentalmatrix von γ bzgl. $(w_1,\ldots,w_n)$ gegeben durch $G' = (g'_{ij})$ mit

$$\begin{aligned} g'_{ij} &= (\gamma(w_i,w_j)) \\ &= \gamma\left(\sum_{k=1}^{n} s_{ki}v_k, \sum_{\ell=1}^{n} s_{\ell j}v_\ell\right) \\ &= \sum_{k=1}^{n}\sum_{\ell=1}^{n} s_{ki}g_{k\ell}s_{\ell j} \end{aligned}$$

Also $G' = S^t G S$. □

Bemerkung. Bei Basiswechsel $G \to S^t G S$ gilt $\det(S^t G S) = \det(S)^2 \cdot \det(G)$. Die Determinante der Fundamentalmatrix ist also *nicht* basisunabhängig. Es gilt jedoch $r(G) = r(S^t G S)$ und $\det(G) = 0 \Leftrightarrow \det(S^t G S) = 0$.

Definition 4.5. Sei $\dim_K V = n$ und $\gamma\colon V \times V \to K$ eine Bilinearform. Der *Rang* $r(\gamma)$ von γ ist der Rang der Fundamentalmatrix G von γ bezüglich einer beliebigen Basis von V.

Satz 4.6. *Sei $\gamma\colon V \times V \to K$ eine Bilinearform. Dann ist*

$$\Gamma_\gamma\colon V \to V^*, \quad w \mapsto V \xrightarrow{v \mapsto \gamma(v,w)} K$$

eine lineare Abbildung. Die Zuordnung

$$\mathrm{Bil}(V) \to \mathrm{Hom}_K(V, V^*), \quad \gamma \mapsto \Gamma_\gamma$$

ist ein linearer Isomorphismus. Ist V endlichdimensional mit Basis $(v_1, \dots, v_n)$ und ist G die Fundamentalmatrix von γ bezüglich dieser Basis, so gilt

$$M^{v_1,\dots,v_n}_{v_1^*,\dots,v_n^*}(\Gamma_\gamma) = G.$$

Beweis.
Linearität von Γ_γ: Standard.
Linearität von $\gamma \mapsto \Gamma_\gamma$: Auch Standard: Seien $\alpha \in K$, $\gamma_1, \gamma_2 \in \mathrm{Bil}(V)$, $v, w \in V$. Dann gilt

$$(\Gamma_{(\alpha\gamma_1+\gamma_2)}(w))(v) = \alpha\gamma_1(v,w) + \gamma_2(v,w) = ((\alpha\Gamma_{\gamma_1})(w))(v) + (\Gamma_{\gamma_2}(w))(v).$$

Da dies für alle $v, w \in V$ gilt, folgt

$$\Gamma_{(\alpha\gamma_1+\gamma_2)} = \alpha\Gamma_{\gamma_1} + \Gamma_{\gamma_2}.$$

Dies ist ein Isomorphismus, denn durch

$$\mathrm{Hom}_K(V, V^*) \to \mathrm{Bil}(V), \quad \phi \mapsto \gamma_\phi$$

ist eine Inverse gegeben.
Schließlich gilt

$$\begin{aligned} &(\Gamma_\gamma(v_j))(v_i) = \gamma(v_i, v_j), \quad v_i^*(v_j) = \delta_{ij} \\ \Rightarrow \quad &\Gamma_\gamma(v_j) = \sum_{i=1}^{n} \gamma(v_i, v_j) v_i^* \end{aligned}$$

und damit $M^{v_1,\dots,v_n}_{v_1^*,\dots,v_n^*}(\Gamma_\gamma) = G$. □

Lemma 4.7. *Sei $\gamma\colon V \times V \to K$ eine Bilinearform auf einem endlichdimensionalen Vektorraum V mit Basis $(v_1, \dots, v_n)$. Sei $G = \varphi_{v_1,\dots,v_n}(\gamma)$ die Fundamentalmatrix von γ bezüglich dieser Basis. Dann gilt*

$$\Gamma_{\gamma^*} = \Gamma_\gamma^*\colon V = V^{**} \to V^*$$

und $G^t = \varphi_{v_1,\dots,v_n}(\gamma^*)$.

Beweis. Es gilt für $w \in V$

$$\begin{aligned} \Gamma_\gamma^*(w)\colon V &\mapsto K, \quad v \mapsto (\Gamma_\gamma(v))(w) = \gamma(w, v) \\ \Gamma_{\gamma^*}(w)\colon V &\mapsto K, \quad v \mapsto \gamma^*(v, w) = \gamma(w, v). \end{aligned}$$

und

$$G^t = (\gamma(v_j, v_i)) = (\gamma^*(v_i, v_j)) = \varphi_{v_1,\dots,v_n}(\gamma^*).$$

□

Definition 4.8. Eine Bilinearform $\gamma : V \times V \to K$ heißt *nicht ausgeartet*, wenn die zugehörige Abbildung $\Gamma_\gamma\colon V \to V^*$ ein Isomorphismus ist (und anderenfalls ausgeartet).

Satz 4.9 (Charakterisierung nicht ausgearteter Bilinearformen)**.** *Sei $\gamma\colon V \times V \to K$ eine Bilinearform auf dem n-dimensionalen K-Vektorraum V. Es sei $(v_1, \dots, v_n)$ eine Basis von V und $G = \varphi_{v_1,\dots,v_n}(\gamma) \in M_{n,n}(K)$ die Fundamentalmatrix von γ bezüglich $(v_1, \dots, v_n)$. Dann sind die folgenden Aussagen äquivalent:*

(i) *γ ist nicht ausgeartet.*

(ii) *G ist invertierbar.*

(iii) *$r(\gamma) = n$*

(iv) *γ^* ist nicht ausgeartet.*

(v) *Gilt $\gamma(v, w) = 0$ für alle $v \in V$, so gilt $w = 0$.*

(vi) *Gilt $\gamma(v, w) = 0$ für alle $w \in V$, so gilt $v = 0$.*

Beweis.
$(i) \Leftrightarrow (ii)$: folgt sofort aus 4.6.
$(ii) \Leftrightarrow (iii)$: Es gilt $r(\gamma) = r(G)$ und G ist invertierbar genau dann, wenn $r(G) = n$.
$(ii) \Leftrightarrow (iv)$: Mit G ist auch G^t invertierbar. Dies ist die Fundamentalmatrix von γ^*
$(i) \Leftrightarrow (v)$: Wegen $\dim V^* = \dim V$ (LA I, 3.42) ist der Homomorphismus $\Gamma_\gamma\colon V \to V^*$ genau dann ein Isomorphismus, wenn er injektiv ist (LA I, 3.30), d. h. aus

$\Gamma_\gamma(w) = 0$ folgt $w = 0$. Nun gilt $\Gamma_\gamma(w) = 0 \in V^*$ genau dann, wenn für alle $v \in V$ gilt

$$(\Gamma_\gamma(w))(v) = \gamma(v, w) = 0.$$

$(iv) \Leftrightarrow (vi)$: Wie $(i) \Leftrightarrow (v)$. □

Definition 4.10. Eine Bilinearform $\gamma\colon V \times V \longrightarrow K$ heißt

(i) *symmetrisch*, wenn $\gamma = \gamma^*$.

(ii) *antisymmetrisch*, wenn $\gamma = -\gamma^*$.

(iii) *alternierend*, wenn $\gamma(v, v) = 0$ für alle $v \in V$.

Lemma 4.11. *Ist γ alternierend, so ist γ auch antisymmetrisch. Ist* $\operatorname{char} K \neq 2$*, so sind die beiden Begriffe äquivalent.*

Beweis. Sei γ alternierend und $v, w \in V$. Dann gilt

$$\begin{aligned}\gamma(v, w) + \gamma(w, v) &= \gamma(v, v) + \gamma(v, w) + \gamma(w, v) + \gamma(w, w)\\ &= \gamma(v, v + w) + \gamma(w, v + w) = \gamma(v + w, v + w) = 0.\end{aligned}$$

Ist γ antisymmetrisch und $\operatorname{char} K \neq 2$, so folgt aus $0 = 2\gamma(v, v)$, dass $\gamma(v, v) = 0$. □

Bemerkung. Im Fall $\operatorname{char}(K) = 2$ gilt $-1_K = 1_K$, also gilt in diesem Fall 'symmetrisch'= 'antisymmetrisch'. Die Bilinearform

$$\gamma : K^3 \times K^3 \longrightarrow K, (x, y) \mapsto x^t y = x_1y_1 + x_2y_2 + x_3y_3$$

ist im Fall $\operatorname{char}(K) = 2$ antisymmetrisch, aber nicht alternierend.

Lemma 4.12. *Sei $\gamma\colon V \times V \to K$ eine Bilinearform und $(v_1, \ldots, v_n)$ eine Basis von V. Sei $G = (g_{ij}) = \varphi_{v_1,\ldots,v_n}(\gamma)$ die Fundamentalmatrix. Dann gilt*

(i) γ symmetrisch $\Longleftrightarrow$ G ist symmetrische Matrix (d.h. $G^t = G$).

(ii) γ antisymmetrisch $\Longleftrightarrow$ G ist antisymmetrische Matrix (d.h. $G^t = -G$).

Beweis. Zu (i):
$(\Rightarrow) : g_{ij} = \gamma(v_i, v_j) = \gamma(v_j, v_i) = g_{ji}$.
$(\Leftarrow)$: Sei $v = \lambda_1 v_1 + \cdots + \lambda_n v_n,\ w = \mu_1 v_1 + \cdots + \mu_n v_n$ und sei G symmetrisch. Dann gilt

$$\gamma(v, w) = (\lambda_1, \ldots, \lambda_n)G \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix} = (\mu_1, \ldots, \mu_n)G^t \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \gamma(w, v)$$

(ii) geht analog. □

4.2 Quadratische Räume

Sei K ein Körper.

Definition 4.13. Sei V ein K-Vektorraum. Eine *quadratische Form* ist eine Abbildung $q\colon V \to K$, so dass

(i) $q(\alpha v) = \alpha^2 q(v)$ für alle $v \in V$, $\alpha \in K$ (d. h. q ist homogen vom Grad 2).

(ii) Die Abbildung $V \times V \to K$, $(v, w) \mapsto q(v + w) - q(v) - q(w)$ ist eine (automatisch symmetrische) Bilinearform.

Zwei quadratische Formen $q\colon V \to K$, $q'\colon W \to K$ heißen *äquivalent*, wenn es einen K-linearen Isomorphismus $f\colon V \to W$ mit $q' = q \circ f$ gibt.

Beispiele.

(i) Sei
$$q(x_1, \ldots, x_n) = \sum_{i=1}^{n} \sum_{j=i}^{n} a_{ij} x_i x_j \in K[x_1, \ldots, x_n].$$
Dann ist $q\colon K^n \to K$ eine quadratische Form.

(ii) Ist $\gamma\colon V \times V \to K$ eine symmetrische Bilinearform, so ist
$$q_\gamma\colon V \to K, \quad v \mapsto \gamma(v, v)$$
eine quadratische Form.

(iii) Sei jetzt $\operatorname{char} K \neq 2$. Ist $q\colon V \to K$ eine quadratische Form, so ist
$$\gamma_q\colon V \times V \to K, \quad (v, w) \mapsto \frac{1}{2}(q(v + w) - q(v) - q(w))$$
eine symmetrische Bilinearform und es gilt $q_{\gamma_q} = q$, $\gamma_{q_\gamma} = \gamma$. Für $\operatorname{char} K \neq 2$ sind quadratische Formen und symmetrische Bilinearformen also im Wesentlichen dasselbe.

(iv) Für $\operatorname{char} K \neq 2$ sei $\gamma\colon K^n \times K^n$ bezüglich der Standardbasis durch die symmetrische Fundamentalmatrix $A = (a_{ij})$ gegeben. Setze
$$q(x_1, \ldots, x_n) = \sum_{i=1}^{n} \left(a_{ii} x_i^2 + 2 \sum_{j=i+1}^{n} a_{ij} x_i x_j \right)$$
Dann gilt $q_\gamma = q\colon K^n \to K$. Die quadratischen Formen wie in (i) sind also bereits alle quadratische Formen des K^n (das gilt auch für $\operatorname{char} K = 2$).

Sei $\operatorname{char} K \neq 2$.

Definition 4.14. Ein n-dimensionaler K-Vektorraum V zusammen mit einer symmetrischen Bilinearform $\gamma\colon V \times V \to K$ heißt *quadratischer Raum* der Dimension n über K. Zwei Elemente $v, w \in V$ heißen *orthogonal*, wenn $\gamma(v, w) = 0$. Eine Basis $(v_1, \ldots, v_n)$ von V heißt *Orthogonalbasis*, wenn $\gamma(v_i, v_j) = 0$ für $i \neq j$ gilt.

Bemerkungen.

(i) $(v_1, \ldots, v_n)$ ist genau dann eine Orthogonalbasis, wenn die Fundamentalmatrix $G = (\gamma(v_i, v_j))$ eine Diagonalmatrix ist.

(ii) Der Kürze halber schreiben wir von jetzt an auch $\gamma(v, w) = \langle v, w\rangle$.

(iii) Ist $\operatorname{char} K = 2$, so ist ein quadratischer Raum ein Vektorraum mit einer quadratischen Form.

Definition 4.15. Es seien (H_1, γ_1) und (H_2, γ_2) zwei quadratische Räume. Ein *Homomorphismus quadratischer Räume*

$$f\colon (H_1, \gamma_1) \longrightarrow (H_2, \gamma_2)$$

ist ein Vektorraumhomomorphismus $f\colon H_1 \to H_2$, so dass gilt:

$$\gamma_2(f(v), f(w)) = \gamma_1(v, w)$$

für alle $v, w \in H_1$. Ist f zusätzlich bijektiv, so wird f *lineare Isometrie* genannt.

Bemerkungen.

(i) Ist $f\colon (H_1, \gamma_1) \to (H_2, \gamma_2)$ eine Isometrie, so ist auch die Inverse f^{-1} eine lineare Isometrie.

(ii) Zwei quadratische Formen $q_1\colon H_1 \to K$, $q_2\colon H_2 \to K$ sind genau dann äquivalent, wenn die quadratischen Räume (H_1, γ_{q_1}) und (H_2, γ_{q_2}) isometrisch sind.

Aufgabe: Klassifikation der quadratischen Räume bis auf lineare Isometrie bzw. der quadratischen Formen bis auf Äquivalenz.

Definition 4.16. Sind (V_1, γ_1) und (V_2, γ_2) zwei quadratische Räume, so heißt (V, γ) mit

$$V = V_1 \oplus V_2, \quad \gamma\Big((v_1, v_2), (w_1, w_2)\Big) = \gamma_1(v_1, w_1) + \gamma_2(v_2, w_2)$$

die *orthogonale direkte Summe* von (V_1, γ_1) und (V_2, γ_2).
Bezeichnung: $(V, \gamma) = (V_1, \gamma_1) \hat{\oplus} (V_2, \gamma_2)$, oder einfach $V = V_1 \hat{\oplus} V_2$.

Definition/Lemma 4.17. *Seien U_1, U_2 zwei Untervektorräume eines quadratischen Raumes (V, γ). Dann ist der induzierte Homomorphismus*

$$f : (U_1, \gamma|_{U_1}) \hat{\oplus} (U_2, \gamma|_{U_2}) \longrightarrow (V, \gamma),\ f(u_1, u_2) = u_1 + u_2$$

genau dann ein Homomorphismus quadratischer Räume, wenn $\gamma(u_1, u_2) = 0$ für alle $u_1 \in U_1$, $u_2 \in U_2$ gilt. Ist dies der Fall und ist überdies f ein Isomorphismus (dies ist äquivalent zu $U_1 \cap U_2 = \{0\}$ und $U_1 + U_2 = V$, vgl. LA I, 3.7), so sagt man, dass V die orthogonale direkte Summe *seiner Unterräume U_1 und U_2 ist, und schreibt $V = U_1 \hat{\oplus} U_2$.*

Beweis. Sei h die Bilinearform auf $(U_1, \gamma|_{U_1}) \hat{\oplus} (U_2, \gamma|_{U_2})$, siehe Definition 4.16. Für $u_1, u_1' \in U_1$, $u_2, u_2' \in U_2$ gilt

$$h((u_1, u_2), (u_1', u_2')) = \gamma(u_1, u_1') + \gamma(u_2, u_2').$$

Es ist f genau dann ein Homomorphismus, wenn für beliebige $u_1, u_1' \in U_1$, $u_2, u_2' \in U_2$ gilt

$$h((u_1, u_2), (u_1', u_2')) = \gamma(f(u_1, u_2), f(u_1', u_2')) = \gamma(u_1 + u_2, u_1' + u_2'),$$

also

$$\gamma(u_1, u_1') + \gamma(u_2, u_2') = \gamma(u_1, u_1') + \gamma(u_1, u_2') + \gamma(u_2, u_1') + \gamma(u_2, u_2'),$$

d.h.

$$0 = \gamma(u_1, u_2') + \gamma(u_1', u_2).$$

Dies ist äquivalent dazu, dass $\gamma(u_1, u_2) = 0$ für alle $u_1 \in U_1$, $u_2 \in U_2$ gilt. □

Theorem 4.18. *Sei (V, γ) ein quadratischer Raum. Dann gibt es eine Orthogonalbasis $(v_1, \ldots, v_n)$.*

Beweis. Induktion über die Dimension. Der Fall $n = 1$ ist trivial.
Sei $n \geq 2$. Gilt $\langle v, v\rangle = 0$ für alle $v \in V$, so gilt auch $\langle v + w, v + w\rangle = 2\langle v, w\rangle = 0$ für alle $v, w \in V$ und wegen char $K \neq 2$ ist γ identisch 0. In diesem Fall ist jede Basis orthogonal. Ansonsten existiert ein $v_1 \in V$ mit $\langle v_1, v_1\rangle =: a_1 \neq 0$. Sei

$$H = \{v \in V | \langle v, v_1\rangle = 0\}.$$

Dann gilt $H = \ker(\Gamma_\gamma(v_1) \colon V \to K)$, also $\dim H \in \{n, n-1\}$ nach der Dimensionsformel. Wegen $v_1 \notin H$ gilt $\dim H = n - 1$ und $V \cong Kv_1 \oplus H$.
Nun ist $(H, \gamma|_{H\times H})$ ein quadratischer Raum der Dimension $n - 1$. Nach Induktionsvoraussetzung existiert eine Orthogonalbasis $v_2, \ldots, v_n$ von H. Dann ist $v_1, \ldots, v_n$ eine Basis von V, und die Fundamentalmatrix ist diagonal wegen $\langle v_i, v_j\rangle = 0$ für $i \neq j$. □

Korollar 4.19. *Sei $A \in M_{n,n}(K)$ eine symmetrische Matrix. Dann gibt es eine Matrix $S \in \mathrm{Gl}_n(K)$, so dass S^tAS Diagonalform hat.*

Beweis. Bezüglich der Standardbasis definiert die Matrix A eine symmetrische Bilinearform auf dem K^n. Bzgl. einer Orthogonalbasis des K^n hat diese Diagonalform. Der Basiswechsel von der Standardbasis zu dieses Orthogonalbasis überführt A in S^tAS für ein $S \in \mathrm{Gl}_n(K)$ und S^tAS hat Diagonalgestalt. □

Korollar 4.20. *Sei $\dim_K V = n$ und $q\colon V \to K$ eine quadratische Form mit $r(\gamma_q) = r$. Dann gibt es $\lambda_1, \dots, \lambda_r \in K^\times$, so dass q äquivalent ist zu der quadratischen Form*

$$Q\colon K^n \to K, \qquad (x_i) \mapsto \sum_{i=1}^{r} \lambda_i x_i^2.$$

Theorem 4.21 (Klassifikation quadratischer Räume über $\mathbb{C}$)**.** *Sei (V, γ) ein quadratischer Raum über $\mathbb{C}$ der Dimension n. Dann existiert eine Orthogonalbasis $(v_1, \dots, v_r, w_1, \dots, w_{n-r})$ von V, so dass $\gamma(v_i, v_i) = 1$, $\gamma(w_i, w_i) = 0$. Insbesondere ist (V, γ) isometrisch zu $(\mathbb{C}^n, \gamma_{\left(\begin{smallmatrix} E_r & 0 \\ 0 & 0 \end{smallmatrix}\right)})$. Die Isometrieklasse von (V, γ) ist durch die Zahlen $n = \dim_K V$ und $r = r(\gamma)$ eindeutig bestimmt.*

Beweis. Sei $(\tilde{v}_1, \dots, \tilde{v}_n)$ eine Orthogonalbasis. Setze

$$v_i = \begin{cases} \tilde{v}_i & \text{falls} \quad \tilde{\lambda}_i = \gamma(\tilde{v}_i, \tilde{v}_i) = 0 \\ \frac{1}{\sqrt{\tilde{\lambda}_i}} \tilde{v}_i & \text{falls} \quad \tilde{\lambda}_i = \gamma(\tilde{v}_i, \tilde{v}_i) \neq 0 \end{cases}$$

Hier ist $\sqrt{\tilde{\lambda}_i}$ eine beliebig gewählte komplexe Zahl α mit $\alpha^2 = \tilde{\lambda}_i$.
Dann ist $(v_1, \dots, v_n)$ eine OB mit $\lambda_i = \langle v_i, v_i \rangle \in \{0, 1\}$. Die gesuchte OB erhalten wir durch Umsortierung. Für die Fundamentalmatrix $G = \mathrm{diag}(\lambda_i)$ gilt dann $r = r(G)$. Bezüglich einer anderen OB hat γ die Darstellungsmatrix T^tGT für ein $T \in \mathrm{Gl}_n(\mathbb{C})$, und es gilt $r(T^tGT) = r(G)$. Daher ist r und n unabhängig von der Auswahl der OB. □

Korollar 4.22. *Sei G eine symmetrische komplexe $n \times n$-Matrix. Dann existiert ein $T \in \mathrm{Gl}_n(\mathbb{C})$, so dass*

$$T^tGT = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}.$$

Die Zahl $r = r(G)$ ist unabhängig von der Wahl von T.

Korollar 4.23. *Sei $q\colon V \to \mathbb{C}$ eine quadratische Form mit $\dim_{\mathbb{C}} V = n$. Dann gibt es einen linearen Isomorphismus $f\colon \mathbb{C}^n \to V$ so dass*

$$(q \circ f)(x_1, \dots, x_n) = x_1^2 + \cdots + x_r^2.$$

Die Zahl $r = r(\gamma_q)$ ist durch q eindeutig bestimmt.

Theorem 4.24 (Klassifikation quadratischer Räume über $\mathbb{R}$)**.** *Sei (V, γ) ein quadratischer Raum über $\mathbb{R}$. Dann existiert eine OB*

$$(u_1, \ldots, u_{r_+}, v_1, \ldots, v_{r_-}, w_1, \ldots, w_{n-r_+-r_-})$$

von V, so dass

$$\langle u_i, u_i \rangle = 1, \quad \langle v_i, v_i \rangle = -1, \quad \langle w_i, w_i \rangle = 0.$$

*Die Isometrieklasse von (V, γ) ist durch die Dimension $n = \dim_K V$ und durch das Paar (r_+, r_-) (*Signatur *von γ) eindeutig bestimmt.*

Beweis. Sei $(\tilde{v}_1, \ldots, \tilde{v}_n)$ eine OB. Setze

$$v_i = \begin{cases} \tilde{v}_i & \text{falls} \quad \tilde{\lambda}_i = \gamma(\tilde{v}_i, \tilde{v}_i) = 0 \\ \frac{1}{\sqrt{|\tilde{\lambda}_i|}} v_i & \text{falls} \quad \tilde{\lambda}_i = \gamma(\tilde{v}_i, \tilde{v}_i) \neq 0. \end{cases}$$

Nach Umsortieren erhalten wir die gewünschte OB, bezüglich der γ die Fundamentalmatrix

$$G = \operatorname{diag}(\underbrace{1, \ldots, 1}_{r_+}, \underbrace{-1, \ldots, -1}_{r_-}, 0, \ldots, 0)$$

hat. Wie im Komplexen erhalten wir, dass $r_+ + r_- = r(G)$ von der Wahl der OB unabhängig ist. Daher genügt es zu zeigen, dass r_+ auch unabhängig davon ist. Setze

$$\begin{aligned} V_+ &=< u_1, \ldots, u_{r_+} > \\ V_- &=< v_1, \ldots, v_{r_-} > \\ V_0 &=< w_1, \ldots, w_{n-r_+-r_-} > \end{aligned}$$

Dann gilt $V = V_+ \oplus V_- \oplus V_0$. Setze

$$a = \max\{\dim(W) \mid W \subset V \text{ mit } \gamma(w, w) > 0 \text{ für alle } 0 \neq w \in W\}.$$

Zunächst hat V_+ diese Eigenschaft, also $a \geq r_+$. Wäre $a > r_+$, so existiert ein UVR $W \subset V$ mit der obigen Eigenschaft und $\dim W > r_+$. Hieraus folgt $\dim W + \dim V_- + \dim V_0 > n$. Die Dimensionsformel liefert $W \cap (V_- \oplus V_0) > 0$, es gibt also ein $w \in W$ mit $\gamma(w, w) > 0$ und $\gamma(w, w) \leq 0$. Dieser Widerspruch zeigt $r_+ = a$ und a ist unabhängig von der Auswahl der OB, also auch r_+. □

Korollar 4.25 (Sylvesterscher Trägheitssatz)**.** *Sei $G \in M_{n,n}(\mathbb{R})$ eine symmetrische reelle $n \times n$ Matrix. Dann existiert ein $T \in Gl_n(\mathbb{R})$, so dass*

$$T^t G T = \begin{pmatrix} E_{r_+} & 0 & 0 \\ 0 & -E_{r_-} & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Die Zahlen r_+ und r_- sind unabhängig von der Auswahl von T.

Korollar 4.26. *Sei $q\colon V \to \mathbb{R}$ eine quadratische Form mit $\dim_{\mathbb{R}} V = n$. Dann gibt es einen linearen Isomorphismus $f\colon \mathbb{R}^n \to V$ so dass*

$$(q \circ f)(x_1, \ldots, x_n) = x_1^2 + \ldots x_{r+}^2 - x_{r_+ +1}^2 - \cdots - x_r^2.$$

Die Zahlen r_+ und r sind durch q eindeutig bestimmt.

Bemerkung. Die vollständige Klassifikation der quadratischen Räume über $\mathbb{Q}$ ist um einiges schwieriger, siehe z. B. Serre: *A course in arithmetic*.

4.3 Euklidische Räume

Definition 4.27. Eine symmetrische Bilinearform $\gamma\colon V \times V \to \mathbb{R}$ auf einem endlich-dimensionalen $\mathbb{R}$-Vektorraum V heißt *positiv definit* (bzw. *positiv semi-definit*), wenn $\gamma(v, v) > 0$ (bzw. $\gamma(v, v) \geq 0$) für alle $v \in V \setminus \{0\}$ gilt. Analog definiert sich *negativ (semi-)definit*.

Beispiel. $\mathbb{R}^n$ mit dem Standardskalarprodukt

$$\langle x, y\rangle = x^t y = \sum_i x_i y_i$$

ist positiv definit, wegen

$$\langle x, x\rangle = x_1^2 + \cdots + x_n^2.$$

Definition 4.28. Ein *euklidischer Raum* ist reeller quadratischer Raum (V, γ) mit einer positiv definiten symmetrischen Bilinearform γ. Für ein $v \in V$ nennt man $\|v\| = \sqrt{\langle v, v\rangle}$ die *Norm* von v. Eine Basis $e_1, \ldots, e_n$ eines euklidischen Vektorraums heißt *Orthonormalbasis*, wenn $\langle e_i, e_j\rangle = \delta_{ij}$ gilt.

Satz 4.29. *Sei (V, γ) ein euklidischer Raum. Dann gelten für $x, y \in V$:*

(i) Schwarz'sche Ungleichung: $|\langle x, y\rangle| \leq \|x\| \cdot \|y\|$.

(ii) Dreiecksungleichung: $\|x + y\| \leq \|x\| + \|y\|$.

(iii) Polarisierungs-Identität: $\langle x, y\rangle = \frac{1}{4}(\|x + y\|^2 - \|x - y\|^2)$.

(iv) Satz des Pythagoras: Sind x und y orthogonal, so gilt $\|x+y\|^2 = \|x\|^2+\|y\|^2$.

Beweis.
(i): Ohne Einschränkung $x \neq 0, y \neq 0$. Dann gilt für $\lambda \in \mathbb{R}$

$$0 \leq \|x - \lambda y\|^2 = \|x\|^2 - 2\lambda\langle x, y\rangle + \lambda^2\|y\|^2.$$

Speziell für $\lambda = \frac{\langle x,y\rangle}{\|y\|^2}$ erhält man

$$0 \leq \|x\|^2 - \langle x, y\rangle^2\|y\|-2.$$

Also

$$\langle x, y\rangle^2 \leq \|x\|^2\|y\|^2.$$

Die Schwarz'sche Ungleichung folgt nach Wurzelziehen.
(ii): Es gilt

$$\|x+y\|^2 = \|x\|^2 + 2\langle x, y\rangle + \|y\|^2 \overset{(i)}{\leq} \|x\|^2 + 2\|x\|\|y\| + \|y\|^2 = (\|x\| + \|y\|)^2.$$

Die Dreiecksungleichung folgt nach Wurzelziehen.
(iii): Es gilt

$$\begin{aligned} \|x+y\|^2 &= \|x\|^2 + 2\langle x, y\rangle + \|y\|^2 \\ \|x-y\|^2 &= \|x\|^2 - 2\langle x, y\rangle + \|y\|^2 \\ \|x+y\|^2 - \|x-y\|^2 &= 4\langle x, y\rangle. \end{aligned}$$

(iv):

$$0 = 2\langle x, y\rangle = \|x+y\|^2 - \|x\|^2 - \|y\|^2.$$

□

Definition 4.30. Sei (V, γ) ein euklidischer Vektorraum. Der *Winkel* zwischen $x, y \in V$ ist definiert durch $\sphericalangle(x, y) = \cos^{-1}\left(\langle \frac{x}{\|x\|}, \frac{y}{\|y\|}\rangle\right) \in [0, \pi]$. Der *Abstand* zwischen x und y ist $d(x, y) = \|x - y\|$.

Bemerkungen.

(i) Mit $d\colon V \times V \to R$ wird der euklidische Raum V zu einem metrischen Raum.

(ii) Jeder Homomorphismus $f\colon (V, \gamma) \to (W, \gamma')$ euklidischer Räume ist injektiv, *abstandstreu* und *winkeltreu*: Es gilt für $x, y \in V$

$$\begin{aligned} f(x) = 0 \Leftrightarrow \|f(x)\| = 0 \Leftrightarrow \|x\| = 0 \Leftrightarrow x = 0 \\ d(f(x), f(y)) = d(x, y), \qquad \sphericalangle(f(x), f(y)) = \sphericalangle(x, y) \end{aligned}$$

weil beides mittels des Skalarproduktes definiert ist.

(iii) Umgekehrt gilt: Ist $f\colon V \to V$ abstandstreu, so ist f schon eine *affine Isometrie*, d. h.: Es gibt eine lineare Isometrie $\varphi\colon V \to V$ und ein $b \in V$, so dass

$$f(x) = \varphi(x) + b \quad \forall x \in V$$

(Übungsaufgabe).

Theorem 4.31. *Jeder euklidische Vektorraum (V, γ) besitzt eine Orthonormalbasis.*

Beweis. Sei $(v_1, \dots, v_n)$ eine Orthogonalbasis von V und G die Fundamentalmatrix von γ bzgl. $(v_1, \dots, v_n)$. Auf der Diagonale stehen die Werte $\langle v_i, v_i \rangle > 0$. Setze nun $e_i = \frac{1}{\sqrt{\langle v_i, v_i \rangle}} v_i$. Dann gilt $\langle e_i, e_j \rangle = \delta_{ij}$. □

Korollar 4.32. *Eine positiv definite symmetrische Bilinearform ist nicht ausgeartet. Es gibt eine Basis, bezüglich derer sie durch die Einheitsmatrix dargestellt wird.*

Korollar 4.33. *Ein euklidischer Raum (V, γ) mit $\dim_{\mathbb{R}} V = n$ ist isometrisch zum $\mathbb{R}^n$ mit dem Standardskalarprodukt.*

Beweis. Sei $(v_1, \dots, v_n)$ eine ONB von V. Dann ist $\varphi \colon (\mathbb{R}^n, \langle\ ,\ \rangle_{\text{Standard}}) \to (V, \gamma)$, $e_i \mapsto v_i$, eine Isometrie. □

Umgekehrt gilt:

Lemma 4.34. *Sei (V, γ) ein euklidischer Raum und $v_1, \dots, v_k$ paarweise orthogonal (d.h. $\gamma(v_i, v_j) = 0$ für $i \neq j$) und alle von 0 verschieden. Dann ist $(v_1, \dots, v_k)$ linear unabhängig.*

Beweis. Ist $\lambda_1 v_1 + \dots + \lambda_k v_k = 0$, so folgt für $i = 1, \dots, k$

$$0 = \gamma(\lambda_1 v_1 + \dots + \lambda_k v_k, v_i) = \lambda_i \gamma(v_i, v_i)$$

also $\lambda_i = 0$ für $i = 1, \dots, k$. □

Definition 4.35. Sei (V, γ) ein euklidischer Raum und $U \subset V$ ein Untervektorraum. Der Untervektorraum

$$U^\perp = \{v \in V \mid \langle u, v \rangle = 0 \text{ für alle } u \in U\}$$

heißt das *orthogonale Komplement* zu U.

Satz 4.36. *Sei $V = (V, \gamma)$ ein euklidischer Raum, $U \subset V$ ein Untervektorraum. Dann ist $U = (U, \gamma|_{U \times U})$ ein euklidischer Raum und es gilt $V = U \hat{\oplus} U^\perp$.*

Beweis. Klsr gilt $\langle u, u \rangle > 0$ für $0 \neq u \in U$, also ist U euklidisch.
Ist $u \in U \cap U^\perp$ so gilt $\langle u, u \rangle = 0$, also $u = 0 \Rightarrow U \cap U^\perp = 0$. Es bleibt zu zeigen: $U + U^\perp = V$. Sei $(u_1, \dots, u_m)$ eine ONB von U. Für $v \in V$ sei

$$v' = v - \sum_{i=1}^{m} \langle v, u_i \rangle u_i.$$

Dann gilt $\langle v', u_i \rangle = \langle v, u_i \rangle - \langle v, u_i \rangle = 0$ für $i = 1, \dots, m$, also $v' \in U^\perp$ und natürlich $\sum_{i=1}^{m} \langle v, u_i \rangle u_i \in U$. Daher gilt $V = U \oplus U^\perp$. Schließlich gilt $\langle u, v \rangle = \langle v, u \rangle = 0$ für alle $u \in U, v \in U^\perp$, weshalb die Summe orthogonal ist, siehe 4.17. □

4.4 Gram-Schmidt-Orthonormalisierung

Explizites Verfahren zur Bestimmung einer ONB (Gram-Schmidt-Verfahren).
Sei (V, γ) ein euklidischer Raum und $(v_1, \ldots, v_n)$ eine Basis. Wir konstruieren daraus induktiv eine ONB $(w_1, \ldots, w_n)$.

Schritt N_1 (Normalisieren): $w_1 := \frac{1}{\|v_1\|} \cdot v_1$

Sei $k \geq 2$ und sei eine ONB $w_1, \ldots, w_{k-1}$ von $\mathrm{Lin}(v_1, \ldots, v_{k-1})$ bereits konstruiert.

Schritt O_k (Orthogonalisieren): Setze

$$w'_k = v_k - \sum_{i=1}^{k-1} \gamma(v_k, w_i) w_i$$

Dann gilt für $i = 1, \ldots, k-1$

$$\begin{aligned} \gamma(w'_k, w_i) &= \gamma\Big(v_k - \sum_{j=1}^{k-1} \gamma(v_k, w_j) w_j, w_i\Big) \\ &= \gamma(v_k, w_i) - \gamma(v_k, w_i) \cdot \gamma(w_i, w_i) \\ &= 0. \end{aligned}$$

Außerdem gilt

$$v_k \notin \mathrm{Lin}(v_1, \ldots, v_{k-1}) = \mathrm{Lin}(w_1, \ldots, w_{k-1}),$$

also folgt auch

$$w'_k \notin \mathrm{Lin}(w_1, \ldots, w_{k-1}).$$

Hieraus folgt, dass $(w_1, \ldots, w_{k-1}, w'_k)$ eine OB von $\mathrm{Lin}(v_1, \ldots, v_k)$ ist.

Schritt N_k (Normalisieren): Setze $w_k = \frac{w'_k}{\|w'_k\|}$. Dann ist $(w_1, \ldots, w_k)$ eine ONB von $\mathrm{Lin}(v_1, \ldots, v_k)$.

Im Schritt N_n erhalten wir so eine ONB $(w_1, \ldots, w_n)$ von (V, γ) .

Beispiel. Im $\mathbb{R}^2$ mit dem Standardskalarprodukt sei die folgende Basis gegeben: $v_1 = \binom{3}{1}$, $v_2 = \binom{2}{2}$.

Schritt N_1: $|v_1| = \sqrt{3^2 + 1^2} = \sqrt{10}$. Also $w_1 = \begin{pmatrix} \frac{3}{\sqrt{10}} \\ \frac{1}{\sqrt{10}} \end{pmatrix}$.
Schritt O_2:

$$\begin{aligned} w'_2 = v_2 - \langle v_2, w_1 \rangle w_1 &= \begin{pmatrix} 2 \\ 2 \end{pmatrix} - \langle \begin{pmatrix} 2 \\ 2 \end{pmatrix}, \begin{pmatrix} \frac{3}{\sqrt{10}} \\ \frac{1}{\sqrt{10}} \end{pmatrix} \rangle \begin{pmatrix} \frac{3}{\sqrt{10}} \\ \frac{1}{\sqrt{10}} \end{pmatrix} \\ = \begin{pmatrix} 2 \\ 2 \end{pmatrix} - \frac{8}{\sqrt{10}} \cdot \begin{pmatrix} \frac{3}{\sqrt{10}} \\ \frac{1}{\sqrt{10}} \end{pmatrix} &= \begin{pmatrix} 2 \\ 2 \end{pmatrix} - \begin{pmatrix} \frac{24}{10} \\ \frac{8}{10} \end{pmatrix} = \begin{pmatrix} \frac{-2}{5} \\ \frac{6}{5} \end{pmatrix} \end{aligned}$$

Schritt N_2: $|w_2'| = \sqrt{\frac{40}{25}} = \frac{2\sqrt{10}}{5}$ und somit

$$w_2 = \frac{5}{2\sqrt{10}} \cdot \begin{pmatrix} \frac{-2}{5} \\ \frac{6}{5} \end{pmatrix} = \frac{1}{\sqrt{10}} \begin{pmatrix} -1 \\ 3 \end{pmatrix}.$$

Daher ist $\left(\begin{pmatrix} \frac{3}{\sqrt{10}} \\ \frac{1}{\sqrt{10}} \end{pmatrix}, \begin{pmatrix} \frac{-1}{\sqrt{10}} \\ \frac{3}{\sqrt{10}} \end{pmatrix} \right)$ eine ONB. Die Standardbasis ist natürlich auch eine ONB, aber wir erhalten sie hier nicht aus dem Gram-Schmidt-Verfahren.

Definition 4.37. Eine symmetrische reelle Matrix G heißt *positiv definit* (Bezeichnung: $G > 0$), wenn die zugehörige Bilinearform

$$(x, y) \longmapsto x^t G y$$

positiv definit ist.

Satz 4.38 (Cholesky-Zerlegung)**.** *Sei G positiv definit. Dann existiert eine obere Dreiecksmatrix T mit positiven Diagonaleinträgen, so dass $G = T^t T$. Die Matrix T ist eindeutig bestimmt.*

Beweis. Wende das GS-Verfahren auf $(\mathbb{R}^n, \gamma_G)$ und die Standardbasis $v = e$ an. Setze $w_1' = v_1$ und

$$T_{N_k} = M^{w_1,\dots,w_k,v_{k+1},\dots,v_n}_{w_1,\dots,w_k',v_{k+1},\dots,v_n}(\mathrm{id}) = \mathrm{diag}(1, \dots, \underbrace{\|w_k'\|}_{k}, \dots, 1).$$

$$T_{O_k} = M^{w_1,\dots,w_k',v_{k+1},\dots,v_n}_{w_1,\dots,v_k,v_{k+1},\dots,v_n}(\mathrm{id}) = \begin{pmatrix} E_{k-1} & \begin{pmatrix} \gamma_G(v_k, w_i) \end{pmatrix}_{i=1,\dots,k-1} & 0 \\ 0 & 1 & 0 \\ 0 & & E_{n-k-1} \end{pmatrix}$$

$$T = M^{v_1,\dots,v_n}_{w_1,\dots,w_n}(\mathrm{id}) = T_{N_n} T_{O_n} \cdots T_{N_1}.$$

Dann ist T als Produkt oberer Dreiecksmatrizen mit positiven Diagonaleinträgen eine obere Dreiecksmatrix mit positiven Diagonaleinträgen und es gilt $E = (T^{-1})^t G (T^{-1})$ und somit $G = T^t T$. Beachte dabei, dass $\det T$ gerade das Produkt der Diagonaleinträge ist, also ist T invertierbar. Ist S eine weitere obere Dreiecksmatrix mit positiven Diagonaleinträgen mit $S^t S = T^t T = G$, so ist

$$D = T S^{-1} = (T^t)^{-1} S^t = (S T^{-1})^t = (D^{-1})^t$$

sowohl eine untere als auch obere Dreiecksmatrix, also eine Diagonalmatrix. Wegen $D = D^{-1}$ sind die Quadrate der Diagonaleinträge gleich 1. Da die Diagonaleinträge positiv sind, sind sie selbst schon gleich 1, also $D = E$ und $T = S$. □

Satz 4.39. *Für eine reelle symmetrische Matrix G sind die folgenden Aussagen äquivalent:*

(i) *G ist positiv definit.*

(ii) *es existiert eine obere Dreiecksmatrix mit positiven Diagonaleinträgen T mit $G = T^tT$.*

(iii) *es existiert eine invertierbare Matrix A mit $G = A^tA$.*

Beweis.
$(i) \Rightarrow (ii)$: vorheriger Satz.
$(ii) \Rightarrow (iii)$: trivial
$(iii) \Rightarrow (i)$: Sei $G = T^tT$. Dann gilt für $x \in \mathbb{R}^n \setminus \{0\}$:

$$\gamma(x,x) = x^tGx = x^tT^tTx = \langle Tx, Tx\rangle_{\text{Standard}} > 0.$$

Daher ist G positiv definit. □

Definition 4.40. Es sei $A = (a_{ij})_{\substack{i=1,\dots,n\\ j=1,\dots,n}}$ eine $n \times n$-Matrix, $K = \{1,\dots,k\}$. Der Minor $\det\limits_{K,K}(A)$ heißt der *k-te Hauptminor* von A.

Satz 4.41 (Hauptminorenkriterium)**.** *Eine symmetrische reelle $n \times n$-Matrix G ist genau dann positiv definit, wenn die k-ten Hauptminoren $k = 1,\dots,n$ sämtlich größer als Null sind.*

Beweis. Sei G positiv definit, dann gilt $G = T^tT$ für eine invertierbare Matrix T und also $\det(G) = \det(T^t)\det(T) = \det(T)^2 > 0$. Schränkt man die positiv definite Bilinearform $\gamma(x,y) = x^tGy$ auf dem $\mathbb{R}^n$ auf den von $e_1,\dots,e_k$ aufgespannten Unterraum ein, erhält man die Bilinearform auf dem $\mathbb{R}^k$, die durch die Matrix

$$G_k = (\gamma(e_i,e_j))_{i,j=1\dots k}$$

gegeben ist. Daher ist G_k positiv definit und es gilt daher auch $\det(G_k) > 0$ für jedes $k = 1,\dots,n$.
Sei umgekehrt $\det G_k > 0$ für $k = 1,\dots,n$. Wir schauen uns das Gram-Schmidt-Verfahren an, ohne zu wissen, dass die Form $\gamma(x,y) = x^tGy$ positiv definit ist. Wenn das Verfahren durchläuft, erhalten wir eine Orthonormalbasis, und G ist positiv definit. Wir starten mit der kanonischen Basis $(e_1,\dots,e_n)$.
Hinreichend für das Durchlaufen des Algorithmus: Für jedes k gilt für den Vektor

$$w_k' := e_k - \sum_{i=1}^{k-1} \gamma(e_k, w_i)w_i$$

dass $\gamma(w_k', w_k') > 0$.
Die Form $\gamma|_{\mathbb{R}^k}$ auf dem $\mathbb{R}^k$ wird bzgl. der kanonischen Basis durch die Matrix G_k dargestellt. Es ist $(w_1,\dots,w_{k-1},w_k')$ eine Orthogonalbasis von $(\mathbb{R}^k, \gamma|_{\mathbb{R}^k})$. Die

darstellende $k \times k$ Matrix A hat die Form $\mathrm{diag}(1, \ldots, 1, \gamma(w_k', w_k'))$, hat also insbesondere die Determinante $\gamma(w_k', w_k')$. Andererseits gilt $A = T^t G_k T$ für eine invertierbare Matrix T, also gilt

$$\gamma(w_k', w_k') = \det(T^t G_k T) = \det(T)^2 \det(G_k) > 0.$$

Daher läuft der Algorithmus durch und wir erhalten eine ONB. Also ist G positiv definit. □

4.5 Orthogonale Matrizen

Wie sehen Koordinatenwechselmatrizen von einer ONB zur anderen aus?

Definition 4.42. Eine Matrix $A \in M_{n,n}(\mathbb{R})$ heißt *orthogonal*, wenn $A^t A = E$ gilt.

Lemma 4.43.

(i) Eine orthogonale Matrix A ist invertierbar und $A^{-1} = A^t$.

(ii) Ist A orthogonal, so gilt $\det A = \pm 1$.

(iii) Ist A orthogonal, so gilt $A \cdot A^t = E$.

Beweis.
(i) folgt aus $A^t A = E$.
(ii) aus $\det(A)^2 = \det(A^t)\det(A) = \det(E) = 1$
(iii) folgt aus $A^t = A^{-1}$. □

Definition/Lemma 4.44. *Die Menge $O(n)$ der orthogonalen $n \times n$-Matrizen ist eine Untergruppe der* $\mathrm{Gl}_n(\mathbb{R})$. *Sie heißt die* Orthogonale Gruppe *vom Rang n. Die Untergruppe*

$$SO(n) = \ker(\det \colon O(n) \longrightarrow \mathbb{R}^\times)$$

heißt die Spezielle Orthogonale Gruppe *vom Rang n.*

Beweis. Untergruppenkriterium: $E \in O(n)$ o.k.
$A, B \in O(n) \Rightarrow (A \cdot B)^t \cdot (A \cdot B) = B^t A^t A B = B^t B = E$, also $A \cdot B \in O(n)$.
$A \in O(n) \Rightarrow A^t A = E \Rightarrow A A^t = E \Rightarrow A^{-1} = A^t \in O(n)$. □

Theorem 4.45 (QR-Zerlegung)**.** *Sei $A \in \mathrm{Gl}_n(\mathbb{R})$. Dann gibt es eindeutig bestimmte Matrizen Q und R mit $Q \in O(n)$, R eine obere Dreiecksmatrix mit positiven Diagonaleinträgen und $A = QR$.*

Beweis. Sei $v = (v_1, \ldots, v_n)$ das System der Spalten von A. Da $A \in \mathrm{Gl}_n(\mathbb{R})$ ist v eine Basis von $\mathbb{R}^n$ und $A = M_e^v(\mathrm{id})$. Wende das Gram-Schmidt-Verfahren auf v und das Standardskalarprodukt an. Das liefert eine ONB $w = (w_1, \ldots, w_n)$ so dass $R = M_w^v(\mathrm{id})$ eine obere Dreieckmatrix mit strikt postiven Diagonaleinträgen ist. Sei $Q = M_e^w(\mathrm{id})$ die Matrix mit den Basisvektoren aus w als Spalten. Dann gilt

$$QR = M_e^v(\mathrm{id}) = A, \quad Q^tQ = (w_i^t w_j) = E, \quad \text{also } Q \in O(n).$$

Nach 4.39 ist A^tA positiv definit. Ist $A = PS$ eine weitere Zerlegung mit den obigen Eigenschaften, so gilt

$$R^tR = R^tQ^tQR = A^tA = S^tP^tPS = S^tS.$$

Wegen der Eindeutigkeit der Cholesky-Zerlegung folgt $S = T$ und damit $P = Q$. □

Bemerkung. Insbesondere gilt $R = Q^{-1}A = Q^tA = (w_i^t v_j)$ mit $w_i^t v_j = 0$ für $i > j$ und $w_i^t v_i > 0$.

Satz 4.46. *Sei $A \in M_{n,n}(\mathbb{R})$. Dann sind äquivalent:*

(i) $A \in O(n)$,

(ii) $A\colon (\mathbb{R}^n, \langle\ ,\ \rangle) \longrightarrow (\mathbb{R}^n, \langle\ ,\ \rangle)$ *ist eine lineare Isometrie.*

(iii) Die Spalten von A sind eine ONB von $(\mathbb{R}^n, \langle\ ,\ \rangle)$.

Beweis. Für $x, y \in \mathbb{R}^n$ gilt $\langle Ax, Ay\rangle = x^tA^tAy$. Daher ist A genau dann eine Isometrie, wenn die durch A^tA gegebene Bilinearform das Standardskalarprodukt ist, d.h. wenn $A^tA = E$ gilt. Ist v_i die i-te Spalte von A, so gilt $A^tA = E$ genau dann, wenn $v_i^t v_j = \langle v_i, v_j\rangle = \delta_{ij}$, d. h. wenn $(v_1, \ldots, v_n)$ ONB ist. □

4.6 Der Spektralsatz

Sei (V, γ) ein euklidischer Raum und $f \in \mathrm{End}_{\mathbb{R}}(V)$ (nicht notwendig eine Isometrie).

Definition 4.47. Die *Adjungierte* zu f ist die Komposition

$$V \xrightarrow[\cong]{\Gamma_\gamma} V^* \xrightarrow{f^*} V^* \xrightarrow{\Gamma_\gamma^{-1}} V$$

und wird ebenfalls mit $f^*\colon V \to V$ bezeichnet. Der Endomorphismus f heißt *selbstadjungiert* (s.a.), wenn $f = f^*$ gilt.

Lemma 4.48.

(i) Die Adjungierte $f^* \in \mathrm{End}(V)$ ist durch die Eigenschaft

$$\gamma(v, f^*(w)) = \gamma(f(v), w) \quad \text{für alle } v, w \in V$$

eindeutig bestimmt.

(ii) Wird f bzgl. einer ONB $(v_1, \dots, v_n)$ durch die Matrix G dargestellt, so wird f^* bzgl. dieser Basis durch G^* dargestellt. Es ist f genau dann selbstadjungiert, wenn G symmetrisch ist.

Beweis.
(i): Sei $g\colon V^* \to V^*, \quad \ell \mapsto \ell \circ f$ die duale Abbildung. Dann gilt für $w \in V$

$$\Gamma_\gamma(f^*(w)) = g(\Gamma_\gamma(w)) = \Gamma_\gamma(w) \circ f.$$

Also gilt für $v \in V$

$$\gamma(v, f^*(w)) = \Gamma_\gamma(f^*(w))(v) = (\Gamma_\gamma(w))(f(v)) = \gamma(f(v), w).$$

Ist $h \in \mathrm{End}_K(V)$ eine weitere Abbildung mit dieser Eigenschaft so gilt für alle $v \in V$

$$\begin{aligned}\gamma\Big(h(v) - f^*(v), h(v) - f^*(v)\Big) = \\ \gamma\Big(h(v) - f^*(v), h(v)\Big) - \gamma\Big(h(v) - f^*(v), f^*(v)\Big) \\ = \gamma\Big(f(h(v) - f^*(v)), v\Big) - \gamma\Big(f(h(v) - f^*(v)), v\Big) = 0,\end{aligned}$$

also $h(v) - f^*(v) = 0$. Dies zeigt die Eindeutigkeit.
(ii): Sei $(v_1, \dots, v_n)$ eine ONB, G die Darstellungsmatrix von f. Dann gilt

$$\begin{aligned}M^{v_1,\dots,v_n}_{v_1^*,\dots,v_n^*}(\Gamma_\gamma) &= E_n \\ M^{v_1^*,\dots,v_n^*}_{v_1^*,\dots,v_n^*}(g) &= G^t \\ M^{v_1,\dots,v_n}_{v_1,\dots,v_n}(f^*) &= E_n^{-1} G^t E_n = G^t.\end{aligned}$$

Ist $f = f^*$, so folgt $G = G^t$ und umgekehrt.

□

Lemma 4.49. *Sei (V, γ) ein euklidischer Raum mit Orthonormalbasis $(v_1, \dots, v_n)$. Ist $f \in \mathrm{End}_{\mathbb{R}}(V)$ selbstadjungiert, so ist*

$$\gamma'\colon V \times V \to \mathbb{R}, \quad (v, w) \mapsto \gamma(v, f(w))$$

eine symmetrische Bilinearform und es gilt

$$\varphi_{v_1,\dots,v_n}(\gamma') = M^{v_1,\dots,v_n}_{v_1,\dots,v_n}(f).$$

Die Abbildung

$$\alpha\colon \{f \in \mathrm{End}_{\mathbb{R}}(V) | f = f^*\} \to \{\gamma' \in \mathrm{Bil}(V) | \gamma' = (\gamma')^*\}, \quad f \mapsto \gamma(\cdot, f(\cdot))$$

ist ein linearer Isomorphismus.

Beweis.
γ' ist symmetrisch: Sei $x, y \in V$. Dann gilt

$$\gamma'(x,y) = \gamma(x, f(y)) \overset{f \text{ s.a.}}{=} \gamma(f(x), y) \overset{\gamma=\gamma^*}{=} \gamma(y, f(x)) = \gamma'(x,y).$$

Sei $A = (a_{ij})$ die Darstellungsmatrix von f bezüglich $(v_1, \ldots, v_n)$. Dann gilt

$$\gamma'(v_i, v_j) = \gamma(v_i, \sum_{k=1}^{n} a_{kj} v_k) = \sum_{k=1}^{n} a_{kj} \gamma(v_i, v_k) = a_{ij}.$$

Also gilt $\varphi_{v_1,\ldots,v_n}(\gamma') = A$.

Sei umgekehrt $\gamma' \colon V \times V \to \mathbb{R}$ eine symmetrische Bilinearform. Setze

$$f \colon V \xrightarrow{\Gamma_{\gamma'}} V^* \xrightarrow{\Gamma_\gamma^{-1}} V.$$

Dann gilt für $y \in V$

$$\Gamma_\gamma(f(y)) = \Gamma_{\gamma'}(y)$$

und somit für $x \in V$

$$\gamma(x, f(y)) = \Gamma_\gamma(f(y))(x) = \Gamma_{\gamma'}(y)(x) = \gamma'(x,y).$$

Damit folgt auch

$$\gamma(x, f(y)) = \gamma'(x,y) = \gamma'(y,x) = \gamma(y, f(x)) = \gamma(f(x), y).$$

Also ist $f = f^*$ und $\alpha(f) = \gamma'$. Die Linearität von α ist klar. □

Lemma 4.50. *Sei f selbstadjungiert. Eigenvektoren zu unterschiedlichen Eigenwerten von f sind orthogonal.*

Beweis. Seien $v, w \in V$ Eigenvektoren zu den Eigenwerten $\lambda \neq \mu$. Dann gilt

$$\lambda \langle v, w \rangle = \langle f(v), w \rangle = \langle v, f(w) \rangle = \mu \langle v, w \rangle,$$

Also $\langle v, w \rangle = 0$. □

Theorem 4.51 (Spektralsatz für selbstadjungierte Operatoren)**.** *Sei (V, γ) ein euklidischer Raum und $f \in \mathrm{End}(V)$ ein selbstadjungierter Endomorphismus. Dann gibt es eine ONB von V aus Eigenvektoren von f.*

Algorithmus:

1. Bestimme zu jedem Eigenwert λ eine Basis des Eigenraums $V_\lambda = \ker(\lambda \mathrm{id} - f)$.

2. Wende Gram-Schmidt an, um daraus eine ONB zu machen.

3. Weil f nach 4.51 diagonalisierbar ist und nach 4.50 gilt $V = \hat{\bigoplus} V_\lambda$. Die ONB der Eigenräume bilden zusammen also eine ONB von V.

Für den Beweis des Spektralsatzes starten wir mit zwei Lemmata:

Erinnerung: Für $z = x + iy \in \mathbb{C}$ ist $\overline{z} = x - iy$ die *konjugiert komplexe* Zahl zu z.

Notation: Für $A = (a_{ij}) \in M_{m,n}(\mathbb{C})$ schreiben wir $\overline{A} = (\overline{a_{ij}})$, $A^* = \overline{A}^t$.

Lemma 4.52. *Sei $A = (a_{ij}) \in M_{n,n}(\mathbb{C})$. Gilt $A = A^*$, so gilt*

$$\chi_A(t) = (t - \lambda_1) \cdots (t - \lambda_n)$$

mit $\lambda_i \in \mathbb{R}$.

Beweis. Über $\mathbb{C}$ zerfällt χ_A in Linearfaktoren, d.h.

$$\chi_A(t) = (x - \lambda_1) \dots (x - \lambda_n),\ \lambda_i \in \mathbb{C}.$$

Sei $\lambda = \lambda_i$.
Für $v = (v_i) \in \mathbb{C}^n \setminus \{0\}$ ist

$$v^t \overline{v} = \sum_{i=1}^{n} v_i \overline{v_i} = \sum_{i=1}^{n} |v_i|^2$$

reell und größer 0.

Ist nun $v \in \mathbb{C}^n \setminus \{0\}$ ein Eigenvektor zu λ so gilt

$$\begin{aligned} \lambda \cdot v^t \overline{v} = (\lambda v)^t \overline{v} = (Av)^t \overline{v} = v^t A^t \overline{v} = v^t \overline{A} \overline{v} \\ = v^t \overline{Av} = z^t \cdot \overline{Az} = v^t \overline{\lambda v} = \overline{\lambda} v^t \overline{v}. \end{aligned}$$

Wegen $v^t \overline{v} > 0$ folgt $\lambda = \overline{\lambda}$, also $\lambda \in \mathbb{R}$. □

Lemma 4.53. *Sei f s.a. Ist U ein Untervektorraum mit $f(U) \subset U$, so gilt $f(U^\perp) \subset U^\perp$.*

Beweis. Sei $v \in U^\perp$. Dann gilt für alle $u \in U$: $\langle u, f(v) \rangle = \langle f(u), v \rangle = 0$. Also $f(v) \in U^\perp$. □

Beweis von Theorem 4.51. Da die Darstellungsmatrix $A \in M_{n,n}(\mathbb{R}) \subset M_{n,n}(\mathbb{C})$ von f bezüglich einer Orthonormalbasis von (V, γ) symmetrisch ist, folgt aus 4.52, dass χ_f über $\mathbb{R}$ in Linearfaktoren zerfällt.
Induktion über $\dim V$:
Anfang: $\dim V = 1$ trivial.
Schritt: Sei $n = \dim V \geq 2$. Sei $\lambda \in \mathbb{R}$ ein EW von f und $v_1 \neq 0$ ein Eigenvektor, d. h. $f(v_1) = \lambda v_1$. Ersetzt man v_1 durch $\frac{v_1}{\|v_1\|}$, so hat man $\|v_1\| = 1$. Sei $U = \mathbb{R} v_1$. Dann gilt $f(U) \subset U$ und $f(U^\perp) \subset U^\perp$ (4.53). Nun gilt $V = U \oplus U^\perp$ (4.36) und $\dim U^\perp = n - 1$. Ist $(v_2, \dots, v_n)$ eine ONB von $U^\perp$ aus Eigenvektoren zu f, so ist $(v_1, \dots, v_n)$ die gesuchte ONB. □

Korollar 4.54. *Sei (V, γ) ein euklidischer Raum und $\gamma' \colon V \times V \to \mathbb{R}$ eine symmetrische Bilinearform. Dann gibt es eine ONB von (V, γ) die OB für (V, γ') ist, d.h. bezüglich derer die Fundamentalmatrix von γ' Diagonalgestalt hat.*

Beweis. Sei $f \colon V \to V$ der nach 4.49 eindeutig bestimmte s.a. Endomorphismus mit $\gamma'(x, y) = \gamma(f(x), y)$. Und sei $(v_1, \ldots, v_n)$ eine ONB von V aus Eigenwerten von f. Gilt $f(v_i) = \lambda_i v_i$, so gilt $\gamma'(v_i, v_j) = \gamma(\lambda_i v_i, v_j) = \lambda_i \gamma(v_i, v_j) = \lambda_i \delta_{ij}$ □

Korollar 4.55. *Sei*

$$f \colon \mathbb{R}^n \to \mathbb{R}, \qquad x \mapsto \sum_{i=1}^{n} (a_{ii} x_i^2 + 2 \sum_{j=i+1}^{n} a_{ij} x_i x_j)$$

eine quadratische Form. Dann gibt es eine Isometrie α des euklidischen Raums $\mathbb{R}^n$ so dass

$$f \circ \alpha(x) = \sum_{i=1}^{n} \lambda_i x_i^2.$$

Beweis. Wende 4.54 auf $\gamma_f(x, y) = \frac{1}{2}(f(x + y) - f(x) - f(y))$ an. □

In Matrizen lesen sich diese Ergebnisse so

Satz 4.56 (Hauptachsentransformation)**.** *Ist G eine symmetrische reelle $n \times n$-Matrix mit Eigenwerten $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$, so existiert ein $T \in SO(n)$, so dass*

$$TGT^{-1} = \operatorname{diag}(\lambda_1, \ldots, \lambda_n).$$

Beweis. Wir betrachten den $\mathbb{R}^n$ mit dem Standardskalarprodukt. Die symmetrische Matrix G definiert einen s.a. Endomorphismus $f \colon \mathbb{R}^n \to \mathbb{R}^n$. Ist $(v_1, \ldots, v_n)$ eine ONB des $\mathbb{R}^n$ aus Eigenvektoren von f wie in 4.51 und T die Transformationsmatrix von $(e_1, \ldots, e_n)$ nach $(v_1, \ldots, v_n)$, so gilt $T \in O(n)$. Ersetzt man, falls nötig, v_1 durch $-v_1$, gilt sogar $T \in SO(n)$. Bzgl. $(v_1, \ldots, v_n)$ hat f die Darstellungsmatrix

$$TGT^{-1} = \operatorname{diag}(\lambda_1, \ldots, \lambda_n).$$

□

Korollar 4.57. *Eine symmetrische Matrix P ist genau dann positiv definit, wenn alle Eigenwerte von P positiv sind.*

Beweis. Sei $T \in SO(n)$ mit $TGT^{-1} = TGT^t = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$. Dann ist T positiv definit genau dann, wenn TGT^t positiv definit ist. Die Hauptminoren von TGT^t sind

$$\lambda_1, \lambda_1\lambda_2, \ldots, \lambda_1 \cdots \lambda_n$$

Diese sind genau dann alle positiv, wenn alle λ_i positiv sind. Genau dann ist nach dem Hauptminorenkriterium auch T positiv definit. □

4.7 Unitäre Räume

Definition 4.58. Eine Abbildung $f\colon V \to W$ von $\mathbb{C}$-Vektorräumen heißt *semilinear* (bezüglich der komplexen Konjugation), wenn für $u, v \in V$, $\alpha, \beta \in \mathbb{C}$

$$f(\alpha u + \beta v) = \overline{\alpha} f(u) + \overline{\beta} f(v).$$

Bemerkungen.

(i) Seien $(v_1, \dots, v_n)$, $(w_1, \dots, w_m)$ Basen von V und W und $f\colon V \to W$ semilinear mit $f(v_j) = \sum_i a_{ij} w_i$. Dann heißt $A = (a_{ij})$ die Darstellungsmatrix von f und das Diagramm

$$\begin{array}{ccc} \mathbb{C}^n & \xrightarrow{z \mapsto \sum z_i v_i} & V \\ {\scriptstyle z \mapsto A\overline{z}}\downarrow & & \downarrow{\scriptstyle f} \\ \mathbb{C}^m & \xrightarrow[z \mapsto \sum z_i w_i]{} & W \end{array}$$

kommutiert. Durch A ist f eindeutig festgelegt.

(ii) Die Komposition von zwei semilinearen Abbildungen ist *linear*. Die Komposition von einer linearen und einer semilinearen Abbildung ist semilinear.

Definition 4.59. Eine Abbildung $\gamma\colon V \times V \to \mathbb{C}$ heißt *Sesquilinearform* („sesqui"=„eineinhalb"), wenn sie linear im ersten Argument und semilinear im zweiten Argument ist, d. h. es gilt für $u, v, w \in V$, $\lambda, \mu \in \mathbb{C}$:

$$\gamma(\lambda u + \mu v, w) = \lambda\gamma(u, w) + \mu\gamma(v, w)$$
$$\gamma(u, \lambda v + \mu w) = \overline{\lambda}\gamma(u, v) + \overline{\mu}\gamma(u, w).$$

Ist $(v_1, \dots, v_n)$ eine Basis von V, so heißt

$$\varphi_{v_1,\dots,v_n}(\gamma) = (\gamma(v_i, v_j))$$

die *Fundamentalmatrix* von γ bezüglich dieser Basis.
Eine Sequilinearform γ heißt *hermitesch* bzw. *antihermitesch*, wenn

$$\gamma(v, w) = \overline{\gamma(w, v)}, \quad \text{bzw} - \overline{\gamma(w, v)}$$

für alle $v, w \in V$ gilt.

Definition 4.60. Für $A = (a_{ij}) \in M_{m,n}(\mathbb{C})$ setzen wir $A^* = \overline{A}^t = (\overline{a_{ji}}) \in M_{n,m}(\mathbb{C})$. Eine Matrix $A \in M_{n,n}(\mathbb{C})$ heißt *hermitesch*, wenn $A = A^*$, *antihermitesch*, wenn $A = -A^*$, *normal*, wenn $A^*A = AA^*$ und *unitär*, wenn $A^* = A^{-1}$. Die Menge der unitären $n \times n$-Matrizen bilden eine Untergruppe $U(n) \subset \mathrm{Gl}_n(\mathbb{C})$, die *unitäre Gruppe vom Rang n*. Die Untergruppe

$$SU(n) = \{A \in U(n) | \det(A) = 1\}$$

heißt *spezielle unitäre Gruppe vom Rang n*.

Bemerkungen. Sei $\gamma\colon V \times V \to \mathbb{C}$ eine Sesquilinearform.

(i) Die Abbildung $\Gamma_\gamma\colon V \to V^*, \quad w \mapsto V \xrightarrow{v\mapsto\gamma(v,w)} \mathbb{C}$ ist semilinear. Umgekehrt ist für jede semilineare Abbildung $f\colon V \to V^*$ die Abbildung $\gamma_f\colon V \times V \to \mathbb{C}, \quad (v,w) \mapsto (f(w))(v)$ eine Sesquilinearform.

(ii) Ist γ hermitesch, so gilt $\gamma(v,v) = \overline{\gamma(v,v)}$, also $\gamma(v,v) \in \mathbb{R}$ für alle $v \in V$.

(iii) Sei $(v_1,\dots,v_n)$ eine Basis von V und $A = \varphi_{v_1,\dots,v_n}(\gamma)$. Dann ist A auch die Darstellungsmatrix von $\Gamma_\gamma\colon V \to V^*$. Es ist γ genau dann hermitesch, wenn A hermitesch ist. Ist $B \in M_{n,n}(\mathbb{C})$, so ist

$$\gamma'\colon V \times V \to \mathbb{C}, \quad \gamma'(\sum_{i=1}^n \lambda_i v_i, \sum_{j=1}^n \mu_j v_j) = \lambda^t B \overline{\mu}$$

eine Sesquilinearform auf V mit $B = \varphi_{v_1,\dots,v_n}(\gamma')$.

(iv) Sowohl hermitesche, antihermitesche als auch unitäre Matrizen A sind normal, reelle (anti-)symmetrische Matrizen sind (anti-)hermitesch, reelle orthogonale Matrizen sind unitär. Ist A hermitesch, so ist iA antihermitesch und umgekehrt.

(v) Die Eigenwerte von (anti-)hermiteschen Matrizen sind nach 4.52 reell (rein imaginär).

Satz 4.61 (Transformationssatz für Sequilinearformen)**.** *Sei V ein n-dimensionaler $\mathbb{C}$-Vektorraum und seien $(v_1,\dots,v_n)$ und $(w_1,\dots,w_n)$ Basen von V. Ist $S = M_{v_1,\dots,v_n}^{w_1,\dots,w_n}(\mathrm{id}_V)$, so gilt*

$$\varphi_{w_1,\dots,w_n}(\gamma) = S^* \varphi_{v_1,\dots,v_n}(\gamma) S,$$

Beweis. Wie 4.4. □

Definition 4.62. Eine hermitesche Form $\gamma\colon V \times V \to \mathbb{C}$ heißt *positiv definit* oder *hermitisches Skalarprodukt*, wenn gilt:

$$\gamma(v,v) > 0 \ \text{ für alle } v \in V,\ v \neq 0.$$

Ein *unitärer Raum* (V,γ) ist ein endlich-dimensionaler $\mathbb{C}$-Vektorraum V mit einem hermiteschen Skalarprodukt $\gamma\colon V \times V \to \mathbb{C}$.
Ein Homomorphismus $f\colon (V,\gamma) \to (W,\gamma')$ unitärer Räume ist eine lineare Abbildung $f\colon V \to W$ mit $\gamma'(f(v),f(w)) = \gamma(v,w)$.
Ist f bijektiv, so heißt f *lineare Isometrie*.

Beispiel. Der Vektorraum $\mathbb{C}^n$ mit dem *Standard-Skalarprodukt*

$$\langle x,y\rangle_{\mathbb{C}^n} = x^t \overline{y}$$

ist ein unitärer Raum.

Definition 4.63. Sei (V, γ) ein unitärer Raum. Die Begriffe *Norm* $\|v\| = \sqrt{\gamma(v,v)}$, *Orthogonalität*, *Orthogonalbasis*, *Orthonormalbasis*, *orthogonale direkte Summe*, *orthogonales Komplement* werden analog zu euklidischen Räumen definiert.

Die Beweise aller folgenden Sätze sind im Wesentlichen die gleichen wie bei euklidischen Vektorräumen.

Satz 4.64. *Ist (V, γ) unitär und $U \subset V$ ein Untervektorraum, so gilt $V = U \hat{\oplus} U^\perp$.*

Beweis. Wie 4.36. □

Satz 4.65. *Sei (V, γ) ein unitärer Raum. Dann gelten für $x, y \in V$:*

(i) Schwarz'sche Ungleichung: $|\langle x, y\rangle| \leq \|x\| \cdot \|y\|$.

(ii) Dreiecksungleichung: $\|x + y\| \leq \|x\| + \|y\|$.

(iii) Polarisierungs-Identität: $\langle x, y\rangle = \frac{1}{4}(\sum_{k=1}^{4} i^k \|x + i^k y\|^2)$.

(iv) Satz des Pythagoras: Gilt $\mathrm{Re}(\langle x, y\rangle) = 0$, *so gilt* $\|x + y\|^2 = \|x\|^2 + \|y\|^2$.

Beweis. (i): Ohne Einschränkung $x \neq 0, y \neq 0$. Dann gilt für $\lambda \in \mathbb{C}$

$$0 \leq \|x - \lambda y\|^2 = \|x\|^2 - \underbrace{\lambda\langle x, y\rangle - \overline{\lambda\langle x, y\rangle}}_{2\,\mathrm{Re}(\lambda\langle x,y\rangle)} + |\lambda|^2\|y\|^2$$

Speziell für $\lambda = \frac{\langle y,x\rangle}{\|y\|^2}$. erhält man

$$\begin{aligned} 0 &\leq \|x\|^2 - 2\,\mathrm{Re}\Big(\frac{\langle y, x\rangle\langle x, y\rangle}{\|y\|^2}\Big) + \frac{|\langle y, x\rangle|^2}{\|y\|^2} \\ &= \|x\|^2 - \frac{|\langle x, y\rangle|^2}{\|y\|^2}. \end{aligned}$$

Also

$$|\langle x, y\rangle|^2 \leq \|x\|^2\|y\|^2.$$

Die Schwarz'sche Ungleichung folgt nach Wurzelziehen.
(ii): Folgt wie im Reellen aus (i).
(iii): Es gilt

$$\begin{aligned} \|x + y\|^2 &= \|x\|^2 + 2\,\mathrm{Re}(\langle x, y\rangle) + \|y\|^2 \\ \|x - y\|^2 &= \|x\|^2 - 2\,\mathrm{Re}(\langle x, y\rangle) + \|y\|^2 \\ \|x + iy\|^2 &= \|x\|^2 + 2\,\mathrm{Im}(\langle x, y\rangle) - \|y\|^2 \\ \|x - iy\|^2 &= \|x\|^2 - 2\,\mathrm{Im}(\langle x, y\rangle) - \|y\|^2 \end{aligned}$$

$$\sum_{k=1}^{4} i^k \|x + i^k y\|^2 = 4(\mathrm{Re}(\langle x, y\rangle) + i\,\mathrm{Im}(\langle x, y\rangle)) = 4\langle x, y\rangle.$$

(iv):

$$0 = 2\,\mathrm{Re}(\langle x, y\rangle) = \|x+y\|^2 - \|x\|^2 - \|y\|^2.$$

□

Satz 4.66. *Jeder unitäre Raum (V, γ) hat eine ONB, d.h. er ist isometrisch zum $\mathbb{C}^n$ mit dem Standard-Skalarprodukt.*

Beweis. Mit dem Gram-Schmidt-Verfahren können wir jede Basis $(v_1, \ldots, v_n)$ zu einer ONB umformen. □

Lemma 4.67. *Sei $G \in M_{n,n}(\mathbb{C})$. Die folgenden Aussagen sind äquivalent:*

(i) $G \in U(n)$,

(ii) $(\mathbb{C}^n, \langle\ ,\ \rangle_{\mathbb{C}^n}) \xrightarrow{G\cdot} (\mathbb{C}^n, \langle\ ,\ \rangle_{\mathbb{C}^n})$ *ist eine Isometrie,*

(iii) Die Spalten von G sind eine Orthonormalbasis von $(\mathbb{C}^n, \langle\ ,\ \rangle_{\mathbb{C}^n})$.

Alle Eigenwerte von unitären Matrizen haben Betrag 1.

Beweis. Seien $v_1, \ldots, v_n$ die Spalten von G. Dann gilt

$$\begin{aligned} G \in U(n) \Leftrightarrow G^t\overline{G} = E_n \Leftrightarrow \forall i,j\colon \langle v_i, v_j\rangle = v_i^t\overline{v_j} = \delta_{ij} \Leftrightarrow (v_1,\ldots,v_n) \text{ ONB} \\ \Leftrightarrow \forall x, y \in \mathbb{C}^n\colon \langle Gx, Gy\rangle = x^tG^t\overline{G}\overline{y} = x^t\overline{y} = \langle x, y\rangle. \end{aligned}$$

Sei nun G unitär und $0 \neq x \in \mathbb{C}^n$ ein Eigenvektor zum Eigenwert λ. Dann gilt

$$|\lambda|^2\|x\|^2 = \|\lambda x\|^2 = \|Gx\|^2 = \|x\|^2.$$

Wegen $\|x\|^2 \neq 0$ folgt $|\lambda| = 1$. □

Satz 4.68 (komplexe Cholesky-Zerlegung)**.** *Ist $G \in M_{n,n}(\mathbb{C})$ hermitesch und positiv definit (d. h. $\langle x, Gx\rangle_{\mathbb{C}^n} > 0$ für $0 \neq x$), so gibt es eine eindeutig bestimmte obere Dreieckmatrix T mit positiv reellen Diagonaleinträgen so dass $G = T^*T$.*

Beweis. Wie 4.38. □

Analog: komplexe QR-Zerlegung $A = QR$ mit $Q \in U(n)$.

Definition 4.69. Sei (V, γ) ein unitärer Raum und $f \in \mathrm{End}(V)$. Dann heißt die lineare Abbildung

$$V \xrightarrow{\Gamma_\gamma} V^* \xrightarrow{f^*} V^* \xrightarrow{\Gamma_\gamma^{-1}} V$$

die *Adjungierte* zu f. Sie wird ebenfalls mit f^* bezeichnet. Wenn $f = f^*$, so heißt f *selbstadjungiert*. Wenn $f^* \circ f = f \circ f^*$, so heißt f normal.

Lemma 4.70.

(i) *Die Adjungierte $f^* \in \mathrm{End}(V)$ ist durch die Eigenschaft*

$$\gamma(v, f^*(w)) = \gamma(f(v), w) \quad \text{für alle } v, w \in V$$

eindeutig bestimmt.

(ii) *Wird f bzgl. einer ONB $(v_1, \dots, v_n)$ durch die Matrix G dargestellt, so wird f^* bzgl. dieser Basis durch G^* dargestellt. Es ist f genau dann selbstadjungiert (normal), wenn G hermitesch (normal) ist.*

Beweis. Wie in 4.48. Hier ein alternativer Beweis für (ii): Sei $(v_1, \dots, v_n)$ eine ONB. Wir berechnen die Darstellungsmatrix von f^*: Sei G die Darstellungsmatrix von f und $g \in \mathrm{End}(V)$ der durch G^* dargestellte Endomorphismus. Dann gilt für $v = \sum x_i v_i, w = \sum y_i v_i \in V$, $x = (x_i), y = (y_i) \in \mathbb{C}^n$:

$$\gamma(v, f^*(w)) = \gamma(f(v), w) = (Gx)^t \overline{y} = x^t G^t \overline{y} = x^t \overline{G^* y} = \gamma(v, g(w))$$

Wegen der Eindeutigkeit von f^* aus (i) folgt $f^* = g$. □

Lemma 4.71. *Sei (V, γ) ein unitärer Raum und $f \in \mathrm{End}(V)$.*

(i) *Ist $U \subset V$ ein Untervektorraum mit $f(U) \subset U$, so gilt $f^*(U^\perp) \subset U^\perp$.*

(ii) *Ist f normal und $v \in V$ ein Eigenvektor von f zum Eigenwert λ, so ist v ein Eigenvektor zu f^* zum Eigenwert $\overline{\lambda}$. Eigenvektoren zu unterschiedlichen Eigenwerten sind orthogonal.*

Beweis.
(i): Sei $v \in U^\perp$. Dann gilt $\gamma(f^*(v), u) = \gamma(v, f(u)) = 0$ für alle $u \in U$, also $f^*(v) \in U^\perp$.

(ii): Sei f normal. Dann gilt für alle $u \in V$, $\mu \in \mathbb{C}$

$$\begin{aligned} \|f(u)\|^2 &= \gamma(u, f^*(f(u))) = \gamma(u, f(f^*(u))) = \|f^*(u)\|^2, \\ \gamma(f(u), \mu u) &= \overline{\mu}\gamma(u, f^*(u)) = \gamma(\overline{\mu}u, f^*(u)) = \overline{\gamma(f^*(u), \overline{\mu}u)} \end{aligned}$$

Sei jetzt $V \in V$ ein Eigenvektor von f zum Eigenwert λ. Dann gilt

$$\begin{aligned} 0 = \|f(v) - \lambda v\|^2 &= \|f(v)\|^2 - 2\,\mathrm{Re}(\langle f(v), \lambda v\rangle) + |\lambda|^2 \|v\|^2 \\ &= \|f^*(v)\|^2 - 2\,\mathrm{Re}(\underbrace{\overline{\langle f(v), \lambda v\rangle}}_{=\gamma(f^*(v), \overline{\lambda} v)}) + |\lambda|^2 \|v\|^2 \\ &= \|f^*(v) - \overline{\lambda} v\|^2. \end{aligned}$$

Also $f^*(v) = \overline{\lambda} v$. Ist w ein Eigenvektor von f zum Eigenwert $\mu \neq \lambda$, so gilt

$$\lambda \langle v, w\rangle = \langle f(v), w\rangle = \langle v, f^*(w)\rangle = \langle v, \overline{\mu} w\rangle = \mu \langle v, w\rangle,$$

also $v \perp w$. □

Satz 4.72 (Spektralsatz für normale Operatoren)**.** *Sei (V,γ) ein unitärer Raum und $f \in \mathrm{End}(V)$ normal. Dann existiert eine ONB von (V,γ) aus Eigenvektoren zu f.*

Beweis. Per Induktion über die Dimension. Der Fall $n = 1$ ist trivial. Sei $n > 1$. Das charakteristische Polynom $\chi_f(t)$ zerfällt über $\mathbb{C}$ in Linearfaktoren, also hat f mindestens einen Eigenwert. Sei λ ein Eigenwert und v ein Eigenvektor zu λ mit $\|v\| = 1$. Sei $L = \mathbb{C} \cdot v$. Dann gilt $f(L) \subset L$ und wegen 4.71.(ii) auch $f^*(L) \subset L$. Wegen 4.71.(i) erhalten wir

$$f(L^\perp) \subset L^\perp \ , \ f^*(L^\perp) \subset L^\perp.$$

Daher induziert f einen normalen Endomorphismus des unitären Raums $(L^\perp, \gamma|_{L^\perp})$, sowie von $(L, \gamma|_L)$. Ist nun $v_2, \ldots, v_n$ eine ONB von $L^\perp$ aus Eigenvektoren zu f (existiert nach Induktionsvoraussetzung), so ist $(v, v_2, \ldots, v_n)$ eine ONB von $V = L \hat{\oplus} L^\perp$ aus Eigenvektoren zu f. □

In Matrizen formuliert sich der Spektralsatz folgendermaßen:

Korollar 4.73. *Ist $A \in M_{n,n}(\mathbb{C})$ normal mit Eigenwerten $\lambda_1, \ldots, \lambda_n$, so existiert eine unitäre Matrix $U \in SU(n)$ so dass*

$$U^* A U = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$$

Diagonalgestalt hat.

Beweis. Ist $(v_1, \ldots, v_n)$ eine ONB des $\mathbb{C}^n$ aus Eigenvektoren von A wie in 4.72 und U die Transformationsmatrix von $(v_1, \ldots, v_n)$ nach $(e_1, \ldots, e_n)$, so gilt $U \in U(n)$. Ersetzt man U durch $U' = U\mathrm{diag}(\overline{\det(U)}, 1, \ldots, 1)$ so gilt $U' \in SU(n)$ und

$$(U')^* A U' = U^* A U = \mathrm{diag}(\lambda_1, \ldots, \lambda_n).$$

□

Korollar 4.74 (Normalform reeller normaler Matrizen)**.** *Sei $A \in M_{n,n}(\mathbb{R})$ eine reelle normale Matrix (d. h. $A^t A = A A^t$) mit reellen Eigenwerten $\rho_1, \ldots, \rho_p$ und Paaren von komplexen Eigenwerten $\lambda_1, \overline{\lambda}_1, \ldots, \lambda_q, \overline{\lambda}_q$, $p + 2q = n$ als Matrix über $\mathbb{C}$. Dann existiert $T \in SO(n)$ so dass*

$$T^t A T = \begin{pmatrix} \rho_1 & & & & & & \\ & \ddots & & & & & \\ & & \rho_p & & & & \\ & & & J_{\lambda_1} & & & \\ & & & & \ddots & & \\ & & & & & J_{\lambda_q} \end{pmatrix}, \qquad J_{\lambda_s} = \begin{pmatrix} \mathrm{Re}(\lambda_s) & -\mathrm{Im}(\lambda_s) \\ \mathrm{Im}(\lambda_s) & \mathrm{Re}(\lambda_s) \end{pmatrix}.$$

Beweis. Sei

$$\begin{aligned}
V_{\rho_s} &= \ker(\mathbb{R}^n \xrightarrow{A-\rho_s E} \mathbb{R}^n) && \text{(reeller Eigenraum)}\\
V_{\mathbb{C},\rho_s} &= \ker(\mathbb{C}^n \xrightarrow{A-\rho_s E} \mathbb{C}^n) && \text{(komplexer Eigenraum)}\\
V_{\mathbb{C},\lambda_s},\quad & V_{\mathbb{C},\overline{\lambda_s}} && \text{ebenso}\\
V_{\lambda_s,\overline{\lambda}_s} &= \ker(\mathbb{R}^n \xrightarrow{A^2-2\operatorname{Re}(\lambda)A+|\lambda_s|^2E})\mathbb{R}^n && \text{(gemeinsamer reeller Eigenraum)}
\end{aligned}$$

Dann gilt

$$\begin{aligned}
V_{\rho_s} &= V_{\mathbb{C},\rho_s} \cap \mathbb{R}^n\\
V_{\mathbb{C},\lambda_s} + V_{\mathbb{C},\overline{\lambda}_s} &= \ker(\mathbb{C}^n \xrightarrow{A^2-2\operatorname{Re}(\lambda)A+|\lambda_s|^2E} \mathbb{C}^n) = \ker(\mathbb{C}^n \xrightarrow{(A-\lambda_s E)(A-\overline{\lambda_s}E)})\mathbb{C}^n\\
V_{\lambda_s,\overline{\lambda}_i} &= (V_{\mathbb{C},\lambda_s} + V_{\mathbb{C},\overline{\lambda_s}}) \cap \mathbb{R}^n
\end{aligned}$$

Ferner ist

$$V_{\mathbb{C},\lambda_s} \to V_{\mathbb{C},\overline{\lambda}_s}, \quad v \mapsto \overline{v}$$

ein semilinearer Isomorphismus: Ist $v \in V_{\mathbb{C},\lambda_s}$, so gilt

$$\overline{\lambda_s}\overline{v} = \overline{\lambda_s v} = \overline{A}\overline{v} = A\overline{v}$$

also $\overline{v} \in V_{\mathbb{C},\overline{\lambda}_s}$. Umgekehrt gilt das genauso. Außerdem gilt

$$\begin{aligned}
\dim_{\mathbb{R}} V_{\rho_s} &= r(A-\rho_s E) = \dim_{\mathbb{C}} V_{\mathbb{C},\rho_s}\\
\dim_{\mathbb{R}} V_{\lambda_s,\overline{\lambda}_s} &= r(A^2 - 2\operatorname{Re}(\lambda)A + |\lambda|^2 E) = \dim_{\mathbb{C}} V_{\mathbb{C},\lambda_s} + \dim_{\mathbb{C}} V_{\mathbb{C},\overline{\lambda}_s} = 2\dim_{\mathbb{C}} V_{\mathbb{C},\lambda_s},
\end{aligned}$$

denn der Rang einer Matrix ändert sich nicht, wenn man den Körper vergrössert (siehe z. B. 2.40 und 2.41). Also ist jede Basis des $\mathbb{R}$-Vektorraums V_{ρ_s} auch eine Basis des $\mathbb{C}$-Vektorraums $V_{\mathbb{C},\rho_s}$. Dasselbe gilt auch für ONB und mit Gram-Schmidt können wir uns eine solche konstruieren.
Sei nun $(v_1,\dots,v_t)$ eine $\mathbb{C}$-ONB von $V_{\mathbb{C},\lambda_s}$. Dann ist $(\overline{v_1},\dots,\overline{v_t})$ eine ONB von $V_{\mathbb{C},\overline{\lambda}_s}$ und $\langle v_k, \overline{v_\ell}\rangle = 0$ für *alle* k,ℓ, weil es sich um Eigenvektoren zu verschiedenen Eigenwerten handelt. Setze

$$\left.\begin{aligned}
\tilde{w}_k &= \tfrac{1}{2}(v_k + \overline{v_k}) = \operatorname{Re}(v_k) \neq 0,\\
\tilde{w}'_k &= \tfrac{i}{2}(\overline{v_k} - v_k) = \operatorname{Im}(v_k) \neq 0,
\end{aligned}\right\} \quad \text{(wegen } V_{\mathbb{C},\lambda_s} \cap V_{\mathbb{C},\overline{\lambda}_s} = 0\text{)}$$

$$w_k = \frac{\tilde{w}_k}{\|\tilde{w}_k\|}, \quad w'_k = \frac{\tilde{w}'_k}{\|\tilde{w}'_k\|}.$$

Dann gilt $w_k, w'_k \in V_{\lambda_s,\overline{\lambda}_s}$ und für $k \neq \ell$:

$$\begin{aligned}
&\langle w_k, w_\ell\rangle = (\text{Skalar})\langle v_k + \overline{v}_k, v_\ell + \overline{v}_\ell\rangle = 0,\\
&\langle w_k, w'_\ell\rangle = 0 \quad \text{ebenso},\\
&\langle w_k, w'_k\rangle = (\text{Skalar})\langle v_k + \overline{v}_k, i(\overline{v}_k - v_k)\rangle = (\text{Skalar})(-i\underbrace{\|v_k\|^2}_{=1} + i\underbrace{\|\overline{v}_k\|^2}_{=1}) = 0.
\end{aligned}$$

Nach Lemma 4.34 ist damit $(w_1, w_1', \ldots, w_t, w_t')$ eine ONB von $V_{\lambda_s,\overline{\lambda}_s}$ und es gilt

$$\begin{aligned} Aw_k &= \frac{1}{2\|\tilde{w}_k\|}(Av_k + A\overline{v}_k) = \frac{1}{2\|\tilde{w}_k\|}(\lambda_s v_k + \overline{\lambda_s v_k}) \\ &= \frac{1}{2\|\tilde{w}_k\|}(\operatorname{Re}(\lambda_s)\operatorname{Re}(v_k) - \operatorname{Im}(\lambda_s)\operatorname{Im}(v_k)) = \operatorname{Re}(\lambda_s)w_k - \operatorname{Im}(\lambda_s)w_k'. \end{aligned}$$

Analog:

$$Aw_k' = \operatorname{Im}(\lambda_s)w_k + \operatorname{Re}(\lambda_s)w_k'.$$

Da die Räume $V_{\mathbb{C},\rho_i}$, $V_{\mathbb{C},\rho_j}$, $V_{\mathbb{C},\lambda_k} + V_{\mathbb{C},\overline{\lambda}_k}$, $V_{\mathbb{C},\lambda_\ell} + V_{\mathbb{C},\overline{\lambda}_\ell}$ für $\rho_i \neq \rho_j$ und $\lambda_k \neq \lambda_\ell$, $\lambda_k \neq \overline{\lambda}_\ell$ paarweise orthogonal sind, gilt dies auch für ihre Durchschnitte mit $\mathbb{R}^n$. Alle ONB zusammen ergeben deshalb eine ONB ω von $\mathbb{R}^n$. Sei T die Transformationsmatrix von ω nach e. Dann gilt $T \in O(n)$ und T^tAT hat die gewünschte Gestalt.
Falls $T \notin SO(n)$ und $p > 0$ ersetze einen Vektor der ONB von V_{ρ_1} durch sein Negatives. Falls $p = 0$ vertausche w_1 und w_1' in der ONB von $V_{\lambda_1,\overline{\lambda}_1}$. Danach gilt $T \in SO(n)$. □

Beispiele.

$$A \in O(n) \quad \Rightarrow \quad \rho_k = \pm 1, \qquad E_{\lambda_k} = \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix}, \quad \lambda_k = e^{i\varphi}.$$

$$A = -A^t \quad \Rightarrow \quad \rho_k = 0, \qquad E_{\lambda_k} = \begin{pmatrix} 0 & -y \\ y & 0 \end{pmatrix}, \quad \lambda_k = iy, \quad y \neq 0$$

5 Multilineare Algebra

5.1 Multilineare Abbildungen und Tensorprodukte

Sei R ein kommutativer Ring.

Definition 5.1. Seien M, N, P R-Moduln. Eine Abbildung $f\colon M \times N \to P$ heißt (R-) *bilinear*, wenn

(i) für jedes $m \in M$ ist die Abbildung $N \to P$, $n \mapsto f(m,n)$ R-linear.

(ii) für jedes $n \in N$ ist die Abbildung $M \to P$, $m \mapsto f(m,n)$ R-linear.

Wir schreiben $\mathrm{Bil}_R(M, N; P)$ für die Menge der bilinearen Abbildungen von $M \times N$ nach P.

Bemerkungen.

(i) $\mathrm{Bil}_R(M, M; R)$ ist die Menge der Bilinearformen auf M.

(ii) $\mathrm{Bil}_R(M, N; P)$ wird zu einem R-Modul durch $(rf)(m,n) = r(f(m,n))$, $(f+g)(m,n) = f(m,n) + g(m,n)$ für $f, g \in Bil_R(M, N; P)$, $r \in R$, $m \in M$, $n \in N$.

(iii) Sind $\alpha\colon M' \to M$, $\beta\colon N' \to N$, $\gamma\colon P \to P'$ R-linear, so ist

$$\mathrm{Bil}_R(M, N; P) \to \mathrm{Bil}_R(M', N'; P'), \quad f \mapsto \gamma \circ f \circ (\alpha \times \beta)$$
$$\text{mit } \gamma \circ f \circ (\alpha \times \beta)\colon M' \times N' \to P', (m', n') \mapsto \gamma(f(\alpha(m'), \beta(n')))$$

ebenfalls R-linear.

Allgemeiner:

Definition 5.2. Sei $(M_i)_{i \in I}$ eine Familie von R-Moduln, P ein R-Modul. Eine Abbildung

$$f\colon \prod_{i \in I} \to P$$

heißt *R-multilinear*, wenn sie in jedem Argument R-linear ist.

Ziel: Beschreibung multilinearer Abbildungen mittels linearer Abbildungen.

Satz 5.3. *Seien M, N, P R-Moduln. Die natürliche Abbildung*

$$\Psi\colon \mathrm{Hom}_R(N, \mathrm{Hom}_R(M, P)) \to \mathrm{Bil}_R(M, N; P) \quad \phi \mapsto f_\phi$$
$$\textit{mit } f_\phi\colon M \times N \to P, \quad (m,n) \mapsto (\phi(n))(m))$$

ist ein R-linearer Isomorphismus.

Beweis. Bilinearität von f_ϕ: $\phi(n)$ ist für jedes n linear und für $m \in M$, $n, n' \in N$, $r \in R$ gilt:

$$\begin{aligned} f_\phi(m, n + rn') &= \phi(n + rn')(m) = (\phi(n) + r\phi(n'))(m) \\ &= (\phi(n))(m) + r(\phi(n'))(m) = f_\phi(m, n) + r f_\phi(m, n'). \end{aligned}$$

R-Linearität vom Ψ: Standard.
Bijektivität: Sei $f\colon M \times N \to P$ bilinear, $n \in N$. Setze

$$\Gamma_f(n)\colon M \to P, \quad m \mapsto f(m, n).$$

Dann gilt $\Gamma_f(n) \in \mathrm{Hom}_R(M, P)$ wegen der Linearität von f im 2. Argument. Die Zuordnung $\Gamma_f\colon N \to \mathrm{Hom}_R(M, P), \quad n \mapsto \Gamma_f(n)$ ist linear, denn für $m \in M$, $n, n' \in N$, $r \in R$ gilt

$$(\Gamma_f(n + rn'))(m) = f(m, n + rn') = f(m, n) + r f(m, n') = (\Gamma_f(n) + r\Gamma_f(n'))(m).$$

und $\Gamma\colon \mathrm{Bil}_R(M, N; P) \to \mathrm{Hom}_R(N, \mathrm{Hom}_R(M, P)), \quad f \mapsto \Gamma_f$ ist die Inverse zu Ψ. □

Satz 5.4. *Seien R-Moduln M, N gegeben. Es gibt ein Paar (T, g) bestehend aus einem R-Modul T und einer bilinearen Abbildung $g\colon M \times N \to T$ mit folgender Universaleigenschaft:*

„Zu jedem R-Modul P und jeder bilinearen Abbildung $f\colon M \times N \to P$ existiert ein eindeutig bestimmter R-Modulhomomorphismus $h : T \to P$, so dass $f = h \circ g$ gilt."

Beweis. Sei

$$C = \{ \sum_{(m,n) \in M \times N} a_{m,n}(m, n) | a_{m,n} \in R, \text{ fast alle gleich } 0\} = R^{(M \times N)}$$

d. h. Elemente von C sind formale endliche R-Linearkombinationen von Elementen aus $M \times N$. Wir betrachten den Untermodul D von C, der durch alle Elemente der Form

$$(rm + m', sn + n') - rs(m, n) - r(m, n') - s(m', n) - (m', n')$$

für $m, m' \in M, n, n' \in N, r, s \in R$ erzeugt wird und setzen $T = C/D$. Wir bezeichnen das Bild von $1 \cdot (m, n) \in C$ in T mit $m \otimes n$. Dann ist T durch Elemente der Form $m \otimes n$ erzeugt, und diese erfüllen:

$$(rm + m') \otimes (sn + n') = rs(m \otimes n) + r(m \otimes n') + s(m \otimes n) + (m' \otimes n')$$

Insbesondere ist die Abbildung

$$g\colon M \times N \to T, \qquad (m, n) \mapsto m \otimes n$$

bilinear.
Ist nun $f : M \times N \to P$ eine bilineare Abbildung, so erhalten wir eine natürliche R-lineare Abbildung

$$\bar{f}\colon C \to P, \qquad \sum_{(m,n)\in M\times N} a_{m,n}(m,n) \mapsto \sum_{(m,n)\in M\times N} a_{m,n} f(m,n)$$

Es gilt

$$\begin{aligned}\bar{f}((rm+m', sn+n') - rs(m,n) - r(m,n') - s(m',n) - (m',n')) = \\ f(rm+m', sn+n') - rsf(m,n) - rf(m,n') - sf(m',n) - f(m',n') = 0.\end{aligned}$$

Also verschwindet $\bar{f}$ auf den Erzeugern von D und daher auf ganz D. Nach dem Homomorphiesatz induziert $\bar{f}$ einen wohldefinierte Homomorphismus $h : C/D = T \to P$ mit

$$h(g(m,n)) = h(m \otimes n) = \bar{f}((m,n)) = f(m,n).$$

Da die Elemente $m \otimes n$ den R-Modul T erzeugen, ist der Homomorphismus h durch diese Eigenschaft eindeutig bestimmt. □

Definition 5.5. Der R-Modul $T = M \otimes_R N$ heißt *Tensorprodukt* von M und N. Die Elemente in T der Form $g(m,n) = m \otimes n$ heißen *Elementartensoren*.

Bemerkungen.

(i) Die Universaleigenschaft ist äquivalent zu:

$$\mathrm{Hom}_R(T,P) \to \mathrm{Bil}_R(M,N;P), \qquad h \mapsto h \circ g$$

ist ein R-linearer Isomorphismus.

(ii) (T,g) ist eindeutig bis auf kanonische Isomorphie: Ist (T',g') ein weiteres Paar mit obiger Universaleigenschaft, so gibt es nach der Universaleigenschaft für (T,g) eine eindeutige R-lineare Abbildung $h\colon T \to T'$ mit $g' = h \circ g$. Andersrum gibt es auch eine eindeutige R-lineare Abbildung $h'\colon T' \to T$ mit $g = h' \circ g'$. Nun gilt $h \circ h' \circ g' = g'$. Wegen der Eindeutigkeitsbedingung in der Universaleigenschaft folgt $h \circ h' = \mathrm{id}_{T'}$. Analog folgt $h' \circ h = \mathrm{id}_T$.

(iii) Nicht jedes Element von $M \otimes N$ ist ein Elementartensor. Die Elemente von $M \otimes N$ sind endliche Summen $\sum_{i=1}^{r} m_i \otimes n_i$, die man nicht immer weiter vereinfachen kann.

(iv) Für $m \in M$ gilt $m \otimes 0 = 0$ in $M \otimes N$ wegen $m \otimes 0 = m \otimes (0+0) = m \otimes 0 + m \otimes 0$. Analog $0 \otimes n = 0$ für $n \in N$.

(v) Ist $(m_i)_{i\in I}$ ein Erzeugendensystem von M und $(n_j)_{j\in J}$ ein Erzeugendensystem von N, so ist

$$(m_i \otimes n_j)_{i\in I, j\in J}$$

ein Erzeugendensystem von $M \otimes N$: Da die Elementartensoren $m \otimes n$ ein Erzeugendensystem bilden, reicht es, jeden Elementartensor als Linearkombination der $m_i \otimes n_j$ darzustellen. Sei $m = \sum_i r_i m_i$, $n = \sum_j s_j n_j$. Dann gilt

$$m \otimes n = \sum_i \sum_j r_i s_j m_i \otimes n_j.$$

Insbesondere ist das Tensorprodukt endlich erzeugter R-Moduln wieder endlich erzeugt.

(vi) Die konkrete Konstruktion des Tensorprodukts braucht man nur, um die Existenz nachzuweisen. Alle wichtigen Eigenschaften des Tensorprodukts lassen sich aus der Universaleigenschaft ableiten.

(vii) Ganz analog: Ist $(M_i)_{i\in I}$ eine Familie von R-Moduln, so existiert ein bis auf kanonische Isomorphie eindeutiges Tensorprodukt $\bigotimes_{i\in I} M_i$ zusammen mit einer multilinearen Abbildung $g\colon \prod_{i\in I} M_i \to \bigotimes_{i\in I} M_i$, so dass für jeden R-Modul P die Abbildung

$$\mathrm{Hom}_R(\bigotimes_{i\in I} M_i, P) \to \{f\colon \prod_{i\in I} M_i \to P | f \text{ multilinear}\}$$

ein R-linearer Isomorphismus ist. Als R-Modul wird $\bigotimes_{i\in I} M_i$ durch die Elemente $g((m_i)_(i \in I)) = \otimes_{i\in I} m_i$ erzeugt.

Korollar 5.6 (Adjunktionseigenschaft des Tensorprodukts)**.**

$$\begin{aligned} \mathrm{Hom}_R(M \otimes N, P) &\to \mathrm{Hom}_R(N, \mathrm{Hom}_R(M, P)), \qquad h \mapsto \phi_h \\ \textit{mit } \phi_h\colon N &\to \mathrm{Hom}_R(M, P), \qquad n \mapsto \phi_h(n) \\ \textit{mit } \phi_h(n)\colon M &\to P, \qquad m \mapsto h(m \otimes n) \end{aligned}$$

ist ein R-linearer Isomorphismus. (Man sagt, das Tensorprodukt $\cdot \otimes_R N$ ist linksadjungiert zu $\mathrm{Hom}_R(N, \cdot)$*.)*

Beweis. Dies ist gerade die Zusammensetzung des Isomorphismus

$$\mathrm{Hom}_R(M \otimes N, P) \to \mathrm{Bil}_R(M, N; P)$$

mit dem Isomorphismus

$$\mathrm{Bil}_R(M, N; P) \to \mathrm{Hom}_R(N, \mathrm{Hom}_R(M, P))$$

aus Satz 5.3. □

Lemma 5.7. *Seien M, N, P R-Moduln. Dann gibt es eindeutig bestimmte R-Modulisomorphismen*

(i) $\phi_c\colon M \otimes N \xrightarrow{\sim} N \otimes M$ *mit* $\phi_c(m \otimes n) = n \otimes m$,

(ii) $\phi_a\colon (M \otimes N) \otimes P \xrightarrow{\sim} M \otimes (N \otimes P)$ *mit* $\phi_a((m \otimes n) \otimes p) = m \otimes (n \otimes p)$.

(iii) $\phi_d\colon (M \oplus N) \otimes P \xrightarrow{\sim} M \otimes P \oplus N \otimes P$ *mit* $\phi_d((m, n) \otimes p) = (m \otimes p, n \otimes p)$

(iv) $\phi_n\colon R \otimes M \xrightarrow{\sim} M$ *mit* $\phi_n(r \otimes m) = rm$

für $m \in M$, $n \in N$, $p \in P$, $r \in R$.

Beweis. Die Eindeutigkeit folgt dadurch, dass die Abbildungen auf den Elementartensoren vorgegeben sind, und diese das Tensorprodukt erzeugen. Zum Beweis der Existenz müssen wir jeweils eine geeignete bilineare Abbildung konstruieren.
(i) Betrachte $\Phi_c\colon M \times N \to N \otimes M, (m, n) \mapsto n \otimes m$. Φ_c ist offensichtlich bilinear und induziert deshalb nach der universellen Eigenschaft eine R-lineare Abbildung $\phi_c\colon M \otimes N \to N \otimes M$ mit $\phi_c(m \otimes n) = \Phi_c(m, n) = n \otimes m$. Die Inverse von ϕ_c ist die analog konstruierte Abbildung $\phi_c'\colon N \otimes M \to M \otimes N$. Denn $\phi_c' \circ \phi_c(m \otimes n) = m \otimes n$, d. h. auf den durch die Elementartensoren gegebenen Erzeugendensystem stimmt $\phi_c' \circ \phi_c$ mit der Identität überein, also auch auf ganz $M \otimes N$. Analog für $\phi_c \circ \phi_c'$.
(ii) Für jedes $p \in P$ ist $F_p\colon M \times N \to M \otimes (N \otimes P), (m, n) \mapsto m \otimes (n \otimes p)$ bilinear: Es gilt für $n, n' \in N$, $r \in R$:

$$m \otimes (n + rn') \otimes p) = m \otimes (n \otimes p + r(n' \otimes p)) = m \otimes (n \otimes p) + r(m \otimes (n' \otimes p)).$$

Analog: Linearität im 1. Argument. Damit gibt es eine eindeutige R-lineare Abbildung $f_p\colon M \otimes N \to (M \otimes N) \otimes P$ mit $f_p(m \otimes n) = m \otimes (n \otimes p)$. Für $p, p' \in P$ und $r \in R$ gilt dabei

$$f_{p+rp'}(m \otimes n) = m \otimes (n \otimes (p + rp')) = f_p(m \otimes n) + r f_{p'}(m \otimes n)$$

also auch $f_{p+rp'} = f_p + r f_{p'}$. Betrachte nun $\Phi_a\colon M \otimes N \times P \to M \otimes (N \otimes P)(x, p) \mapsto f_p(x)$. Dann ist Φ_a nach eben linear in p und auch linear in x, weil f_p linear ist. Also existiert ϕ_a mit

$$\phi_a((m \otimes n) \otimes p) = \Phi_a(m \otimes n, p) = f_p(m \otimes n) = m \otimes (n \otimes p).$$

Die Inverse läßt sich entsprechend konstruieren.
(iii) Betrachte die bilineare Abbildung

$$\Phi_d\colon (M \oplus N) \times P \to (M \otimes P) \oplus (N \otimes P), \qquad ((m, n), p) \mapsto (m \otimes p, n \otimes p).$$

Diese induziert ϕ_d. Zur Konstruktion der Inversen betrachten wir die bilinearen Abbildungen

$$\Psi_1\colon M \times P \to (M \oplus N) \otimes P, \qquad (m, p) \mapsto ((m, 0) \otimes p)$$
$$\Psi_2\colon N \times P \to (M \oplus N) \otimes P, \qquad (n, p) \mapsto ((0, n) \otimes p)$$

und die induzierten linearen Abbildungen $\psi_1 \colon M \otimes P \to (M \oplus N) \otimes P$ und $\psi_2 \colon N \otimes P \to (M \oplus N) \otimes P$. Setze

$$\psi \colon (M \otimes P) \oplus (N \otimes P) \to (M \oplus N) \otimes P, \qquad (x, y) \mapsto \psi_1(x) + \psi_2(y).$$

Dann gilt

$$\begin{aligned} \phi_d(\psi(m \otimes p, n \otimes p')) &= \phi_d((m,0) \otimes p + (0,n) \otimes p') \\ &= (m \otimes p, 0 \otimes p) + (0 \otimes p', n \otimes p') = (m \otimes p, n \otimes p'), \end{aligned}$$

also $\phi_d \circ \psi = \mathrm{id}$. Andersherum gilt

$$\psi(\phi_d((m,n) \otimes p)) = \psi(m \otimes p, n \otimes p) = (m,0) \otimes p + (0,n) \otimes p = (m,n) \otimes p,$$

also auch $\psi \circ \phi_d = \mathrm{id}$.
(iv) ϕ_n wird induziert von

$$\Phi_n \colon R \times M \to M, \qquad (r, m) \to rm.$$

Die Inverse ist die R-lineare Abbildung

$$\psi \colon M \to R \otimes M, \qquad m \mapsto 1 \otimes m,$$

denn

$$\psi(\phi(r \otimes m)) = 1 \otimes rm = r(1 \otimes m) = r \otimes m, \phi(\psi(m)) = \phi(1 \otimes m) = m.$$

□

Korollar 5.8. *Es gilt*

$$R^m \otimes R^n \cong R^{m \cdot n}$$

Insbesondere ist das Tensorprodukt von zwei endlich erzeugten freien Moduln wieder endlich erzeugt und frei.

Beweis.

$$\begin{aligned} R^m \otimes R^n &= (\underbrace{R \oplus \cdots \oplus R}_{m\text{-mal}}) \otimes (\underbrace{R \oplus \cdots \oplus R}_{n\text{-mal}}) \\ &= \underbrace{(R \otimes R) \oplus \cdots \oplus (R \otimes R)}_{mn\text{-mal}} \\ &= R^{mn}. \end{aligned}$$

□

Bemerkung. Sind M und N freie R-Moduln mit $(x_1, \ldots, x_m)$ und $(y_1, \ldots, y_n)$ als Basen, so folgt, dass

$$(x_1 \otimes y_1, x_1 \otimes y_2, \ldots, x_1 \otimes y_n, \ldots, x_m \otimes y_n)$$

eine Basis von $M \otimes_R N$ ist.

Das Tensorprodukt vertauscht nicht nur mit endlichen, sondern auch mit beliebigen direkten Summen

Lemma 5.9. *Sei $(M_i)_{i\in I}$ eine Familie von R-Moduln und N ein weiterer R-Modul. Dann gibt es einen natürlichen Isomorphismus*

$$\Big(\bigoplus_{i\in I} M_i\Big) \otimes N \cong \bigoplus_{i\in I} M_i \otimes N.$$

Beweis. Den Beweis lassen wir als Übungsaufgabe. □

Korollar 5.10. *Ist M ein R-Modul und I eine Indexmenge, so gilt*

$$(R^{(I)}) \otimes M = M^{(I)}.$$

Beweis. Nach 5.7(iv) gilt $R \otimes M \cong M$. Nach 5.9 folgt

$$(R^{(I)}) \otimes M = \Big(\bigoplus_{i\in I} R\Big) \otimes M \cong \bigoplus_{i\in I} R \otimes M \cong \bigoplus_{i\in I} M = M^{(I)}.$$

□

Sei nun S ein weiterer kommutativer Ring, $f\colon R \to S$ ein Ringhomomorphismus und N ein S-Modul. Vermöge $r \cdot y \overset{df}{=} f(r) \cdot y$ wird N zum R-Modul. Umgekehrt:

Definition 5.11. Sei M ein R-Modul. Dann heißt der S-Modul

$$M_S = S \otimes_R M$$

mit Multiplikation $s(\sum s_i \otimes x_i) = \sum ss_i \otimes x_i$ die *Skalar-Erweiterung von M nach S*.

Lemma 5.12. *Ist M ein endlich erzeugter freier R-Modul vom Rang n, so ist M_S ein endlich erzeugter freier S-Modul vom Rang n.*

Beweis. $M \cong R^n \Rightarrow M_S = S \otimes_R M \cong S \otimes_R R^n = (S \otimes_R R)^n = S^n$. □

Beispiel. Sei $f\colon \mathbb{R} \hookrightarrow \mathbb{C}$ die natürliche Inklusion. Wir können jeden n-dimensionalen $\mathbb{C}$-Vektorraum als $2n$-dimensionalen $\mathbb{R}$-Vektorraum auffassen. Ist V ein $\mathbb{R}$-Vektorraum der Dimension n mit Basis $(v_1, \ldots, v_n)$, so ist $V_{\mathbb{C}}$ ein $\mathbb{C}$-Vektorraum der Dimension n mit Basis $(1 \otimes v_1, \ldots, 1 \otimes v_n)$.

5.2 Funktorialität des Tensorprodukts

Definition/Lemma 5.13. *Seien $f\colon M_1 \to M_2$, $g\colon N_1 \to N_2$ R-lineare Abbildungen. Dann gibt es eine wohldefinierte R-lineare Abbildung*

$$f \otimes g\colon M_1 \otimes N_1 \longrightarrow M_2 \otimes N_2$$

mit $f \otimes g(m \otimes n) = f(m) \otimes g(n)$. Die Abbildung $f \otimes g$ heißt das Tensorprodukt von f und g.

Beweis. Die Abbildung

$$M_1 \times N_1 \to M_2 \otimes N \qquad (m, n) \mapsto f(m) \otimes g(n)$$

ist bilinear. Nach Universaleigenschaft existiert daher die Abbildung $M_1 \otimes N_1 \to M_2 \otimes N_2$ wie beschrieben. □

Lemma 5.14. *Seien R-lineare Abbildungen $f\colon M_1 \to M_2$, $f'\colon M_2 \to M_3$ und $g\colon N_1 \to N_2$, $g'\colon N_2 \to N_3$ gegeben. Dann gilt*

$$(f' \circ f) \otimes (g' \circ g) = (f' \otimes g') \circ (f \otimes g)$$

Insbesondere gilt

$$f \otimes g = (f \otimes \mathrm{id}_{N_2}) \circ (\mathrm{id}_{M_1} \otimes g) = (\mathrm{id}_{M_2} \otimes g) \circ (f \otimes \mathrm{id}_{N_1}.$$

Beweis. Es gilt für $m \in M_1$, $n \in N_2$

$$\begin{aligned}(f' \circ f) \otimes (g' \circ g)(m \otimes n) &= f' \circ f(m) \otimes g' \circ g(n) \\ &= (f' \otimes g')(f(m) \otimes g(n)) \\ &= (f' \otimes g') \circ (f \otimes g)(m \otimes n).\end{aligned}$$

Da die Elementartensoren $M_1 \otimes N_2$ als R-Modul erzeugen, folgt die Aussage. □

Lemma 5.15. *Ist $f\colon M_1 \to N_1$ surjektiv so auch $f \otimes \mathrm{id}_N\colon M_1 \otimes N \to M_2 \otimes N$ für jeden R-Modul N.*

Beweis. Es reicht, Urbilder der Elementartensoren $m \otimes n$ mit $m \in M_2$ und $n \in N$ zu finden, da diese $M_2 \otimes N$ erzeugen. Da f surjektiv ist, gibt es ein $m' \in M_1$ mit $f(m') = m$. Somit gilt $f \otimes \mathrm{id}_N(m' \otimes n) = m \otimes n$. □

Warnung: Ist f injektiv, so braucht das $f \otimes id_N$ nicht zu sein.

Beispiel. Betrachte die injektiven Homomorphismen von $\mathbb{Z}$-Moduln:

$$f : \mathbb{Z} \to \mathbb{Z},\ x \mapsto 2x$$

Dann ist

$$f \otimes \mathrm{id}_{\mathbb{Z}/(2)} : \mathbb{Z} \otimes \mathbb{Z}/(2) \longrightarrow \mathbb{Z} \otimes \mathbb{Z}/(2)$$

die Nullabbildung wegen

$$(f \otimes \mathrm{id})(x \otimes y) = 2x \otimes y = x \otimes 2y = x \otimes 0 = 0$$

für beliebige $x \in \mathbb{Z}$, $y \in \mathbb{Z}/2\mathbb{Z}$.

Lemma 5.16. *Ist $f\colon M_1 \to M_2$ injektiv. Ist N frei, so ist $f \otimes \mathrm{id}_N$ injektiv.*

Beweis. Sei $N = R^{(I)}$ ein freier R-Modul. Dann ist das Diagramm

$$\begin{array}{ccc} M_1 \otimes R^{(I)} & \xrightarrow{f\otimes \mathrm{id}} & M_2 \otimes R^{(I)} \\ {\scriptstyle m\otimes (r_i)_{i\in I} \mapsto (r_i m)_{i\in I}}\downarrow \cong & & \cong \downarrow {\scriptstyle m\otimes (r_i)_{i\in I} \mapsto (r_i m)_{i\in I}} \\ M_1^{(I)} & \xrightarrow{(m_i)_{i\in I} \mapsto (f(m_i))_{i\in I}} & M_2^{(I)} \end{array}$$

kommutativ. Die untere Abbildung ist injektiv, also auch die obere. □

Sei $f\colon M \to N$ eine lineare Abbildung zwischen freien endlich erzeugten R-Moduln und f werde bezüglich Basen $(x_1, \dots, x_n)$, $(y_1, \dots, y_m)$ durch die $m \times n$-Matrix A dargestellt. Mit analogen Bezeichnungen sei $f'\colon M' \to N'$ eine weitere solche Abbildung die bezüglich Basen $(x'_1, \dots, x'_{n'})$, $(y'_1, \dots, y_{m'})$ durch die $m' \times n'$-Matrix A' dargestellt wird.

Definition 5.17. Die, den Homomorphismus $f \otimes f'\colon M \otimes M' \to N \otimes N'$ bezüglich der Basen: $(x_1 \otimes x'_1, \dots, x_1 \otimes x'_{n'}, x_2 \otimes x'_1, x_2 \otimes x'_2 \dots)$ und $(y_1 \otimes y'_1, \dots, y_1 \otimes y'_{m'}$, $y_2 \otimes y'_1, \dots)$ darstellende, $mm' \times nn'$ Matrix heißt das *Tensorprodukt* oder *Kroneckerprodukt* von A und A'.
Bildungsvorschrift: $A = (a_{ij})$, $A' = (a'_{ij})$

$$A \otimes A' = \left(\begin{array}{c|c|c} a_{11}A' & a_{12}A' & \vdots \\ \hline \vdots & \vdots & \vdots \\ \hline a_{m1}A' & \dots & a_{mn}A' \end{array}\right)$$

Beispiel.

$$\begin{pmatrix} 1 & 2 \\ 3 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 2 & 3 \\ 0 & 2 & 1 \end{pmatrix} = \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 2 & 4 & 6 \\ 0 & 2 & 1 & 0 & 4 & 2 \\ \hline 3 & 6 & 9 & 0 & 0 & 0 \\ 0 & 6 & 3 & 0 & 0 & 0 \end{array}\right).$$

5.3 Äußere Potenzen

Definition 5.18. Sei M ein R-Modul und $n \in \mathbb{N}$. Eine *n-fach alternierende Abbildung*

$$g\colon \underbrace{M \times \cdots \times M}_{n\text{-mal}} \longrightarrow N$$

in einen R-Modul N ist eine n-lineare Abbildung mit der Eigenschaft, dass $g(x_1, \ldots, x_n) = 0$ falls $x_i = x_j$ für irgendwelche Indizes $i \neq j$ gilt.

Beispiel. Die Abbildung

$$(R^n)^n \xrightarrow[\cong]{((r_{ij}))\mapsto(r_{ij})} M_{n,n}(R) \xrightarrow{\det} R$$

ist bis auf Multiplikation mit einem Skalar aus R die einzige n-fach alternierende Abbildung auf R^n in R (LA I, Satz 6.17)

Lemma 5.19. *Eine n-fach alternierende Abbildung ist stets antisymmetrisch, d.h. beim Vertauschen zweier Einträge ändert sich das Vorzeichen.*

Beweis. Sei $(x_1, \ldots, x_n) \in M^n$ und $1 \leq i < j \leq n$. Es gilt

$$0 = g(x_1, \ldots, x_i + x_j, \ldots, x_i + x_j, \ldots, n),$$

wobei $x_i + x_j$ an der i-ten und j-ten Stelle steht. Löst man dies linear auf, erhält man

$$\begin{aligned} 0 = {} & g(x_1, \ldots, x_i, \ldots, x_j, \ldots, n) + g(x_1, \ldots, x_j, \ldots, x_i, \ldots, n) \\ & + g(x_1, \ldots, x_i, \ldots, x_i, \ldots, n) + g(x_1, \ldots, x_j, \ldots, x_j, \ldots, n). \end{aligned}$$

Die letzten beiden Summanden sind 0, was die Behauptung zeigt. □

Satz 5.20. *Es gibt ein Paar (A, f) bestehend aus einem R-Modul A und einer n-fach alternierenden Abbildung $f\colon M \times \cdots \times M \to A$ mit folgender Universaleigenschaft:*

„Zu jeder n-fach alternierenden Abbildung $g\colon M \times \cdots \times M \to N$ in einen R-Modul N gibt es einen eindeutig bestimmten R-Modulhomomorphismus $\phi\colon A \to N$ mit $g = \phi \circ f$."

Beweis. Sei $B = M \otimes \cdots \otimes M$ und $H \subset B$ der Untermodul erzeugt von allen Tensoren $x_1 \otimes \cdots \otimes x_n$ mit $x_i = x_j$ für ein $i \neq j$. Setze $A = B/H$, bezeichne das Bild von $x_1 \otimes \cdots \otimes x_n$ in B/H mit $x_1 \wedge \cdots \wedge x_n$ und definiere $f\colon M \times \cdots \times M \to A$ durch

$$f(x_1, \ldots, x_n) = x_1 \wedge \cdots \wedge x_n.$$

Dann ist f eine n-fach alternierende Abbildung.

Ist nun $g\colon M \times \cdots \times M \to N$ eine n-fach alternierende Abbildung, so gibt es nach Universaleigenschaft des Tensorprodukts eine eindeutig bestimmte Abbildung $\psi\colon M \otimes \cdots \otimes M \to N$ mit $\psi(x_1 \cdots x_n) = g(x_1, \ldots, x_n)$ und ψ verschwindet auf H. Dies induziert

$$\phi\colon A \longrightarrow N \quad \text{mit} \quad \phi(x_1 \wedge \cdots \wedge x_n) = g(x_1, \ldots, x_n)$$

in eindeutiger Weise. □

Definition 5.21. A aus 5.20 heißt die *n-te äußere Potenz* von M.
Bezeichnung: $\bigwedge^n M$. Man setzt $\bigwedge^0 M = R$.

Bemerkungen.

(i) Bezeichnen wir den Modul der n-fach alternierenden Abbildungen auf M mit Werten in P mit $\mathrm{Alt}^n(M, P)$, so bedeutet die Universaleigenschaft, dass es einen natürlichen Isomorphismus

$$\mathrm{Alt}^n(M, P) \cong \mathrm{Hom}_R(\bigwedge^n M, P)$$

gibt.

(ii) Das Paar (A, f) ist eindeutig bis auf kanonische Isomorphie: Ist (B, g) ein anderes Paar mit der Universaleigenschaft, so folgt aus der Universaleigenschaft die Existenz eines eindeutigen R-linearen Isomorphismus $\alpha\colon A \to B$ mit $g = \alpha \circ f$.

(iii) $\bigwedge^n(M)$ wird als R-Modul von den Elementen $x_1 \wedge \cdots \wedge x_n$, $x_i \in M$, erzeugt. Es gelten die folgenden Rechenregeln:

$$x_1 \wedge x_2 \wedge \cdots \wedge x_n + x_1' \wedge x_2 \wedge \cdots \wedge x_n) = (x_1 + x_1') \wedge x_2 \wedge \ldots x_n$$

(und an jeder anderen Stelle auch),

$$r(x_1 \wedge \cdots \wedge x_n) = (rx_1) \wedge \cdots \wedge x_n = \cdots = x_1 \wedge x_2 \wedge x_3 \wedge \cdots \wedge (rx_n),$$

sowie $x_1 \wedge \cdots \wedge x_n = 0$ falls $x_i = x_j$ für irgendwelche Indizes $i \neq j$.

Beispiele. (i) $R = \mathbb{Z}$, $M = \mathbb{Z}$, $n = 2$. Es gilt: $\mathbb{Z} \wedge \mathbb{Z} = 0$.

Grund: Ist N eine abelsche Gruppe und $f\colon \mathbb{Z} \times \mathbb{Z} \to N$ eine alternierende Bilinearform, so gilt:

$$f(a, b) = af(1, b) = abf(1, 1) = 0.$$

Daher ist jede 2-fach alternierende Abbildung auf $\mathbb{Z}$ identisch 0, weshalb der Nullmodul die universelle Eigenschaft des äußeren Produkts erfüllt.

(ii) Sei $R = K$ Körper und $M = K^n$. Für den Dualraum von $\bigwedge^n K^n$ gilt

$$(\bigwedge^n K^n)^* = \mathrm{Hom}(\bigwedge^n K^n, K) = \mathrm{Alt}^n(K^n, K).$$

Nun gilt $\mathrm{Alt}^n(K^n, K) = K \det$. Daher ist $\bigwedge^n K^n$ ein K-Vektorraum, dessen Dualraum die Dimension 1 hat. Hieraus folgt $\dim \bigwedge^n K^n = 1$.

Lemma 5.22. *Ist $\sigma\colon \{1, \dots, n\} \to \{1, \dots, n\}$ eine Permutation, so gilt*

$$x_{\sigma(1)} \wedge \cdots \wedge x_{\sigma(n)} = \mathrm{sgn}(\sigma) x_1 \wedge \cdots \wedge x_n.$$

Beweis. Da jede Permutation als Produkt von Transpositionen geschrieben werden kann (LA I, Lemma 6.2) und sgn ein Homomorphismus ist, können wir ohne Einschränkung annehmen, dass $\sigma = (i \quad j)$, $i < j$, eine Transposition ist. Die Abbildung

$$g\colon M^n \to \bigwedge^n(M), \qquad (x_1, \dots, x_n) \mapsto x_1 \wedge \cdots \wedge x_n$$

ist n-fach alternierend und das Signum einer Transposition ist -1. Nach 5.19, angewandt auf g, folgt die Behauptung. □

Notation:
Wir schreiben $\underline{n} = \{1, \dots, n\}$ für die Menge der natürlichen Zahlen kleiner gleich n.
Für eine r-elementige Teilmenge $I = \{i_1 < i_2 < \cdots < i_r\} \subset \underline{n}$ und ein System $x = (x_i)_{i \in \underline{n}}$ von Elementen in M setzen wir

$$x_I = x_{i_1} \wedge \cdots \wedge x_{i_r} \in \bigwedge^r M.$$

Korollar 5.23. *Ist $x = (x_i)_{i \in \underline{n}}$ ein Erzeugendensystem von M, so ist $(x_I)_{I \subset \underline{n}, \sharp I = r}$ ein Erzeugendensystem von $\bigwedge^r M$. Insbesondere gilt $\bigwedge^r M = 0$, falls M ein Erzeugendensystem mit weniger als r Elementen besitzt.*

Beweis. Das System $(x_{i_1} \otimes \cdots \otimes x_{i_r})_{(i_1, \dots, i_r) \in (\underline{n})^r}$ ist ein Erzeugendensystem von

$$\underbrace{M \otimes \cdots \otimes M}_{r},$$

also ist das System der Bilder $(x_{i_1} \wedge \cdots \wedge x_{i_r})_{(i_1, \dots, i_r) \in (\underline{n})^r}$ ein Erzeugendensystem von $\bigwedge^r M$. Nun gilt

$$x_{i_1} \wedge \cdots \wedge x_{i_r} = \begin{cases} 0 & \text{falls } \sharp\{i_1, \dots, i_r\} < r, \\ \mathrm{sgn}(\sigma) x_{\{i_1, \dots, i_r\}} & \text{sonst.} \end{cases}$$

Dabei bezeichnet $\sigma \in S_r$ die eindeutige Permutation mit $i_{\sigma(1)} < i_{\sigma(2)} < \cdots < i_{\sigma(r)}$. Also wird $\bigwedge^r M$ bereits von dem System der x_I für r-elementige Teilmengen $I \subset \underline{n}$ erzeugt. Ist $r > n$, so gibt es keine r-elementigen Teilmengen und damit gilt $\bigwedge^r M = 0$. □

Lemma 5.24. *Sei M ein endlich erzeugter freier R-Modul mit Basis $x = (x_i)_{i\in\underline{n}}$. Sei r eine natürliche Zahl, $1 \leq r \leq n$. Dann gibt es zu jeder r-elementigen Teilmenge $I \subset \underline{n}$ genau eine R-lineare Abbildung*

$$x_I^*\colon \bigwedge^r M \to R$$

so dass für alle r-elementigen Teilmengen $J \subset \underline{n}$ gilt

$$x_I^*(x_J) = \begin{cases} 1 & \text{falls } I = J, \\ 0 & \text{falls } I \neq J. \end{cases}$$

Beweis. Die Eindeutigkeit von x_I^* ist klar, weil die Werte von x_I^* auf dem Erzeugendensystem $(x_J)_{J\subset\underline{n},\sharp J=r}$ von $\bigwedge^r M$ festgelegt ist. Wir zeigen die Existenz. Sei $(x_1^*, \ldots, x_n^*)$ die duale Basis von $M^* = \mathrm{Hom}_R(M, R)$ die durch $x_i^*(x_j) = \delta_{ij}$ gegeben ist.

Setze

$$\phi_I\colon M^r \to R, \qquad (m_1, \ldots m_r) \mapsto \det(x_i^*(m_j))_{i\in I, j\in\underline{r}}.$$

Dann ist ϕ_I alternierend und r-linear, induziert also eine R-lineare Abbildung

$$x_I^*\colon \bigwedge^r M \to R$$

mit

$$x_I^*(x_J) = \det(x_i^*(x_j))_{i\in I, j\in J}$$

für jede r-elementige Teilmenge $J \subset \underline{n}$. Ist $I = J$, so ist $(x_i^*(x_j))_{i\in I,j\in J} = E_r$ und $\det E_r = 1$. Ist $I \neq J$, so gibt es wegen $\sharp I = \sharp J$ ein $j_0 \in J$ mit $j_0 \notin I$, d. h. $x_i^*(x_{j_0}) = 0$ für alle $i \in I$. Damit enthält die Matrix $(x_i^*(x_j))_{i\in I,j\in J}$ eine Nullspalte, hat also Determinante 0. □

Satz 5.25. *Sei M ein endlich erzeugter freier R-Modul vom Rang n und sei $r \in \mathbb{N}$. Dann gilt $\bigwedge^r M = 0$ für $r > n$ und für $1 \leq r \leq n$ ist $\bigwedge^r M$ ein freier R-Modul vom Rang $\binom{n}{r}$. Ist $x = (x_i)_{i\in\underline{n}}$ eine Basis von M, so ist $(x_I)_{I\subset\underline{n},\sharp I=r}$ eine Basis von $\bigwedge^r M$.*

Beweis. Nach 5.23 ist $(x_I)_{I\subset\underline{n},\sharp I=r}$ ein Erzeugendensystem. Es bleibt zu zeigen, dass dieses System linear unabhängig ist. Angenommen, es gilt

$$0 = \sum_{J\subset\underline{n},\sharp J=r} a_J x_J$$

für Skalare $a_I \in R$. Dann folgt für $I \subset \underline{n}$, $\sharp I = r$:

$$0 = x_I^*\Big(\sum_{J\subset\underline{n},\sharp J=r} a_J x_J\Big) = \sum a_J x_I^*(x_J) = a_I.$$

Damit ist da System linear unabhängig.

Die Abbildung

$$\{\text{Teilmengen von } \underline{n}\} \to \{\text{Wörter der Länge } n \text{ über dem Alphabet } \{x,y\}\}$$
$$I \mapsto a_1 a_2 \dots a_n, \quad a_i = x \text{ falls } i \in I,\ a_i = y \text{ sonst}$$

ist bijektiv. Die r-elementigen Teilmengen entsprechen dabei gerade den Wörtern, in denen r-mal der Buchstaben x und $n-r$-mal der Buchstabe y vorkommt. Ihre Anzahl ist damit gleich dem Koeffizienten von $x^r y^{n-r}$ in dem Polynom $(x+y)^n$. Das ist aber gerade $\binom{n}{r}$. Dies ist damit auch die Anzahl der Basiselemente x_I. □

Korollar 5.26. *Sei V ein endlich-dimensionaler Vektorraum über dem Körper K und $v_1, \dots, v_n$ Vektoren in V. Dann sind $v_1, \dots, v_n$ genau dann linear unabhängig wenn $v_1 \wedge \dots \wedge v_n \neq 0$ in $\bigwedge^n V$.*

Beweis. Sind $v_1, \dots, v_n$ linear unabhängig, so können wir $v_{n+1}, \dots, v_d$, $d = \dim V$ so wählen dass $(v_1, \dots, v_d)$ eine Basis ist. Nach 5.25 ist dann $v_1 \wedge \dots \wedge v_n$ ein Basisvektor in $\bigwedge^n V$ und insbesondere $\neq 0$.
Sind $v_1, \dots, v_n$ linear abhängig, so können wir nach Umnummerierung annehmen, dass

$$v_1 = \alpha_2 v_2 + \dots + \alpha_n v_n \quad , \quad \alpha_2, \dots, \alpha_n \in K.$$

Dann gilt

$$\begin{aligned} v_1 \wedge \dots \wedge v_n &= (\alpha_2 v_2 + \dots + \alpha_n v_n) \wedge v_2 \wedge \dots \wedge v_n \\ &= 0 \end{aligned}$$

□

Lemma 5.27. *Sei n eine natürliche Zahl und $\alpha\colon M \to N$ eine R-lineare Abbildung. Dann existiert genau eine R-lineare Abbildung $\bigwedge^n \alpha\colon \bigwedge^n M \to \bigwedge^n N$ mit*

$$(\bigwedge\nolimits^n \alpha)(m_1 \wedge \dots \wedge m_n) = \alpha(m_1) \wedge \dots \wedge \alpha(m_n)$$

für alle $(m_1, \dots, m_n) \in M^r$.

Beweis. Die Abbildung

$$\bar{\alpha}\colon M^n \to \bigwedge\nolimits^n N, \qquad (m_1, \dots, m_n) \mapsto \alpha(m_1) \wedge \dots \wedge \alpha(m_n)$$

ist n-fach linear und alternierend. Also existiert genau ein

$$\bigwedge\nolimits^n \alpha \in \mathrm{Hom}_R(\bigwedge\nolimits^n M, \bigwedge\nolimits^n N)$$

mit

$$\begin{aligned} \varphi(m_1 \wedge \dots \wedge m_n) &= \bar{\alpha}(m_1, \dots, m_n) \\ &= \alpha(m_1) \wedge \dots \wedge \alpha(m_n). \end{aligned}$$

□

Definition 5.28. $\bigwedge^n \alpha$ heißt die *n-te äußere Potenz* von α.

Satz 5.29. *Sei r eine natürliche Zahl, M und N freie R-Moduln mit Basen $x = (x_j)_{j\in\underline{n}}$, $y = (y_i)_{i\in\underline{m}}$ und $\alpha\colon M \to N$ eine R-lineare Abbildung. Ist $A = M_y^x(\alpha)$ die Darstellungsmatrix von α, so ist $(\det_{I,J} A)_{I\subset\underline{m},J\subset\underline{n},\sharp I=\sharp J=r}$ die Darstellungsmatrix von $\bigwedge^r \alpha$ bezüglich der Basen $(x_J)_{J\subset\underline{n},\sharp J=r}$ und $(y_I)_{I\subset\underline{m},\sharp I=r}$ von $\bigwedge^r M$ und $\bigwedge^r N$.*

Beweis. Für $z \in \bigwedge^r N$ gilt

$$z = \sum_{I\subset\underline{m},\sharp I=r} y_I^*(z) y_I$$

mit den Abbildungen y_I^* aus 5.24. Wählt man $z = \bigwedge^r \alpha(x_J)$ so erhält man

$$y_I^*(\bigwedge{}^r \alpha(x_J)) = \det(y_i^*(\alpha(x_j)))_{i\in I,j\in J}.$$

nach der Konstruktion der y_I im Beweis von 5.24. Nun gilt mit $A = (a_{ij})$

$$\alpha(x_j) = \sum_{i=1}^n y_i^*(\alpha(x_j)) y_i = \sum_{i=1}^n a_{ij} y_i,$$

also $y_i^*(\alpha(x_j)) = a_{ij}$ und

$$y_I^*(\bigwedge{}^r \alpha(x_J)) = \det_{I,J}(A).$$

Es folgt

$$\bigwedge{}^r \alpha(x_J) = z = \sum_{I\subset\underline{m},\sharp I=r} \det_{I,J}(A) y_I,$$

d. h. $\det_{I,J}(A)$ ist der Eintrag zur Position (I, J) der Darstellungsmatrix von $\bigwedge^r \alpha$. □

Korollar 5.30 (Cauchy-Binet-Formel)**.** *Sei $A \in M_{m,n}(R)$, $B \in M_{n,k}(R)$, $I \subset \underline{m}$, $J \subset \underline{k}$ r-elementige Teilmengen. Dann gilt*

$$\det_{I,J}(AB) = \sum_{\substack{K\subset\underline{n}\\ \sharp K=r}} \det_{I,K}(A) \det_{K,J}(B).$$

Beweis. Sei $M = R^k$, $N = R^n$, $P = R^m$,

$$\beta\colon M \to N, \quad x \mapsto Bx, \qquad \alpha\colon N \to P, \quad x \mapsto Bx$$

Die Darstellungsmatrix von $\bigwedge^r(\alpha \circ \beta) = \bigwedge^r(\alpha) \circ \bigwedge^r(\beta)$ bezüglich der Standardbasen ist dann

$$(\det_{I,J}(AB))_{I\subset\underline{m},J\subset\underline{k},\sharp I=\sharp J=r} = (\det_{I,K}(A))_{I\subset\underline{m},K\subset\underline{n},\sharp I=\sharp K=r} (\det_{K,J}(B))_{K\subset\underline{n},J\subset\underline{k},\sharp K=\sharp J=r}.$$

□

Korollar 5.31. *Sei M ein freier R-Modul vom Rang n und $\alpha \in \mathrm{End}_R(M)$. Dann ist $\bigwedge^n M$ ein freier R-Modul vom Rang $\binom{n}{n} = 1$. Insbesondere ist die natürliche Abbildung*

$$\phi\colon R \to \mathrm{End}_R(\bigwedge^n M), \qquad r \mapsto r\mathrm{id}$$

ein R-linearer Isomorphismus.
Es gilt $\phi(\det_R(\alpha)) = \bigwedge^n \alpha$.

Beweis. Wähle eine beliebige Basis $x = (x_i)_{i\in\underline{n}}$ von M. Dann ist $x_{\underline{n}} = x_1 \wedge \cdots \wedge x_n$ eine Basis von $\bigwedge^n M$. Die R-lineare Abbildung

$$\mathrm{End}_R(\bigwedge^n M) \to R, \qquad \beta \mapsto b \qquad \text{mit } \beta(x_{\underline{n}}) = bx_{\underline{n}}$$

ist die Inverse zu ϕ. Sei A die Darstellungsmatrix von α bezüglich x. Dann gilt $\det \alpha = \det(A)$ und

$$\bigwedge^n \alpha(x_{\underline{n}}) = \det(A) x_{\underline{n}}.$$

□

Bemerkung. Äußere Potenzen bilden die Grundlage für den Kalkül der Differentialformen.

Bemerkung. Analog zu äußeren Potenz kann man die k-te symmetrische Potenz $S^k_R(M)$ eines R-Moduls definieren: Setze

$$S^k_R(M) = \underbrace{M \otimes \cdots \otimes M}_{k} \Big/ \left(\begin{array}{l} \text{Untermodul erzeugt von} \\ m_1 \otimes \cdots \otimes m_k - m_{\sigma(1)} \otimes \cdots \otimes m_{\sigma(k)} \\ \text{für } m_i \in M,\ \sigma \in S_k \end{array} \right)$$

und schreibe $m_1 \dots m_k$ für das Bild von $m_1 \otimes \cdots \otimes m_k$ in $S^k_R(M)$. Dann ist

$$\phi\colon M^k \to S^k_R(M), \qquad (m_1, \dots, m_k) \mapsto m_1 \dots m_k$$

eine symmetrische k-lineare Abbildung und für jede symmetrische k-lineare Abbildung $f\colon M^k \to P$ gibt es genau eine lineare Abbildung $\bar{f}\colon S^k_R(M) \to P$ mit $f = \bar{f} \circ \phi$. Ist M frei und $(x_1, \dots, x_n)$ eine Basis von M, so ist $x_1^{r_1} x_2^{r_2} \dots x_n^{r_n}$ mit $r_1 + \ldots + r_n = k$, $r_i \in \mathbb{N}_0$, eine Basis von $S_R(M)$. Insbesondere ist dann $S^k_R(M)$ ein freier R-Modul vom Rang $\binom{k+n-1}{k}$ (Anzahl der Partitionen von $\underline{k}$ in n disjunkte (möglicherweise leere) Teilmengen).

5.4 Tensorprodukte für beliebige Ringe (*)

Sei R ein beliebiger Ring (mit 1).
Problem:
Eine R-Bilinearform $\phi\colon R \times R \to R$ erfüllt

$$rs\phi(1,1) = \phi(r,s) = sr\phi(1,1), \quad \text{also } (rs - sr)\phi(1,1) = 0$$

Ist R nicht kommutativ, so gibt es $r_0, s_0 \in R$ mit $r_0 s_0 \neq s_0 r_0$. Damit folgt $\phi(1,1) = 0$ und somit $\phi(r,s) = 0$ für alle $r, s \in R$.

Definition 5.32. Sei M ein R-Rechtsmodul und N ein R-Linksmodul, A eine abelsche Gruppe. Eine Abbildung

$$\phi\colon M \times N \to A$$

heißt R-ausgewogen (R-balanced), wenn sie $\mathbb{Z}$-bilinear ist und

$$\phi(mr, n) = \phi(m, rn)$$

für alle $m \in M$, $n \in N$ und $r \in R$ gilt. Wir schreiben $\mathrm{Bal}_R(M, N; A)$ für die abelsche Gruppe der R-ausgewogenen Abbildungen.

Satz 5.33. *Seien M, N, A wie oben. Die natürliche Abbildung*

$$\Psi\colon \mathrm{Hom}_R(N, \mathrm{Hom}_{\mathbb{Z}}(M, A)) \to \mathrm{Bal}_R(M, N; A) \quad \phi \mapsto f_\phi$$
$$\text{mit } f_\phi\colon M \times N \to A, \quad (m, n) \mapsto (\phi(n)(m))$$

ist ein $\mathbb{Z}$-linearer Isomorphismus.

Beweis. Wie 5.3. □

Satz 5.34. *Seien M, N wie oben. Es gibt ein Paar (T, g) bestehend aus einer abelschen Gruppe T und einer R-ausgewogenen Abbildung $g\colon M \times N \to T$ mit folgender Universaleigenschaft:*

„Zu jeder abelschen Gruppe A und jeder R-ausgewogenen Abbildung $f\colon M \times N \to A$ existiert ein eindeutig bestimmter Gruppenhomomorphismus $h : T \to A$, so dass $f = h \circ g$ gilt."

Beweis. Sei

$$C = \{ \sum_{(m,n)\in M\times N} a_{m,n}(m, n) | a_{m,n} \in \mathbb{Z}, \text{ fast alle gleich } 0\} = \mathbb{Z}^{(M\times N)}$$

Wir betrachten die Untergruppe D von C, der durch alle Elemente der Form

$$(m, rn) - (mr, n), \quad (m + m', n) - (m, n) - (m', n), \quad (m, n + n') - (m, n) - (m, n')$$

für $m, m' \in M, n, n' \in N, r, s \in R$ erzeugt wird und setzen $T = C/D$. Dann weiter wie in 5.4. □

Satz 5.35. *Ist R kommutativ, so gilt $T \cong M \otimes_R N$ (wobei wir den Rechtsmodul M durch $r \cdot m = mr$ als Linksmodul betrachten).*

Beweis. Die Abbildung $M \times N \to M \otimes_R N$, $(m, n) \to m \otimes n$ ist R-bilinear und damit auch R-ausgewogen, also existiert eine eindeutige Abbildung $T \to M \otimes_R N$ nach der Universaleigenschaft von T. Da R kommutativ ist, ist mit g auch die Abbildung

$$g_s\colon M \times N \to T, \qquad (m, n) \mapsto g(m, sn)$$

für alle $s \in R$ ausgewogen: Es gilt für $r \in R$

$$g_s(mr, n) = g(mr, sn) = g(m, rsn) = g(m, srn) = g_s(m, rn).$$

Aus der universellen Eigenschaft folgt die Existenz eines eindeutigen Gruppenhomomorphismus $\tilde{g}_s \colon M \times N \to M \times N$ mit $\tilde{g}_s(g(m,n)) = g(m, sn)$. Sei $s, s' \in R$. Aus der Eindeutigkeit folgt, dass $\tilde{g}_{s+s'} = \tilde{g}_s + \tilde{g}_{s'}$ gilt. Ferner gilt

$$\tilde{g}_s(\tilde{g}_{s'}(g(m,n))) = \tilde{g}_s(g(m, s'n)) = g(m, ss'm) = \tilde{g}_{ss'}(g(m,n)),$$

also auch $\tilde{g}_s \circ \tilde{g}_{s'} = \tilde{g}_{ss'}$; außerdem gilt $\tilde{g}_1 = \mathrm{id}$. Somit ist

$$R \to \mathrm{End}_{\mathbb{Z}}(T), \qquad s \mapsto \tilde{g}_s$$

ein Ringhomomorphismus und T wird durch

$$R \times T \to T, \qquad (s,t) \mapsto \tilde{g}_s(t)$$

zu einem R-Modul. Wegen

$$g(ms, n) = g(m, sn) = \tilde{g}_s(g(m,n))$$

ist g bezüglich dieser R-Modulstruktur R-bilinear. Also existiert eine eindeutige Abbildung $M \otimes_R N \to T$ nach der Universaleigenschaft von $M \otimes_R N$. Man rechnet nun nach, dass die beiden konstruierten Abbildungen invers zueinander sind. □

Definition 5.36. Wie im kommutativen Fall nennen wir die abelsche Gruppe $T = M \otimes_R N$ *Tensorprodukt* von M und N. Die Elemente in T der Form $g(m,n) = m \otimes n$ heißen *Elementartensoren*.

Korollar 5.37 (Adjungiertheit von $\otimes$ und Hom)**.** *Sei R ein Ring, M ein R-Rechtsmodul, N ein R-Linksmodul und P eine abelsche Gruppe. Dann ist*

$$\mathrm{Hom}_R(N, \mathrm{Hom}_{\mathbb{Z}}(M,P)) \to \mathrm{Hom}_{\mathbb{Z}}(M \otimes_R N, P), \qquad \phi \mapsto (n \otimes m \mapsto (\phi(n))(m))$$

ein Isomorphismus abelscher Gruppen.

Bemerkung. Anders als im kommutativen Fall gibt es für Ringe R, die nicht kommutativ sind, keine sinnvolle Definition für äußere und symmetrische Potenzen.

5.5 Verallgemeinerte Skalarerweiterungen (*)

Ziel:
Verallgemeinerung der Skalarerweiterung aus Definition 5.11.

Seien R und S Ringe (mit 1) und M ein S-R-Bimodul.

Lemma 5.38. *Ist N ein R-Linksmodul, so wird $M \otimes_R N$ zu einem S-Linksmodul durch*

$$s(m \otimes n) = (sm) \otimes n$$

für $s \in S$, $m \in M$ und $n \in N$.

Beweis. Die Abbildungen

$$g_s \colon M \times N \to M \otimes_R N, \qquad (m, n) \mapsto (sm) \otimes n$$

sind R-ausgewogen und induzieren deshalb Abbildungen $\tilde{g}_s \in \mathrm{End}_{\mathbb{Z}}(M \otimes_R N)$. Es gilt für $s, t \in S$

$$\begin{aligned} \tilde{g}_{s+t}(m \otimes n) &= (s+t)m \otimes n = sm \otimes n + tm \otimes n = (\tilde{g}_s + \tilde{g}_t)(m \otimes n) \\ \tilde{g}_{st}(m \otimes n) &= stm \otimes n = \tilde{g}_s(tm \otimes n) = (\tilde{g}_s \circ \tilde{g}_t)(m \otimes n) \\ \tilde{g}_1(m \otimes n) &= m \otimes n = \mathrm{id}_{M \otimes N}(m \otimes n) \end{aligned}$$

Also ist $M \otimes_R N$ mit der S-Operation

$$S \times M \otimes_R N, \qquad (s, x) \mapsto \tilde{g}_s(x)$$

ein S-Linksmodul. □

Satz 5.39 (Adjunktionseigenschaft)**.** *Für alle R-Linksmoduln N und S-Linksmoduln P ist*

$$\gamma \colon \mathrm{Hom}_S(M \otimes_R N, P) \to \mathrm{Hom}_R(N, \mathrm{Hom}_S(M, P)), \qquad \phi \mapsto (n \mapsto \phi(\cdot \otimes n))$$

ein Isomorphismus abelscher Gruppen.

Beweis. Wohldefiniertheit: Sei $\phi \in \mathrm{Hom}_S(M \otimes_R N, P)$. Man rechnet leicht nach, dass für jedes $n \in N$ die Abbildung

$$\phi_n \colon M \to P, \qquad m \mapsto \phi(m \otimes n)$$

S-linear ist. $\mathrm{Hom}_S(M, P)$ wird durch

$$R \times \mathrm{Hom}_S(M, P) \to \mathrm{Hom}_S(M, P), \qquad (r, \alpha) \mapsto (m \mapsto \alpha(mr))$$

zu einem R-Linksmodul (siehe die Bemerkung vor Lemma 1.7). Nun rechnet man nach, dass

$$N \to \mathrm{Hom}_S(M, P), \qquad n \mapsto \phi_n$$

R-linear ist.
Konstruktion der Inversen: Sei $\psi \in \mathrm{Hom}_R(N, \mathrm{Hom}_S(M, P))$. Dann ist

$$\Phi \colon M \times N \to P, \qquad (m, n) \mapsto \psi(n)(m)$$

R-ausgewogen: Sei $r \in R$, $m \in M$, $n \in N$. Dann gilt

$$(\psi(n))(mr) = (r\psi(n))(m) = (\psi(rn))(m).$$

Also induziert Φ eine $\mathbb{Z}$-lineare Abbildung $\phi\colon M \otimes_R N \to P$. Wegen

$$\phi(sm \otimes n) = \Phi(sm, n) = (\psi(n))(sm) = s(\psi(n)(m)) = s\phi(n \otimes m)$$

ist ϕ auch S-linear. Die so konstruierte Zuordnung definiert eine $\mathbb{Z}$-lineare Abbildung

$$\delta\colon \mathrm{Hom}_R(N, \mathrm{Hom}_S(M, N)) \to \mathrm{Hom}_S(M \otimes_R N, P), \qquad \psi \mapsto \phi.$$

Es gilt

$$(\gamma(\phi)(n))(m) = \phi(n \otimes m) = \psi(n)(m),$$

also $\gamma(\phi) = \psi$ und damit $\gamma \circ \delta = \mathrm{id}$. Andersherum gilt

$$(\delta \circ \gamma)(\phi)(n \otimes m) = \phi(n \otimes m),$$

also auch $\delta \circ \gamma = \mathrm{id}$. □

Beispiele.

1. Ist R kommutativ, so ist jeder R-Linksmodul M auf natürliche Weise ein R-R-Bimodul und wir erhalten 5.6 als Spezialfall von 5.39.

2. Ist $\phi\colon R \to S$ ein Ringhomomorphismus, so ist S mit $S \times R \to S, \quad (s, r) \mapsto s\phi(r)$ ein S-R-Bimodul. Für jeden R-Linksmodul N ist $N_S = S \otimes_R N$ die Skalarerweiterung und jeder S-Linksmodul P ist auch ein R-Linksmodul durch $r \cdot p = \phi(r)p$ für $r \in R$, $p \in$. Die Abbildung

   $$\mathrm{Hom}_S(S, P) \to P, \qquad \alpha \mapsto \alpha(1)$$

   ist ein Isomorphismus von R-Linksmoduln (vgl. 1.7). Nach 5.39 gilt

   $$\mathrm{Hom}_S(N_S, P) \cong \mathrm{Hom}_R(N, P)$$

   (Adjunktionseigenschaft der Skalarerweiterung).

3. Jeder R-Rechtsmodul M ist ein $\mathbb{Z}$-R-Bimodul. Ist N ein R-Linksmodul und P eine abelsche Gruppe, so erhalten wir

   $$\mathrm{Hom}_{\mathbb{Z}}(M \otimes_R N, P) \cong \mathrm{Hom}_R(N, \mathrm{Hom}_{\mathbb{Z}}(M, P)),$$

   also 5.6.

Lemma 5.40 (Funktorialität)**.** *Zu jedem Homomorphismus von S-R-Bimoduln $f\colon M \to M'$ und jedem Homomorphismus $g\colon N \to N'$ von R-Linksmoduln gibt es einen eindeutig bestimmten Homomorphismus*

$$g \otimes f\colon M \otimes_R N \to M' \otimes_R N$$

von S-Linksmoduln mit

$$g \otimes f(m \otimes n) = g(m) \otimes f(n)$$

für alle $m \in M$, $n \in N$.

Beweis. Wie 5.13. □

Bemerkung. Insbesondere erhalten wir einen Gruppenhomomorphismus

$$\mathrm{Hom}_R(N, N') \to \mathrm{Hom}_S(M \otimes_R N, M \otimes_R N'), \qquad g \mapsto \mathrm{id}_M \otimes g.$$

Lemma 5.41. *Sei $f\colon N \to N'$ eine injektive R-lineare Abbildung. Ist M frei als R-Rechtsmodul, so ist $\mathrm{id}_M \otimes f$ injektiv.*

Beweis. Wie 5.16. □

5.6 Morita-Äquivalenz für Matrixringe (*)

Sei R ein Ring (mit 1), $S = M_{n,n}(R)$ der Ring der $n \times n$-Matrizen mit Einträgen in R, V der S-R-Bimodul $M_{n,1}(R)$ (Spaltenvektoren), mit der R-Rechtsmultiplikation $(v_i)r = (v_i r)$, W der R-S-Bimodul $M_{n,1}(R)$ (Zeilenvektoren), mit der R-Linksmultiplikation $r(v_i) = (rv_i)$. Wir schreiben $e_i \in V$ für den Spaltenvektor

$$e_i = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} i\text{-te Zeile}$$

und $e_i^t \in W$ für den entsprechenden Zeilenvektor.

Satz 5.42. *Sei X ein R-Linksmodul und Y ein S-Linkssmodul. Dann gilt*

$$\mu_{S,Y}\colon V \otimes_R W \otimes_S Y \xrightarrow{\cong} Y, \qquad v \otimes w \otimes y \mapsto (vw)y \quad \text{(als } S\text{-Linksmoduln)}$$
$$\mu_{R,X}\colon W \otimes_S V \otimes_R X \xrightarrow{\cong} X, \qquad w \otimes v \otimes x \mapsto (wv)x \quad \text{(als } R\text{-Linksmoduln)}$$

Ferner gilt

$$\mathrm{id}_V \otimes \mu_{R,X} = \mu_{S,W \otimes_R X}\colon V \otimes_R W \otimes_S V \otimes_R X \to V \otimes_R X,$$
$$\mathrm{id}_W \otimes \mu_{S,Y} = \mu_{R,V \otimes_S Y}\colon W \otimes_S V \otimes_R W \otimes_S Y \to W \otimes_S Y.$$

Beweis. Für $v \in V$, $w \in W$, $a \in R$, $A \in S$, $x \in X$, $y \in Y$ gilt

$$\begin{aligned} ((va)w)y &= (v(aw))y, & ((wA)v)x &= (w(Av))x, \\ ((Av)w)y &= (A(vw))y, & ((aw)v)x) &= (a(wv))x, \\ (vw)(Ay) &= ((vw)A)y, & (wv)(ax) &= ((wv)a)x \end{aligned}$$

nach der Assoziativität der Matrixmultiplikation. Nach der Universaleigenschaft des Tensorprodukts sind die angegebenen Abbildungen also wohldefiniert und linear.
Setze

$$\phi(y) = \sum_{i=1}^{n} e_i \otimes e_i^t \otimes y.$$

Dann ist $\phi\colon Y \to V \otimes_R W \otimes_S Y$ die Inverse von $\mu_{S,Y}$:

$$\begin{aligned} \mu_{S,Y} \circ \phi(y) &= \sum_{i=1}^{n} (e_i e_i^t) y = E_n y = y. \\ \phi \circ \mu_{S,Y}(v \otimes w \otimes y) &= \sum_{i=1}^{n} e_i \otimes e_i^t \otimes (vw)y \\ &= \sum_{i=1}^{n} e_i \otimes e_i^t vw \otimes y \\ &= \sum_{i=1}^{n} e_i e_i^t v \otimes w \otimes y \\ &= (E_n v) \otimes w \otimes y \\ &= v \otimes w \otimes y. \end{aligned}$$

Setze

$$\psi(x) = (e_1^t \otimes e_1 \otimes x).$$

Dann gilt

$$\begin{aligned} \mu_{R,X} \circ \psi(x) &= e_1^t e_1 x = x \\ \psi \circ \mu_{R,X}(w \otimes v \otimes x) &= e_1^t \otimes e_1 \otimes (wv)x \\ &= e_1^t \otimes e_1 wv \otimes x \\ &= e_1^t e_1 w \otimes v \otimes x \\ &= w \otimes v \otimes x \end{aligned}$$

Also ist ψ die Inverse von μ_R.
Nun gilt für $v, v' \in V$, $w \in W$, $x \in X$:

$$\begin{aligned} \mathrm{id}_V \otimes \mu_{R,X}(v \otimes w \otimes v' \otimes x) = v \otimes (wv')x = (vw)v' \otimes x \\ = \mu_{S,V \otimes_R X}(v \otimes w \otimes v' \otimes x)m \end{aligned}$$

also $\mathrm{id}_V \otimes \mu_{R,X} = \mu_{S,W \otimes_R X}$. Die andere Gleichung beweist man analog. □

Satz 5.43.

(i) Für alle R-Linksmoduln X, X' ist

$$\mathrm{Hom}_R(X, X') \to \mathrm{Hom}_S(V \otimes_R X, V \otimes_R X'), \qquad f \mapsto \mathrm{id}_V \otimes f$$

ein Isomorphismus mit Inverser $g \mapsto \mu_{R,X'} \circ \mathrm{id}_W \otimes g \circ \mu_{R,X}^{-1}$

(ii) Für alle S-Linksmoduln Y, Y' ist

$$\mathrm{Hom}_S(Y, Y') \to \mathrm{Hom}_R(W \otimes_S Y, W \otimes_S Y), \qquad g \mapsto \mathrm{id}_W \otimes g$$

ein Isomorphismus mit Inverser $f \mapsto \mu_{S,Y'} \circ \mathrm{id}_V \otimes g \circ \mu_{S,Y}^{-1}$

Beweis.
Zu (i): Es gilt für $f \in \mathrm{Hom}_R(X, X')$, $x \in X$

$$\begin{aligned}(\mu_{R,X'} \circ \mathrm{id}_W \otimes \mathrm{id}_V \otimes f \circ \mu_{R,X}^{-1})(x) &= \mu_{R,X'} \circ \mathrm{id}_W \otimes \mathrm{id}_V \otimes f(e_1 \otimes e_1^t \otimes x) \\ &= \mu_{R,X'}(e_1 \otimes e_1^t \otimes f(x)) = e_1 e_1^t f(x) = f(x).\end{aligned}$$

Für $g \in \mathrm{Hom}_R(V \otimes_R X, V \otimes_R X')$ gilt

$$\begin{aligned}\mathrm{id}_V \otimes (\mu_{R,X'} \circ \mathrm{id}_W \otimes g \circ \mu_{R,X}^{-1}) &= \mathrm{id}_V \otimes \mu_{R,X'} \circ \mathrm{id}_V \otimes \mathrm{id}_W \otimes g \circ \mathrm{id}_V \otimes \mu_{R,X}^{-1} \\ &= \mu_{S,V\otimes_R X'} \circ \mathrm{id}_V \otimes \mathrm{id}_W \otimes g \circ \mu_{S,V\otimes_R X}^{-1}\end{aligned}$$

Nun gilt für $v \in V$, $x \in X$:

$$\begin{aligned}&(\mu_{S,V\otimes_R X'} \circ \mathrm{id}_V \otimes \mathrm{id}_W \otimes g \circ \mu_{S,V\otimes_R X}^{-1})(v \otimes x) \\ &\quad = (\mu_{S,V\otimes_R X'} \circ \mathrm{id}_W \otimes g)(\sum_{i=1}^n e_i \otimes e_i^t \otimes v \otimes x) \\ &\quad = (\mu_{S,V\otimes_R X'})(\sum_{i=1}^n e_i \otimes e_i^t \otimes g(v \otimes x)) \\ &\quad = \sum_{i=1}^n e_i e_i^t g(v \otimes x) = g(v \otimes x)\end{aligned}$$

Zu (ii): Ähnlich. □

Zusammengefassend kann man 5.42 und 5.43 wie folgt ausdrücken:

Theorem 5.44 (Morita-Äquivalenz)**.** *Durch $X \mapsto V \otimes_R X$ und $Y \mapsto W \otimes_S Y$ sind zueinander quasi-inverse Äquivalenzen zwischen der Kategorie der R-Linksmoduln und der Kategorie der S-Linksmoduln gegeben.*

Insbesondere lassen sich alle Klassifikationresultate für R-Linksmoduln auf S-Linksmoduln übertragen.

Korollar 5.45. *Sei X ein R-Linksmodul. Die Abbildung*

$$\{R\text{-Untermoduln } X' \subset X\} \to \{S\text{-Untermoduln } Y \subset V \otimes_R X\}$$
$$X' \mapsto V \otimes_R X'$$

ist eine inklusionserhaltende Bijektion.

Beweis. Sei $X'' \subset X' \subset X$ und $\iota\colon X' \to X$ die Inklusionsabbildung. Da V als R-Rechtsmodul frei ist, ist nach 5.41 $\mathrm{id}_V \otimes \iota$ injektiv. Wir können also $V \otimes_R X''$ als Untermodul von $V \otimes X'$ ansehen. Wählen wir $X' = X$, so folgt, dass $V \otimes_R X''$ ein Untermodul von $V \otimes_R X$ ist. Die angegebene Abbildung ist also wohldefiniert und inklusionserhaltend für alle R-Linksmoduln X.
Sei nun $Y \subset V \otimes_R X$, $\tau\colon Y \to V \otimes_R X$ und $z \in W \otimes_S Y$ mit $\mathrm{id}_W \otimes \tau(z) = 0$. Wegen $\tau = \mu_{S,V\otimes_R X} \circ \mathrm{id}_V \otimes \mathrm{id}_W \otimes \tau \circ \mu_{S,Y}^{-1}$ ist $\mathrm{id}_V \otimes \mathrm{id}_W \otimes \tau$ injektiv, also $v \otimes z = 0$ für alle $v \in V$. Damit gilt

$$z = \mu_{R,W\otimes_S Y}(\sum_{i=1}^{n} e_i^t \otimes e_i \otimes z) = 0.$$

Also ist

$$\mu_{S,V\otimes_R X} \circ \mathrm{id}_W \otimes \tau\colon W \otimes_S Y \to X$$

injektiv und wir können $W \otimes_S Y$ als Untermodul von X betrachten. Die Abbildung

$$\{S\text{-Untermoduln } Y' \subset V \otimes_R X\} \to \{R\text{-Untermoduln } X' \subset X\}$$
$$Y \mapsto W \otimes_S Y$$

ist dann die Inverse der obigen Abbildung. □

Korollar 5.46. *Sei $R = K$ ein Körper und $S = M_{n,n}(K)$. Dann ist jeder endlich erzeugte S-Linksmodul Y isomorph zu dem S-Linksmodul V^r für ein eindeutiges $r \in \mathbb{N}_0$. Insbesondere ist Y halbeinfach.*

Beweis. Es gilt $Y \cong V \otimes_K W \otimes_S Y$. Sei $(y_1, \ldots, y_s)$ ein S-Erzeugendensystem von Y. Dann ist $(e_i^t \otimes y_j)_{i\in\underline{n},j\in\underline{s}}$ ein Erzeugendensystem des K-Vektorraums $W \otimes_S Y$: Die Elementartensoren $(w \otimes y)_{(w,y)\in W\times Y}$ erzeugen $W \otimes_S Y$ als abelsche Gruppe. Also reicht es, $w \otimes y$ als Linearkombination darzustellen. Es gilt $y = \sum A_j y_j$ mit $A_i \in S$ und $wA_j = r_{ij}e_i^t$ mit $r_{ij} \in K$. Damit folgt

$$w \otimes y = \sum_{j=1}^{s} wA_j \otimes y_j = \sum_{i=1}^{n}\sum_{j=1}^{s} r_{ij}(e_i^t \otimes y_j)$$

wie gewünscht. Sei $r < \infty$ die Dimension von $W \otimes_S Y$ als K-Vektorraum. Dann gibt es einen K-linearen Isomorphismus $\phi\colon K^r \to W \otimes_S Y$ und somit einen S-linearen Isomorphismus

$$V^r \cong V \otimes_K K^r \xrightarrow[\cong]{\mathrm{id}_V\otimes\phi} V \otimes_K W \otimes_S Y \xrightarrow[\cong]{\mu_{S,Y}} Y.$$

Wegen der Eindeutigkeit der Dimension eines K-Vektorraums ist r eindeutig bestimmt. Da K nur die trivialen Untervektorräume 0 und K besitzt, hat $V = V \otimes_K K$ nur die trivialen S-Unterlinksmoduln 0 und V, d. h. V ist ein einfacher S-Linksmodul. Damit ist Y eine endliche direkte Summe einfacher Moduln, also ein halbeinfacher Modul. □

Korollar 5.47. *Die Linksideale von $S = M_{n,n}(K)$ sind gegeben durch $V \otimes_K L$, wobei $L \subset W$ die Untervektorräume von W durchläuft. Das Linksideal $I \subset S$ ist genau dann ein maximales Ideal, wenn* $\dim_K W \otimes_S I = n - 1$.

Beweis. Mittels

$$V \otimes_K W \xrightarrow[\cong]{v\otimes w \mapsto v\otimes w\otimes 1} V \otimes_K W \otimes_S S \xrightarrow[\cong]{\mu_{S,S}} S$$

können wir die S-Unterlinksmoduln von $V \otimes_K W$ mit den Linksidealen von S identifizieren. Die S-Unterlinksmoduln von $V \otimes_K W$ haben aber die gegebene Form.
Das Linksideal $I \subset S$ ist genau dann ein maximales Ideal, wenn es die Form $V \otimes_K L$ mit einem maximalen Untervektorraum $L \subset W$ mit $L \neq W$ hat, d. h. wenn $\dim_K L = n - 1$ gilt. Nun gilt $W \otimes_S V \otimes L \cong L$. □