Lineare Algebra

Vorlesung 2012/2013

Universität Mannheim

gehalten von Ralf Kurbel

Inhaltsverzeichnis

KAPITEL 5

Konjugationsklassen quadratischer Matrizen über Körpern

5.1. Hauptidealringe und euklidische Ringe

DEFINITION 5.1.1. *Ein Integritätsring ist ein nullteilerfreier, kommutativer Ring mit Eins.* □

LEMMA 5.1.2. *Sei R ein Integritätsring. Dann gilt für $a, b, c \in R$ mit $a \neq 0$:*

$$\begin{aligned} ab = 0 &\implies a = 0 \text{ oder } b = 0, \\ ab = ac &\iff b = c, \\ a = ac &\iff c = 1. \end{aligned}$$

□

DEFINITION 5.1.3. *Sei R ein Integritätsring. Zwei Elemente $a, b \in \mathbb{R}$ heißen assoziiert, wenn es eine Einheit $e \in R^*$ gibt mit $a = eb$. Es wird auch notiert:*

$$a \sim b := \quad \exists e \in R^* : b = ae.$$

□

LEMMA 5.1.4. *Sei R ein Integritätsring. Dann ist die Relation:*

$$\sim := \text{ „assoziiert sein“}$$

eine Äquivalenzrelation auf R. Insbesondere bilden die Einheiten von R die Äquivalenzklasse der Eins unter dieser Relation. □

DEFINITION 5.1.5. *Sei R ein Integritätsring, und seien $a, b \in R$. Gibt es ein $c \in R$ mit $ac = b$, so heißt a ein Teiler von b und b ein Vielfaches von a. Dies wird auch ausgedrückt und notiert durch:*

$$a \text{ teilt } b \qquad \text{bzw.} \qquad a \mid b.$$

Ein Element $d \in R$ heißt größter gemeinsamer Teiler (kurz: ggT) von a und b, falls gilt:

- *$d \mid a$ und $d \mid b$,*
- *Gilt für $c \in R$ sowohl $c \mid a$ als auch $c \mid b$, so folgt $c \mid d$.*

Ein Element $k \in R$ heißt kleinstes gemeinsames Vielfaches (kurz: kgV) von a und b, falls gilt:

- *$a \mid k$ und $b \mid k$,*
- *Gilt für $c \in R$ sowohl $a \mid c$ als auch $b \mid c$, so folgt $k \mid c$.*

□

LEMMA 5.1.6. *Sei R ein Integritätsring. Dann gilt für $a, b, c \in R$:*

$$\begin{aligned} a \mid b \text{ und } b \mid a &\iff a \sim b. \\ a \mid b \text{ und } a \sim c &\implies c \mid b. \\ a \mid b \text{ und } b \sim c &\implies a \mid c. \\ a \mid b \text{ und } a \mid c &\implies a \mid (b+c). \\ a \mid (b+c) \text{ und } a \mid b &\implies a \mid c. \\ a \mid b \text{ und } b \mid c &\implies a \mid c. \end{aligned}$$

Weiter gilt für zwei Elemente $a, b \in R$:

$$\begin{aligned} d \text{ und } \widetilde{d} \text{ sind ggTs von } a, b &\implies d \sim \widetilde{d}. \\ d \text{ ist ein ggT von } a, b \text{ und } d \sim \widetilde{d} &\implies \widetilde{d} \text{ ist ein ggT von } a, b. \\ k \text{ und } \widetilde{k} \text{ sind kgVs von } a, b &\implies k \sim \widetilde{k}. \\ k \text{ ist ein kgV von } a, b \text{ und } k \sim \widetilde{k} &\implies \widetilde{k} \text{ ist ein kgV von } a, b. \end{aligned}$$

□

DEFINITION 5.1.7. *Sei R ein Integritätsring. Für zwei Elemente $a, b \in R$ wird, falls ein größter gemeinsamer Teiler d existiert, $d = \mathrm{ggT}(a, b)$ geschrieben, und ebenso bei der Existenz eines kleinsten gemeinsamen Vielfachen k dann $k = \mathrm{kgV}(a, b)$. Dabei sind die Ausdrücke $\mathrm{ggT}(a, b)$ und $\mathrm{kgV}(a, b)$ nach Lemma 5.1.6 nur bis auf Einheiten eindeutig bestimmt, so daß das Gleichheitszeichen hier mißbraucht wird. Die Aussage „$\mathrm{ggT}(a, b) = 1$“ ist so zu verstehen, daß Eins ein ggT ist.*
Zwei Elemente $a, b \in R$ heißen teilerfremd, falls $\mathrm{ggT}(a, b) = 1$ gilt. □

DEFINITION 5.1.8. *Sei R ein Integritätsring und $a \in R$. Dann ist die folgende Menge ein Ideal (Lemma 1.3.26) und heißt das von a erzeugte Hauptideal:*

$$(a)_R := \{\, xa \mid x \in R \,\}.$$ □

LEMMA 5.1.9. *Sei R ein Integritätsring. Dann gilt für $a, b \in R$:*

$$a \mid b \iff (b)_R \subseteq (a)_R.$$

Daraus folgt sofort mit Lemma 5.1.6:

$$a \sim b \iff (a)_R = (b)_R.$$ □

DEFINITION 5.1.10. *Sei R ein Integritätsring.*

- *Ein Element $p \in R$ mit $p \neq 0$ und $p \notin R^*$ heißt prim, falls für alle $a, b \in R$ gilt:*
$$p \mid ab \implies p \mid a \text{ oder } p \mid b.$$
- *Ein Element $u \in R$ mit $u \neq 0$ und $u \notin R^*$ heißt irreduzibel, falls für alle $a, b \in R$ gilt:*
$$u = ab \implies a \in R^* \text{ oder } b \in R^*.$$
Ein Element, das nicht irreduzibel ist, heißt reduzibel. □

LEMMA 5.1.11. *Sei R ein Integritätsring, und $p \in R$. Dann gilt:*

$$p \text{ prim} \implies p \text{ irreduzibel}.$$ □

SATZ 5.1.12. *Sei R ein Integritätsring und $a \in R$. Weiter seien $p_1, \ldots, p_r \in R$ Primelemente mit :*

$$a = p_1 \cdot \ldots \cdot p_r.$$

Dann ist diese Zerlegung bis auf Reihenfolge und Einheiten eindeutig, d.h. für Primelemente $q_1, \ldots, q_k$ mit $a = q_1 \cdot \ldots \cdot q_k$ gilt:

$$k = r, \quad \text{und} \quad \exists \pi \in S_r : p_i \sim q_{\pi(i)}.$$

Eine solche Zerlegung heißt Primfaktorzerlegung von a. □

DEFINITION 5.1.13. *Ein Integritätsring R heißt faktoriell, falls es für jedes Element $a \in R$ mit $a \neq 0$ und $a \notin R^*$ eine Primfaktorzerlegung gibt.* □

LEMMA 5.1.14. *Sei R ein faktorieller Ring, und seien $a, b \in R$. Dann existieren $\mathrm{ggT}(a,b)$ und $\mathrm{kgV}(a,b)$. Sind weiter $a, b \neq 0$, so gibt es eine endliche Menge $\mathcal{P}$ von Primelementen aus R, so daß mit einer Einheit ε folgende Primfaktorzerlegungen von a und b existieren:*

$$a := \prod_{p \in \mathcal{P}} p^{s_p} \quad \text{und} \quad b := \varepsilon \prod_{p \in \mathcal{P}} p^{t_p} \quad \text{mit } s_p, t_p \geq 0.$$

Dann existieren folgender ggT und folgendes kgV von a und b:

$$\mathrm{ggT}(a,b) = \prod_{p \in \mathcal{P}(R)} p^{\min(s_p, t_p)} \quad \text{und} \quad \mathrm{kgV}(a,b) = \prod_{p \in \mathcal{P}(R)} p^{\max(s_p, t_p)}.$$ □

LEMMA 5.1.15. *Sei R ein faktorieller Ring und $u \in R$. Dann gilt:*

$$u \text{ irreduzibel} \iff u \text{ prim.}$$ □

DEFINITION 5.1.16. *Ein Integritätsring R heißt Hauptidealring, falls jedes seiner Ideale $I \subseteq R$ ein Hauptideal ist, d.h. $I = (a)_R$ für ein $a \in R$.* □

LEMMA 5.1.17. *Sei R ein Integritätsring, und seien $I, J \subseteq R$ Ideale. Dann gilt:*

- *$I \cap J$ ist ein Ideal.*
- *$I + J := \{ ai + bj \mid i \in I, j \in J, a, b \in R \}$ ist ein Ideal.* □

LEMMA 5.1.18. *Sei R ein Hauptidealring, und seien $a, b \in R$. Dann gilt:*

$$(a)_R + (b)_R = \big(\mathrm{ggT}(a,b)\big)_R \qquad \text{und} \qquad (a)_R \cap (b)_R = \big(\mathrm{kgV}(a,b)\big)_R.$$

Insbesondere existieren damit ein ggT und ein kgV von a und b.
Weiter gibt es somit Elemente $c, d \in R$ mit:

$$ca + db = \mathrm{ggT}(a,b),$$

und diese können sogar so gewählt werden, daß $\mathrm{ggT}(c,d) = 1$ gilt. □

SATZ 5.1.19. *Sei R ein Integritätsring. Dann gilt:*

$$R \text{ ist ein Hauptidealring} \implies R \text{ ist faktoriell.}$$ □

DEFINITION 5.1.20. *Ein Integritätsring R heißt euklidisch, falls es eine Gradfunktion:*

$$\nu\colon R\setminus\{0\}\longrightarrow\mathbb{N}_0$$

gibt, so daß gilt: Für alle $a,b\in R$ mit $b\neq 0$ existieren (nicht notwendig eindeutige) Elemente $q,r\in R$ mit:

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

Obige Zerlegung wird auch als Division mit Rest bezeichnet, wobei q als der Quotient und r als der Rest bezeichnet wird. □

SATZ 5.1.21. *Sei R ein Integritätsring. Dann gilt:*

$$R\ \text{ist euklidisch}\quad\Longrightarrow\quad R\ \text{ist ein Hauptidealring}$$ □

SATZ 5.1.22. *Sei R ein euklidischer Ring mit einer Grad-Funkion ν, und weiter seien $a,b\in R$ mit $b\neq 0$. Dann seien Elemente $r_0,r_1,\ldots$ und $q_1,q_2,\ldots$ aus R durch folgende iterierte Division mit Rest definiert, solange $r_i\neq 0$ gilt:*

$$\begin{aligned}
r_0&:=a,\quad r_1:=b,\\
a&=q_1b+r_2,\\
b&=q_2r_2+r_3,\\
r_2&=q_3r_3+r_4,\\
r_3&=q_4r_4+r_5,\\
&\vdots\qquad\vdots\\
r_{i-2}&=q_{i-1}r_{i-1}+r_i,\\
&\vdots\qquad\vdots
\end{aligned}$$

Dann gibt es ein $k\in\mathbb{N}$, so daß gilt:

$$r_0,\ldots,r_{k-1}\neq 0,\quad \nu(r_1)>\ldots>\nu(r_{k-1})>0,\quad\text{und}\quad r_k=\mathrm{ggT}(a,b).$$

Dieses Verfahren zur Erzeugung von $\mathrm{ggT}(a,b)$ wird der euklidische Algorithmus genannt.

Die obigen im euklidischen Algorithmus auftretenden Gleichungen (Divisionen mit Rest) können nach den Resten r_i umgeformt werden:

$$\begin{aligned}
a&=q_1b+r_2,\\
b&=q_2r_2+r_3,\\
r_2&=q_3r_3+r_4,\\
r_3&=q_4r_4+r_5,\\
&\vdots\qquad\vdots\\
r_{k-3}&=q_{k-2}r_{k-2}+r_{k-1}\\
r_{k-2}&=q_{k-1}r_{k-1}+r_k,
\end{aligned}
\qquad\Longrightarrow\qquad
\begin{aligned}
r_2&=a-q_1b,\\
r_3&=b-q_2r_2,\\
r_4&=r_2-q_3r_3,\\
r_5&=r_3-q_4r_4,\\
&\vdots\qquad\vdots\\
r_{k-1}&=r_{k-3}-q_{k-2}r_{k-2}\\
r_k&=r_{k-2}-q_{k-1}r_{k-1}.
\end{aligned}$$

Durch iteriertes Einsetzen der r_i „von unten nach oben“ kann dann r_k offensichtlich als Linearkombination von a und b geschrieben werden, denn zuerst ist r_k eine Linearkombination von r_{k-1} und r_{k-2}:

$$r_k=r_{k-2}-q_{k-1}r_{k-1},$$

und nach ersetzen von r_{k-1} durch die entsprechende Gleichung wird es zu einer Linearkombination von r_{k-2} und r_{k-3}:

$$r_k = r_{k-2} - q_{k-1}r_{k-1} = r_{k-2} - q_{k-1}\underbrace{(r_{k-3} - q_{k-2}r_{k-2})}_{=r_{k-1}} = (1 + q_{k-1}q_{k-2})r_{k-2} - q_{k-1}r_{k-3}$$

Dies kann fortgeführt werden, bis r_k eine Linearkombination von $r_0 = a$ und $r_1 = b$ ist, und es ergibt sich dann eine Darstellung von $r_k = \mathrm{ggT}(a,b)$ als Linearkombination von a und b wie in Lemma 5.1.18 postuliert:

$$ca + db = \mathrm{ggT}(a,b),$$

wobei c und d mit Hilfe der q_i berechnet werden wie oben beschrieben.
Dieses Verfahren zur Darstellung von $\mathrm{ggT}(a,b)$ als Linearkombination von a und b wird der erweiterte euklidische Algorithmus genannt. □

Satz 5.1.23.

- *$\mathbb{Z}$ ist ein euklidischer Ring mit der Betragsfunktion als Gradfunktion:*

$$|\cdot| \colon \mathbb{Z} \setminus \{0\} \longrightarrow \mathbb{N} \quad \textit{mit} \quad a \mapsto |a|.$$

- *Ist K ein Körper, so ist der Polynomring $K[t]$ ein euklidischer Ring mit dem Polynomgrad als Gradfunktion:*

$$\mathrm{grad} \colon K[t] \setminus \{0\} \longrightarrow \mathbb{N} \quad \textit{mit} \quad p \mapsto \mathrm{grad}(p).$$ □

Satz 5.1.24. *Sei R ein Hauptidealring und $p \in R$ mit $p \neq 0$. Dann sind äquivalent:*

i.) p ist prim.
ii.) p ist irreduzibel.
iii.) $R/(p)_R$ ist ein Körper. □

Satz 5.1.25. *(Chinesischer Restsatz für Hauptidealringe)*
Sei R ein Hauptidealring, und seien $a_1, \ldots, a_n$ paarweise teilerfremde Elemente, d.h. es gilt $\mathrm{ggT}(a_i, a_j) = 1$ für $i \neq j$. Für $1 \leq i \leq n$ sei π_i die kanonische Projektion:

$$\pi_i \colon R \longrightarrow R/(a_i)_R \quad \textit{mit} \quad x \mapsto x + (a_i)_R.$$

Dann ist die folgende Abbildung π ein Ringepimorphismus:

$$\pi \colon R \longrightarrow R/(a_1)_R \times \cdots \times R/(a_n)_R \quad \textit{mit} \quad x \mapsto \big(\pi_1(x), \ldots, \pi_n(x)\big),$$

und es gilt:

$$\ker(\pi) = (a)_R \quad \textit{mit} \quad a := a_1 \cdot \cdots \cdot a_n,$$

so daß der Homomorphie-Satz 1.3.48 folgenden Ring-Isomorphismus induziert:

$$\xi \colon R/(a)_R \longrightarrow R/(a_1)_R \times \ldots \times R/(a_n)_R \quad \textit{mit} \quad x + (a)_R \mapsto \big(x + (a_1)_R, \ldots, x + (a_n)_R\big).$$ □

BEMERKUNG 5.1.26. *Aus dem Beweis von Satz 5.1.25 ergibt sich folgendes Verfahren, bzgl. der Abbildung:*

$$\pi\colon R \longrightarrow R/(a_1)_R \times \cdots \times R/(a_n)_R \quad \textit{mit} \quad x \mapsto \big(\pi_1(x), \ldots \pi_n(x)\big)$$

für $(x_1, \ldots, x_n) \in R/(a_1)_R \times \ldots R/(a_n)_R$ *ein Urbild zu konstruieren.*

- *Für* $1 \leq j \leq n$ *sei* $b_j := \prod_{i \neq j} a_i$.
- *Es gilt* $\mathrm{ggT}(a_j, b_j) = 1$, *und es existieren* α_j, β_j *mit:*

$$\alpha_j a_j + \beta_j b_j = 1 \qquad \textit{(erweiterter euklidischer Algorithmus).}$$

- $e_j := \beta_j b_j$ *erfüllt die Gleichung:*

$$\pi_i(e_j) = \begin{cases} 1 + (a_i)_R & \textit{für } i = j, \\ 0 + (a_i)_R & \textit{für } i \neq j. \end{cases}$$

Ist jeweils $\widetilde{x}_i$ *ein Urbild von* x_i *unter* π_i, *so ist:*

$$x := \sum_{i=1}^{n} \widetilde{x}_i e_i$$

ein Urbild von $(x_1, \ldots, x_n)$ *unter* π. □

5.2. Moduln über Hauptidealringen

SATZ 5.2.1. *Sei* R *ein kommutativer Ring mit Eins und* M *ein freier* R*-Modul. Sind* $(x_i)_{i \in I}$ *und* $(y_j)_{j \in J}$ *Basen von* M, *so sind* I *und* J *gleichmächtig.* □

DEFINITION 5.2.2. *Sei* R *ein kommutativer Ring mit Eins und* M *ein freier* R*-Modul. Dann ist der Rang von* M *definiert als die Mächtigkeit einer (und nach Satz 5.2.1 jeder) seiner Basen und wird notiert mit* $\mathrm{rg}_R(M)$. □

DEFINITION 5.2.3. *Sei* R *ein kommutativer Ring mit Eins und* M *ein* R*-Modul. Weiter sei* I *eine nicht-leere Menge, und es seien* $U_i \subseteq M$ *Untermodule für* $i \in I$. *Dann ist die Summe der* U_i *definiert als das Erzeugnis aller Vektoren aus den* U_i *(siehe auch Definition 2.2.8):*

$$\sum_{i \in I} U_i := \Big\langle \bigcup_{i \in I} U_i \Big\rangle.$$

Die Summe $\sum_{i \in I} U_i$ *heißt direkte Summe der* U_I, *falls für alle* $j \in I$ *gilt:*

$$U_j \cap \sum_{\substack{i \in I \\ i \neq j}} U_i = \{0\}.$$

Ist die Summe der U_i *direkt, so wird auch notiert:*

$$\bigoplus_{i \in I} U_i.$$ □

SATZ 5.2.4. *Sei* R *ein kommutativer Ring mit Eins,* M *ein* R*-Modul. Weiter sei* I *ein nicht-leere Menge, und es seien* $U_i \subseteq M$ *Untermodule für* $i \in I$. *Dann gilt:*

$$M = \bigoplus_{i \in I} U_i \quad \Longleftrightarrow \quad \textit{Jedes } m \in M \textit{ hat eine eindeutige Darstellung } m = \textstyle\sum_{i \in I} u_i \textit{ mit } u_i \in U_i.$$ □

LEMMA 5.2.5. *Sei R ein kommutativer Ring mit Eins, I eine nicht-leere Teilmenge und $M = \bigoplus_{i\in I} U_i$ mit Untermoduln $U_i \subseteq M$ für $i \in I$.*
Ist dann für $i \in I$ jeweils $(x_{i,j})_{j\in J_i}$ ein linear unabhängiges System in U_i, so ist ein aus allen diesen Systemen zusammengesetztes System linear unabhängig in M. □

LEMMA 5.2.6. *Sei R ein kommutativer Ring mit Eins, I eine nicht-leere Teilmenge und $M = \bigoplus_{i\in I} U_i$ mit Untermoduln $U_i \subseteq M$ für $i \in I$. Sind die U_i freie R-Moduln so ist auch M ein freier R-Modul, und jedes System zusammengesetzt aus Basen der U_i ist eine Basis von M.*
Ist insbesondere I eine endliche Menge und haben alle U_i endliche Basen, so folgt direkt:

$$\operatorname{rg}_R(M) = \sum_{i\in I} \operatorname{rg}_R(U_i).$$ □

LEMMA 5.2.7. *Sei R ein kommutativer Ring mit Eins und M ein R-Modul. Weiter sei $M = U \oplus W$ für Untermoduln $U, W \subseteq M$. Dann gilt:*

$$M/U \cong W.$$ □

DEFINITION 5.2.8. *Sei R ein kommutativer Ring mit Eins und M ein R-Modul. Ein Element $x \in M$ heißt Torsionselement, falls es ein $r \in R$ mit $r \neq 0$ gibt mit $rx = 0$. Die Menge aller Torsionselemente von M wird mit M_{Tor} bezeichnet.*
Gilt $M_{Tor} = \{0\}$, so heißt M torsionsfrei. □

LEMMA 5.2.9. *Sei R ein Integritätsring und M ein R-Modul. Dann ist M_{Tor} ein Untermodul von M.* □

LEMMA 5.2.10. *Sei R ein Integritätsring und M ein R-Modul. Dann gilt:*

$$M \text{ frei} \quad \Longrightarrow \quad M \text{ torsionsfrei.}$$

DEFINITION 5.2.11. *Sei R ein kommutativer Ring mit Eins und M ein R-Modul. Für $x \in M$ ist dann der Annulator definiert als die Menge:*

$$\operatorname{Ann}_R(x) := \{\, r \in R \mid rx = 0 \,\}.$$

Der Annulator des ganzen Moduls M ist definiert als Schnitt aller Annulatoren:

$$\operatorname{Ann}_R(M) := \bigcap_{x\in M} \operatorname{Ann}_R(x) = \{\, r \in R \mid rx = 0 \text{ für alle } x \in M \,\}.$$ □

LEMMA 5.2.12. *Sei R ein kommutativer Ring mit Eins und M ein R-Modul. Dann ist für jedes $x \in M$ der Annulator $\operatorname{Ann}_R(x)$ ein Ideal in R, und ebenso der Annulator $\operatorname{Ann}_R(M)$ des gesamten Moduls.*
Ist M endlich erzeugt von Elementen $x_1, \ldots, x_n$, so gilt:

$$\operatorname{Ann}_R(M) = \bigcap_{i=1}^{n} \operatorname{Ann}_R(x_i).$$

Ist dabei insbesondere R ein Hauptidealring, so sind die Ideale $\operatorname{Ann}_R(x_i)$ Hauptideale der Form $(r_i)_R$ mit $r_i \in R$, und es gilt nach Lemma 5.1.18:

$$\operatorname{Ann}_R(M) = \big(\operatorname{kgV}(r_1, \ldots, r_n)\big)_R.$$ □

SATZ 5.2.13. *Sei R ein Hauptidealring und M ein freier R-Modul endlichen Ranges. Dann gilt für einen Untermodul $U \subseteq M$:*

$$U \text{ ist frei} \qquad \text{und} \qquad \operatorname{rg}_R(U) \leq \operatorname{rg}_R(M). \qquad \square$$

SATZ 5.2.14. *Sei R ein Hauptidealring und M ein endlich erzeugter R-Modul. Dann ist auch jeder Untermodul $U \subseteq M$ endlich erzeugt.*
Existiert dabei in M ein Erzeugendensystem mit n Elementen, so gibt es in jedem Untermodul $U \subseteq M$ ein Erzeugendensystem, welches aus höchstens n Elemente besteht. $\square$

LEMMA 5.2.15. *Sei R ein Hauptidealring und M ein endlich erzeugter torsionsfreier R-Modul. Dann ist M ein freier Modul.* $\square$

LEMMA 5.2.16. *Sei R ein Hauptidealring und $\varphi\colon M \longrightarrow N$ eine R-lineare surjektive Abbildung. Dann gilt:*

$$N \text{ ist ein freier } R\text{-Modul} \quad \Longrightarrow \quad \begin{array}{l} \text{Es gibt einen freien Modul } F \subseteq M \text{ mit} \\ M = \ker(\varphi) \oplus F \text{ und } F \cong N. \end{array}$$

Insbesondere gilt: Ist $(y_i)_{i\in I}$ eine Basis von N, und sind $(x_i)_{i\in I}$ dazu passende Urbilder mit $x_i \in M$ und $\varphi(x_i) = y_i$, so ist das System $(x_i)_{i\in I}$ linear unabhängig und $F := \langle x_i \mid i \in I\rangle \subseteq M$ ein solcher Modul. $\square$

SATZ 5.2.17. *Sei R ein Hauptidealring und M ein endlich erzeugter R-Modul. Dann gibt es einen freien Untermodul $F \subseteq M$ mit:*

$$M = F \oplus M_{Tor}.$$

Der Rang von F ist eindeutig bestimmt. $\square$

SATZ 5.2.18. *(Elementarteilersatz für Moduln)*
Sei R ein Hauptidealring und M ein freier R-Modul vom Rang n. Weiter sei $U \subseteq M$ ein Untermodul mit $U \neq \{0\}$. Dann folgt:

Existenzaussage: *Es gibt eine Basis $x_1, \ldots, x_n$ von M und $\alpha_1, \ldots, \alpha_k \in R \setminus \{0\}$ mit $k \in \mathbb{N}$, so daß gilt:*

$$\alpha_i \mid \alpha_{i+1} \text{ für } 1 \leq i < k \quad \text{und} \quad \alpha_1 x_1, \ldots, \alpha_k x_k \text{ ist ein Basis von } U.$$

Eindeutigkeitsaussage: *Die obigen U zugeordneten Elemte $\alpha_1, \ldots, \alpha_k$ sind bis auf Einheiten eindeutig bestimmt.* $\square$

SATZ 5.2.19. *(Elementarteilersatz für Matrizen)*
Sei R ein Hauptidealring und $A \in \operatorname{Mat}(m \times n, R)$ mit $A \neq 0$. Dann folgt:

Existensaussage: *Es gibt Matrizen $S \in \mathrm{GL}_m(R)$ und $T \in \mathrm{GL}_n(R)$ und Elemente $\alpha_1, \ldots, \alpha_k \in R \setminus \{0\}$ mit $k \in \mathbb{N}$, so daß gilt:*

$$SAT = \begin{pmatrix} \alpha_1 & & & & \\ & \ddots & & & \\ & & \alpha_k & & \\ & & & 0 & \\ & & & & \ddots \\ & & & & & 0 \end{pmatrix} \quad \text{und} \quad \alpha_i \mid \alpha_{i+1} \text{ für } 1 \leq i < k.$$

Eindeutigkeitsaussage: Die obigen A zugeordneten Diagonalelemte $\alpha_1, \ldots, \alpha_k$ sind bis auf Einheiten eindeutig bestimmt. □

BEMERKUNG 5.2.20.

i.) In dem Hauptidealring $\mathbb{Z}$ gibt es nur die Einheiten $\{\pm 1\}$, und damit sind die Äquivalenzklassen assozierter Elemente (siehe Lemma 5.1.4) zweielementig – bis auf die Äquivalenzklasse von 0. Damit gilt für $a \in \mathbb{Z}$:

$$[0]_\sim = \{0\} \quad \textit{oder} \quad [a]_\sim = \{-a, a\} \textit{ für } a \neq 0.$$

Insbesondere liegt in der Äquivalenzklasse eines $a \neq 0$ genau ein Element aus $\mathbb{N}$.

ii.) Sei K ein Körper. Dann sind die Einheiten des Polynomrings $K[t]$ die Konstanten Polynome ungleich Null, d.h. $\big(K[t]\big)^* = K^*$, und für ein Polynom $p \in K[t]$ hat die Äquivalenzklasse seiner assoziierten Elemente die Form:

$$[p]_\sim = \{\, \alpha \cdot p \mid \alpha \in K^* \,\}.$$

Insbesondere enthält für $p \neq 0$ die Äquivalenzklasse genau ein normiertes Polynom. □

DEFINITION 5.2.21. *(Elementarteiler eines Untermoduls)*
Sei R ein Hauptidealring und M ein freier R-Modul endlichen Ranges. Weiter sei $U \subseteq M$ ein Untermodul mit $U \neq \{0\}$. Sei $x_1, \ldots, x_n$ eine Basis von M, und seien $\alpha_1, \ldots, \alpha_k \in R$ Elemente, welche die seienBedingungen aus Satz 5.2.18 erfüllen. Dann heißen $\alpha_1, \ldots, \alpha_k$ Elementarteiler von U bzgl. M (diese sind nur bis auf Einheiten eindeutig bestimmt!), und $x_1, \ldots, x_n$ eine Elementarteilerbasis von M bzgl. U.
Ist $R := \mathbb{Z}$, so existieren nach Bemerkung 5.2.20 eindeutig bestimmte Elemente $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$, die Elementarteiler von U bzgl. M sind, und diese werden „die“ Elementarteiler von U bzgl. M genannt.
Ist $R := K[t]$ für einen Körper K, so existieren nach Bemerkung 5.2.20 eindeutig bestimmte normierte Polynome $p_1, \ldots, p_k$, die Elementarteiler von U bzgl. M sind, und diese werden „die“ Elementarteiler von U bzgl. M genannt. □

DEFINITION 5.2.22. *(Elementarteiler einer Matrix)*
Sei R ein Hauptidealring und $A \in \mathrm{Mat}(m \times n, R)$. Sind $\alpha_1, \ldots, \alpha_k \in R$ Elemente, welche die Bedingungen aus Satz 5.2.18 erfüllen, so heißen diese Elementarteiler von A (diese sind nur bis auf Einheiten eindeutig bestimmt!).
Ist $R := \mathbb{Z}$, so existieren nach Bemerkung 5.2.20 eindeutig bestimmte Elemente $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$, die Elementarteiler von A sind, und diese werden „die“ Elementarteiler von A genannt.
Ist $R := K[t]$ für einen Körper K, so existieren nach Bemerkung 5.2.20 eindeutig bestimmte normierte Polynome $p_1, \ldots, p_k$, die Elementarteiler von A sind, und diese werden „die“ Elementarteiler von A genannt.
Ist $A \in \mathrm{Mat}(m \times n, R)$ gegeben, und gilt für $S \in \mathrm{GL}_m(R)$ und $T \in \mathrm{GL}_n(R)$:

$$SAT = \begin{pmatrix} \alpha_1 & & & & \\ & \ddots & & & \\ & & \alpha_k & & \\ & & & 0 & \\ & & & & \ddots \\ & & & & & 0 \end{pmatrix} \quad \textit{mit} \quad \alpha_i \mid \alpha_{i+1} \quad (\textit{Elementarteiler von } A),$$

so heißt die rechte Diagonalmatrix Smith-Normalform von A. □

BEMERKUNG 5.2.23.

i.) Ist R ein kommutativer Ring mit Eins, so ist auf $\mathrm{Mat}(m \times n, R)$ *eine Äquivalenzrelation definiert durch:*

$$A \sim B: \quad \exists S \in \mathrm{GL}_m(R), T \in \mathrm{GL}_n(R) : B = SAT.$$

Siehe dazu auch Aufgabe 4, Blatt 6 aus LA IIa: dort ist die Aussage für Körper formuliert, und der Beweis über Ringen läuft analog.
In diesem Sinne ist in Definition 5.2.22 die Matrix A äquivalent zu einer Smith-Normalform, und über einem Hauptidealring enthält jede Äquivalenzklasse eine Smith-Normalform.

ii.) Smith-Normalformen einer Matrix in Definition 5.2.22 sind im allgemeinen nicht eindeutig, da auch die Elementarteiler einer Matrix nicht eindeutig sind. Ist $A \in \mathrm{Mat}(m \times n, R)$ gegeben, dann gilt jedoch: Sind die beiden Matrizen

$$\begin{pmatrix} \alpha_1 & & & & \\ & \ddots & & & \\ & & \alpha_k & & \\ & & & 0 & \\ & & & & \ddots \\ & & & & & 0 \end{pmatrix} \quad \textit{und} \quad \begin{pmatrix} \beta_1 & & & & \\ & \ddots & & & \\ & & \beta_r & & \\ & & & 0 & \\ & & & & \ddots \\ & & & & & 0 \end{pmatrix}$$

jeweils Smith-Normalformen von A, so folgt aus dem Elementarteilersatz für Matrizen (Satz 5.2.19)

$$k = r \quad \textit{und} \quad \alpha_i \sim \beta_i \textit{ für } 1 \leq i \leq k.$$

iii.) Über $\mathbb{Z}$ und dem Polynomring $K[t]$ für einen Körper K sind durch spezielle Vereinbahrung in Definition 5.2.22 die Elementarteiler einer Matrix eindeutig bestimmt. Dadurch gibt es in diesen Fällen auch genau eine *Smith-Normalform. Diese beschreiben dann eindeutig die Äquivalenzklassen der obigen Äquivalenzrelation.* □

LEMMA 5.2.24. *Für die beiden Elementarteilersätze 5.2.18 (für Moduln) und 5.2.19 (für Matrizen) gilt:*

$$\textit{Existenzaussage ETS Moduln} \iff \textit{Existenzaussage ETS Matrizen},$$
$$\textit{Eindeutigkeitsaussage ETS Moduln} \iff \textit{Eindeutigkeitsaussage ETS Matrizen}.$$

BEWEIS. Im folgenden sei R ein Hauptidealring.

Existenz „⇒“: Sei $A \in Mat(m \times n, R)$ mit $A \neq 0$ gegeben, und $\varphi_A \colon R^{[n]} \longrightarrow R^{[m]}$ die davon induzierte lineare Abbildung. Dann ist $\mathrm{im}(\varphi_A) \subseteq R^{[m]}$ ein Untermodul des freien R-Moduls $R^{[m]}$. Wegen $A \neq 0$ ist $\mathrm{im}(\varphi_A) \neq \{0\}$, und somit kann auf $\mathrm{im}(\varphi_A) \subseteq R^{[m]}$ der Elementarteilersatz für Moduln (5.2.18) angewandt werden. Es gibt also eine Elementarteilerbasis $Y := (y_1, \ldots, y_m)$ des $R^{[m]}$ bzgl. des Untermoduls $\mathrm{im}(\varphi_A)$, so daß $\alpha_1 y_1, \ldots, \alpha_k y_k$ eine Basis von $\mathrm{im}(\varphi_A)$ ist mit $\alpha_i \in R$ und $\alpha_i \mid \alpha_{i+1}$ für $1 \leq i < k$.

Sei $\varphi\colon R^{[n]} \longrightarrow \mathrm{im}(\varphi_A)$ die von φ_A durch Einschränkung des Wertebereichs induzierte Abbildung, so daß gilt: $\mathrm{im}(\varphi) = \mathrm{im}(\varphi_A)$. Weiter seien $x_1, \ldots, x_k \in R^{[n]}$ Urbilder der $\alpha_i y_i \in \mathrm{im}(\varphi)$, d.h. es gilt $\varphi(x_i) = \alpha_i y_i$.
Dann ist nach Lemma 5.2.16 $F := \langle x_1, \ldots, x_k \rangle \subseteq R^{[n]}$ ein freier Modul mit der Basis $x_1, \ldots, x_k$, und es gilt $R^n = \ker(\varphi) \oplus F$.
$\ker(\varphi)$ ist als Untermodul des freien Moduls $R^{[n]}$ selbst frei (Satz 5.2.13), und nach Lemma 5.2.6 liefert dann eine Basis $v_1, \ldots, v_r$ von $\ker(\varphi)$ zusammengesetzt mit der Basis $x_1, \ldots, x_k$ von F eine Basis $X := (x_1, \ldots, x_k, v_1, \ldots, v_r)$ des $R^{[n]}$.
Die Matrizendarstellung von φ_A bzgl. der Basen X (des $R^{[n]}$) und Y (des $R^{[m]}$) ist dann nach obiger Konstruktion offensichtlich:

$$[\varphi_A]_{Y,X} = \begin{pmatrix} \alpha_1 & & & & \\ & \ddots & & & \\ & & \alpha_k & & \\ & & & 0 & \\ & & & & \ddots \\ & & & & & 0 \end{pmatrix} \quad \text{mit} \quad \alpha_i \mid \alpha_{i+1},$$

Aus $[\varphi_A]_{\mathcal{E}_m,\mathcal{E}_n}$ bzgl. der Standard-Basen $\mathcal{E}_n, \mathcal{E}_m$ folgt dann mit Lemma 3.4.28:

$$[\varphi_A]_{Y,X} = \underbrace{[\mathrm{id}_{R^{[m]}}]_{Y,\mathcal{E}_m}}_{=:S} \cdot \underbrace{[\varphi_A]_{\mathcal{E}_m,\mathcal{E}_n}}_{=A} \cdot \underbrace{[\mathrm{id}_{R^{[n]}}]_{\mathcal{E}_n,X}}_{=:T},$$

so daß zusammengefaßt mit $S \in \mathrm{GL}_m(R)$ und $T \in \mathrm{GL}_n(R)$ gilt:

$$SAT = \begin{pmatrix} \alpha_1 & & & & \\ & \ddots & & & \\ & & \alpha_k & & \\ & & & 0 & \\ & & & & \ddots \\ & & & & & 0 \end{pmatrix} \quad \text{mit} \quad \alpha_i \mid \alpha_{i+1}.$$

Existenz „$\Leftarrow$“: Sei M ein freier R-Modul vom Rang n und $U \subseteq M$ ein Untermodul mit $U \neq \{0\}$. Nach Satz 5.2.13 ist auch U ein freier Modul und $\mathrm{rg}_R(U) \leq \mathrm{rg}_R(M)$. Sei dann $y_1, \ldots, y_k$ eine Basis von U und $Z := (z_1, \ldots, z_n)$ eine Basis von M. Weiter sei auf der Standard-Basis $\mathcal{E}_k$ des $R^{[k]}$ durch lineare Fortsetzung die folgende lineare Abbildung definiert:

$$\varphi\colon R^{[k]} \longrightarrow M \quad \text{mit} \quad e_i \mapsto y_i.$$

Offensichtlich gilt $\mathrm{im}(\varphi) = U$.
Sei $A := [\varphi]_{Z,\mathcal{E}_k} \in \mathrm{Mat}(n \times k, R)$, und es folgt wegen $U \neq \{0\}$ sofort $A \neq 0$. Dann kann der Elementarteilersatz für Matrizen (Satz 5.2.19) auf A angewendet werden, und es existieren somit Matrizen $S \in \mathrm{GL}_n(R)$ und $T \in \mathrm{GL}_k(R)$ mit:

$$S[\varphi]_{Z,\mathcal{E}_k}T = SAT = \begin{pmatrix} \alpha_1 & & & & \\ & \ddots & & & \\ & & \alpha_r & & \\ & & & 0 & \\ & & & & \ddots \\ & & & & & 0 \end{pmatrix} \quad \text{mit} \quad \alpha_i \mid \alpha_{i+1} \text{ für } 1 \leq i < r.$$

Ist $S \in \mathrm{GL}_n(R)$ und die Basis Z von M gegeben, so gibt es eine (eindeutige) Basis $B := (b_1, \ldots, b_n)$ von M mit $S = [\mathrm{id}]_{B,Z}$, und analog gibt es für $T \in \mathrm{GL}_k(R)$ und die gegebene Basis $\mathcal{E}_k$ des $R^{[k]}$ darin (genau) eine Basis $C := (c_1, \ldots, c_k)$ mit $T = [\mathrm{id}]_{\mathcal{E}_k,C}$. Es gilt dann:

$$\begin{pmatrix} \alpha_1 & & & & \\ & \ddots & & & \\ & & \alpha_r & & \\ & & & 0 & \\ & & & & \ddots \\ & & & & & 0 \end{pmatrix} = S[\varphi]_{Z,\mathcal{E}_k}T = [\mathrm{id}]_{B,Z} \cdot [\varphi]_{Z,\mathcal{E}_k} \cdot [\mathrm{id}]_{\mathcal{E}_k,C} = [\varphi]_{B,C}.$$

Diese Matrizendarstellung von φ liefert sofort, daß $\varphi(c_1), \ldots, \varphi(c_r)$ eine Basis von $\mathrm{im}(\varphi) = U$ ist: es ist ein Erzeugendensystem, da die Bilder der anderen Basisvektoren $c_{r+1}, \ldots, c_k$ alle Null sind, und linear unabhängig, da deren Koordinatenvektoren $[\varphi(c_i)]_B$ offensichtlich linear unabhängig sind. Wegen $k = \mathrm{rg}_R(U)$ folgt dann noch $r = k$.

Ebenso folgt aus der Matrizendarstellung $[\varphi]_{B,C}$ sofort $\varphi(c_i) = \alpha_i b_i$ für $1 \leq i \leq k$. Damit ist $b_1, \ldots, b_n$ eine Elementarteilerbasis von M bzgl. U, da $\alpha_1 b_1, \ldots, \alpha_k b_k$ eine Basis von U ist und $\alpha_i \mid \alpha_{i+1}$ für $1 \leq i < k$ gilt.

Eindeutigkeit „⇒“: Sei $A \in \mathrm{Mat}(m \times n, R)$ mit $A \neq 0$, und es gebe Matrizen $S, \widetilde{S} \in \mathrm{GL}_m(R)$ und $T, \widetilde{T} \in \mathrm{GL}_n(R)$ mit:

$$SAT = \begin{pmatrix} \alpha_1 & & & & \\ & \ddots & & & \\ & & \alpha_k & & \\ & & & 0 & \\ & & & & \ddots \\ & & & & & 0 \end{pmatrix} \quad \text{mit} \quad \alpha_i \mid \alpha_{i+1} \text{ für } 1 \leq i < k$$

und

$$\widetilde{S}A\widetilde{T} = \begin{pmatrix} \beta_1 & & & & \\ & \ddots & & & \\ & & \beta_r & & \\ & & & 0 & \\ & & & & \ddots \\ & & & & & 0 \end{pmatrix} \quad \text{mit} \quad \beta_i \mid \beta_{i+1} \text{ für } 1 \leq i < r.$$

Es gibt Basen $B, \widetilde{B}$ des $R^{[m]}$ mit $S = [\mathrm{id}]_{B,\mathcal{E}_m}$ und $\widetilde{S} = [\mathrm{id}]_{\widetilde{B},\mathcal{E}_m}$ und Basen $C, \widetilde{C}$ des $R^{[n]}$ mit $T = [\mathrm{id}]_{\mathcal{E}_n,C}$ und $\widetilde{T} = [\mathrm{id}]_{\mathcal{E}_n,\widetilde{C}}$, und es folgt:

$$\begin{aligned} SAT &= [\mathrm{id}]_{B,\mathcal{E}_m} \cdot [\varphi_A]_{\mathcal{E}_m,\mathcal{E}_n} \cdot [\mathrm{id}]_{\mathcal{E}_n,C} = [\varphi_A]_{B,C}, \\ \widetilde{S}A\widetilde{T} &= [\mathrm{id}]_{\widetilde{B},\mathcal{E}_m} \cdot [\varphi_A]_{\mathcal{E}_m,\mathcal{E}_n} \cdot [\mathrm{id}]_{\mathcal{E}_n,\widetilde{C}} = [\varphi_A]_{\widetilde{B},\widetilde{C}}. \end{aligned}$$

Dann liefert die jeweilige Matrizendarstellung von $[\varphi_A]$ sofort, daß B und $\widetilde{B}$ Elementarteilerbasen des $R^{[m]}$ bzgl. $\mathrm{im}(\varphi_A)$ sind und $\alpha_1, \ldots, \alpha_k$ sowie $\beta_1, \ldots, \beta_r$ Elementarteiler von $\mathrm{im}(\varphi_A)$ bzgl. $R^{[m]}$. Nach dem Elementarteilersatz für Moduln (Satz 5.2.18) sind diese bis auf Einheiten eindeutig bestimmt, so daß $k = r$ folgt

und $\alpha_i \sim \beta_i$ für $1 \leq i \leq k$, womit die Eindeutigkeitsaussage für Matrizen bewiesen ist.

Eindeutigkeit „$\Leftarrow$“: Sei M ein freier R-Modul vom Rang n und $U \subseteq M$ ein Untermodul mit $U \neq \{0\}$. Weiter seien $Y := (y_1, \ldots, y_n)$ und $Z := (z_1, \ldots, z_n)$ Elementarteilerbasen von M bzgl. U mit den dazugehörigen Elementarteilern $\alpha_1, \ldots, \alpha_k$ und $\beta_1, \ldots, \beta_r$ von U bzgl. M, d.h. es gilt $\alpha_i \mid \alpha_{i+1}$ für $1 \leq i < k$ und $\beta_i \mid \beta_{i+1}$ für $1 \leq i < r$. Es folgt sofort $r = k$, da der Rang von U eindeutig bestimmt ist.

Es seien folgende durch lineare Fortsetzung auf den Basen definierte Abbildungen betrachet ($\mathcal{E}_k = (e_1, \ldots, e_k)$ die Standard-Basis auf dem $R^{[k]}$):

$$\varphi_1 \colon R^{[k]} \longrightarrow M \quad \text{mit} \quad e_i \mapsto \alpha_i y_i,$$
$$\varphi_2 \colon R^{[k]} \longrightarrow M \quad \text{mit} \quad e_i \mapsto \beta_i z_i.$$

Offensichtlich gilt $\operatorname{im}(\varphi_1) = U = \operatorname{im}(\varphi_2)$.

φ_1 und φ_2 besitzen folgende Matrizendarstellungen:

$$[\varphi_1]_{Y,\mathcal{E}_k} = \begin{pmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_k \end{pmatrix} \quad \text{und} \quad [\varphi_2]_{Z,\mathcal{E}_k} = \begin{pmatrix} \beta_1 & & \\ & \ddots & \\ & & \beta_k \end{pmatrix},$$

wobei zusätzlich $\alpha_i \mid \alpha_{i+1}$ und $\beta_i \mid \beta_{i+1}$ gilt.

Da φ_2 die Basis $\mathcal{E}_k$ des $R^{[k]}$ auf die Basis $\beta_1 z_1, \ldots, \beta_k z_k$ von $U = \operatorname{im}(\varphi_2)$ abbildet, ist es ein Isomorphismus von $R^{[k]}$ nach U, und es gibt eindeutig bestimmte Urbilder $v_1, \ldots, v_k$ der Basis $\alpha_1 y_1, \ldots, \alpha_k y_k$ von U unter φ_2, und $V := (v_1, \ldots, v_k)$ ist eine Basis des $R^{[k]}$. Sei dann $\psi \colon R^{[k]} \longrightarrow R^{[k]}$ die lineare Fortsetzung der Abbildung:

$$\varphi \colon R^{[k]} \longrightarrow R^{[k]} \quad \text{mit} \quad e_i \mapsto v_i.$$

Dann gilt $\varphi_1 = \varphi_2 \circ \psi$, und es folgt:

$$[\varphi_1]_{Y,\mathcal{E}_k} = [\varphi_2 \circ \psi]_{Y,\mathcal{E}_k} = [\mathrm{id}]_{Y,Z} \cdot [\varphi_2]_{Z,\mathcal{E}_k} \cdot [\psi]_{\mathcal{E}_k,\mathcal{E}_k},$$

so daß sich sofort ergibt:

$$\begin{pmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_k \end{pmatrix} = [\varphi_1]_{Z,\mathcal{E}_k} = [\mathrm{id}]_{Y,Z} \cdot [\varphi_2]_{Z,\mathcal{E}_k} \cdot [\psi]_{\mathcal{E}_k,\mathcal{E}_k} = \underbrace{[\mathrm{id}]_{Y,Z}}_{=:S} \cdot \begin{pmatrix} \beta_1 & & \\ & \ddots & \\ & & \beta_k \end{pmatrix} \cdot \underbrace{[\psi]_{\mathcal{E}_k,\mathcal{E}_k}}_{=:T} \cdot$$

Die Matrix $[\varphi_2]_{Z,\mathcal{E}_k}$ ist schon eine Smith-Normalform, und sie kann in die weitere Smith-Normalform $[\varphi_1]_{Y,\mathcal{E}_k}$ überführt werden, so daß aus dem Elementarteilersatz für Matrizen (Satz 5.2.19) sofort $\alpha_i \sim \beta_i$ für $1 \leq i \leq k$ folgt. □

LEMMA 5.2.25. *Sei R ein Integritätsring und M ein freier R-Modul mit einer Basis $x_1, \ldots, x_n$. Weiter seien $\alpha_1, \ldots, \alpha_k \in R \setminus \{0\}$ und $U \subseteq M$ der freie Untermodul $U := \langle \alpha_1 x_1, \ldots, \alpha_k x_k \rangle$. Dann gibt es einen R-Modulisomorphismus:*

$$M/U = \prod_{i=1}^{k} R/(\alpha_i)_R \times R^{n-k}. \qquad \square$$

LEMMA 5.2.26. *Sei R ein Hauptidealring und M ein R-Modul mit:*

$$M \cong \prod_{i=1}^{k} R/(\alpha_i)_R \quad \text{und} \quad \alpha_1, \ldots, \alpha_k \in R \setminus \{0\} \text{ Nicht-Einheiten mit } \alpha_i \mid \alpha_{i+1}.$$

Dann sind $a_1, \ldots, a_k$ bis auf Einheiten eindeutig bestimmt, d.h. für eine Zerlegung:

$$M \cong \prod_{j=1}^{r} R/(\beta_i)_R \quad \text{und} \quad \beta_1, \ldots, \beta_r \in R \setminus \{0\} \text{ Nicht-Einheiten mit } \beta_i \mid \beta_{i+1}$$

folgt $k = r$ und $a_i \sim b_i$. □

Aus den Konstruktionen im Beweis von Lemma 5.2.24 ergibt sich sofort folgende Aussage:

LEMMA 5.2.27. *Ist R ein Hauptidealring, und sind M, N freie R-Moduln endlichen Ranges, so gilt für eine lineare Abbildung $\varphi\colon M \longrightarrow N$:*

Ist A eine Matrizendarstellung von φ, so hat A die gleichen Elementarteiler wie $\operatorname{im}(\varphi)$ bzgl. N. □

Lemma 5.2.27 liefert sofort ein Verfahren, wie in speziellen Fällen die Elementarteiler eines Moduls berechnet werden können:

BEMERKUNG 5.2.28. *Sei M ein freier Modul endlichen Ranges über dem Hauptidealring R, und es sei $U \subseteq M$ ein Untermodul, der von den Elementen $x_1, \ldots, x_k$ erzeugt wird. Dann läßt sich sofort folgende lineare Abbildung zwischen freien R-Moduln konstruieren mit $\operatorname{im}(\varphi) = U$:*

$$\varphi\colon R^k \longrightarrow M \quad \text{mit} \quad e_i \mapsto x_i.$$

Ist dann B ein Basis von M, so liefert Lemma 5.2.27, daß die Elementarteiler von U bzgl. M gleich den Elementarteilern der Matrizendarstellung $[\varphi]_{B,\mathcal{E}_k}$ sind.
Für das Beispiel $U := \langle \binom{1}{2}, \binom{3}{4} \rangle \subseteq \mathbb{Z}^{[2]}$ folgt dann, daß obiges φ die Form:

$$\varphi\colon \mathbb{Z}^{[2]} \longrightarrow \mathbb{Z}^{[2]} \quad \text{mit} \quad \binom{1}{0} \mapsto \binom{1}{2}, \quad \binom{0}{1} \mapsto \binom{3}{4}$$

hat und bzgl. der Standard-Basis $\mathcal{E}_2$ eine Matrizendarestellung:

$$[\varphi]_{\mathcal{E}_2,\mathcal{E}_2} = \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix}.$$

Nun muß $[\varphi]_{\mathcal{E}_2,\mathcal{E}_2}$ in ihre Smith-Normalform überführt werden, um die Elementarteiler zu finden:

$$\begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} \quad \rightsquigarrow \quad \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}.$$

Also hat U in $\mathbb{Z}^{[2]}$ die Elementarteiler $1, 2$.
Die Umformung von $[\varphi]_{\mathcal{E}_2,\mathcal{E}_2}$ in seine Smith-Normalform kann folgendermaßen beschrieben werden:

$$\underbrace{\begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix}}_{=:S} \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} \underbrace{\begin{pmatrix} 1 & -3 \\ 0 & 1 \end{pmatrix}}_{=:T} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}.$$

Nach dem Beweis von Lemma 5.2.24 gibt es eine Basis B von $\mathbb{Z}^2$ mit $S = [\mathrm{id}]_{B,\mathcal{E}_2}$, und dieses B ist eine Elementarteilerbasis von $\mathbb{Z}^2$ bzgl. U. Dabei kann in diesem Fall B leicht aus den Spalten von $S^{-1} = [\mathrm{id}]_{\mathcal{E}_2,B}$ abgelesen werden:

$$S^{-1} = \begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix} \quad \Longrightarrow \quad \text{Elementarteilerbasis von } M \text{ bzgl. } U\text{: } \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \end{pmatrix}. \quad \square$$

DEFINITION 5.2.29. *Sei R ein Hauptidealring und M ein endlich erzeugter R-Modul. Eine endliche Präsentation von M ist dann eine Kette von Abbildungen:*

$$N \xrightarrow{\psi} P \xrightarrow{\varphi} M,$$

wobei N und P freie R-Moduln endlichen Ranges sind, und zusätzlich gilt:

$$\varphi \text{ ist surjektiv} \quad \text{und} \quad \mathrm{im}(\psi) = \ker(\varphi).$$

Die Elementarteiler der endlichen Präsentation sind dann die Elementarteiler von $\ker(\varphi)$ bzgl. P. $\square$

BEMERKUNG 5.2.30. *Ist R ein Hauptidealring, M ein endlich erzeugter R-Modul eine endliche Präsentation von M gegeben durch:*

$$N \xrightarrow{\psi} P \xrightarrow{\varphi} M,$$

so gilt nach Lemma 5.2.27 für eine Matrizendarstellung A von ψ, daß die Elementarteiler der endlichen Präsentation gleich den Elementarteilern von A sind. $\square$

SATZ 5.2.31. *(Klassifikation endlich erzeugter Moduln über Hauptidealringen) Sei R ein Hauptidealring und M ein endlich erzeugter R-Modul. Weiter sei $F \subseteq M$ ein freier R-Modul eindeutig bestimmten Ranges mit (siehe Satz 5.2.17):*

$$M = F \oplus M_{Tor}.$$

Dann gibt es Nicht-Einheiten $\alpha_1, \ldots, \alpha_k \in R \setminus \{0\}$ mit $\alpha_i \mid \alpha_{i+1}$ für $1 \leq i \leq k$, so daß gilt:

$$M_{Tor} \cong \prod_{i=1}^{k} R/(\alpha_i)_R.$$

Die Elemente $\alpha_1, \ldots, \ldots, \alpha_k$ sind bis auf Einheiten eindeutig bestimmt.

LEMMA 5.2.32. *Sei R ein Hauptidealring und M ein endlich erzeugter R-Modul. Weiter seien $\alpha_1, \ldots, \alpha_k \in R \setminus \{0\}$ die nach Satz 5.2.31 bis auf Einheiten eindeutig bestimmten Nicht-Einheiten mit $\alpha_i \mid \alpha_{i+1}$ für $1 \leq i < k$, so daß gilt:*

$$M \cong M_{Tor} \oplus F \quad \text{mit} \quad M_{Tor} \cong \prod_{i=1}^{k} R/(\alpha_i)_R \text{ und } F \text{ freier } R\text{-Modul.}$$

Ist eine endliche Präsentation von M gegeben der Form (siehe Definition 5.2.29):

$$N \xrightarrow{\psi} P \xrightarrow{\varphi} M,$$

und ist A eine Matrizendarstellung von ψ mit einer Smith-Normalform (SNF):

$$A \xrightarrow{SNF} \begin{pmatrix} \boxed{\begin{matrix} \beta_1 & & \\ & \ddots & \\ & & \beta_r \end{matrix}} & \\ & \end{pmatrix} \in \mathrm{Mat}(m \times n, R),$$

so folgt $\mathrm{rg}_R(F) = m - r$, und die Nicht-Einheiten $\beta_j, \ldots, \beta_r$ unter den $\beta_1, \ldots, \beta_r$ sind assoziert zu den obigen Elementen $\alpha_1, \ldots, \alpha_k$, d.h. es gilt:

$$\alpha_1 \sim \beta_j,\ \alpha_2 \sim \beta_{j+1},\ \ldots\ , \alpha_k \sim \beta_r.$$

Beweis.
Da φ surjektiv ist, gilt nach dem Homomorphie-Satz 2.1.31:

$$M \cong P/\ker(\varphi),$$

und aus $\ker(\varphi) = \mathrm{im}(\psi)$ folgt sofort:

$$M \cong P/\mathrm{im}(\psi).$$

Nach Bemerkung 5.2.30 sind die Elementarteiler $\beta_1, \ldots, \beta_r$ von A gleich den Elementarteilern der endlichen Präsentation, also die von $\ker(\varphi) = \mathrm{im}(\psi)$ bzgl. P.
Ist $A \in \mathrm{Mat}(m \times n, R)$, so gilt $\mathrm{rg}_R(N) = n$ und $\mathrm{rg}_R(P) = m$. Sei dann $x_1, \ldots, x_m$ eine Elementarteilerbasis von P bzgl. $\mathrm{im}(\psi)$ zu den Elementarteilern $\beta_1, \ldots, \beta_r$ von $\mathrm{im}(\psi)$ bzgl. P. Dann gilt nach Lemma 5.2.25:

$$P/\mathrm{im}(\psi) = \langle x_1, \ldots, x_m \rangle / \langle \beta_1 x_1, \ldots, \beta_r x_r \rangle \overset{5.2.25}{\cong} \prod_{i=1}^{r} R/(\beta_i)_R \times R^{m-r}.$$

Wegen $\beta_i \mid \beta_{i+1}$ gibt es ein $1 < j \leq n$, so daß $\beta_1, \ldots, \beta_{j-1}$ Einheiten und $\beta_j, \ldots, \beta_r$ Nicht-Einheiten unter den Elementarteilern von $\mathrm{im}(\psi)$ sind.
Für Einheiten β_i gilt $(\beta_i)_R = R$ und somit $R/(\beta_i)_R = \{0\}$, so daß folgt:

$$P/\mathrm{im}(\psi) \cong \prod_{i=j}^{r} R/(\beta_i)_R \times R^{m-r}. \qquad (*)$$

Es gilt offensichtlich:

$$\Big(\prod_{i=j}^{r} R/(\beta_i)_R \times R^{m-r} \Big)_{\mathrm{Tor}} = \prod_{i=j}^{r} R/(\beta_i)_R,$$

so daß der Isomorphismus $(*)$ eine Zerlegung von $P/\mathrm{im}(\psi)$ induziert der Form:

$$P/\mathrm{im}(\psi) = \big(P/\mathrm{im}(\psi)\big)_{\mathrm{Tor}} \oplus \widetilde{F} \quad \text{mit} \quad \big(P/\mathrm{im}(\psi)\big)_{\mathrm{Tor}} \cong \prod_{i=j}^{r} R/(\beta_i)_R, \quad \widetilde{F} \cong R^{m-r}.$$

Jeder Isomorphismus $M \cong P/\mathrm{im}(\psi)$ bildet die jeweiligen Torsionsuntermoduln aufeinander ab, und es folgt:

$$M_{\mathrm{Tor}} \cong \prod_{i=1}^{k} R/(\alpha_i)_R \quad \text{und} \quad M_{\mathrm{Tor}} \cong \big(P/\mathrm{im}(\psi)\big)_{\mathrm{Tor}} \cong \prod_{i=j}^{r} R/(\beta_i)_R,$$

womit die Eindeutigkeitsaussage des Klassifikationssatzes 5.2.31 dann wie behauptet liefert:

$$\alpha_1 \sim \beta_j, \ldots, \alpha_k \sim \beta_r.$$

Ein Isomorphismus $\Psi\colon P/\operatorname{im}(\psi) \longrightarrow M$ liefert eine Zerlegung:

$$M = \Psi\big(P/\operatorname{im}(\psi)\big) = \underbrace{\Psi\Big(\big(P/\operatorname{im}(\psi)\big)_{\mathrm{Tor}}\Big)}_{=M_{\mathrm{Tor}}} \oplus \Psi(\widetilde{F}) \quad \text{mit} \quad \Psi(\widetilde{F}) \text{ frei},$$

und nach der Eindeutigkeit des Ranges in einer solchen Zerlegung von M (Satz 5.2.17) gilt dann $\operatorname{rg}_R(F) = \operatorname{rg}_R\big(\Psi(\widetilde{F})\big)$. Dies liefert letztendlich die gewünschte Implikation:

$$\Psi(\widetilde{F}) \cong \widetilde{F} \cong R^{m-r} \quad \Longrightarrow \quad \operatorname{rg}_R(F) = m - r. \qquad \square$$

BEMERKUNG 5.2.33. *Es kann gezeigt werden, daß die freien Moduln F, die in einer Zerlegung*

$$M = F \oplus M_{Tor}$$

in obigem Satz auftreten können, alle maximale freie Untermoduln in F sind, und dabei maximal in doppeltem Sinne:

- *Maximal in dem Sinne, daß sie nicht in einem größeren freien Untermodul von M liegen.*
- *Maximal in dem Sinne, daß es keinen freien Untermodul in M gibt, der einen größeren Rang als F hat (nach Satz 5.2.17 ist der Rang eines F mit obiger Eigenschaft eindeutig bestimmt).*

In M können aber maximale freie Untermoduln existieren, die sich nicht mit M_{Tor} zum ganzen Modul ergänzen lassen: Beispiele wären die $\mathbb{Z}$-Untermoduln $\langle p\rangle \subseteq \mathbb{Z}$ für Primzahlen p, die jeweils in beiden Kontexten maximal sind. $\square$

SATZ 5.2.34. *(Klassifikation endlicher abelscher Gruppen)*
Sei G eine endliche abelsche Gruppe und $n := |G|$. Dann gibt es eindeutig bestimmte Zahlen $d_1, \ldots, d_k \in \mathbb{N}$ mit $d_i > 1$, so daß gilt:

$$d_i \mid d_{i+1} \text{ für } 1 \le i \le k, \quad d_1 \cdot \ldots \cdot d_k = n \quad \text{und} \quad G \cong \mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_k}.$$

Wird dann für einen Gruppe G mit $[G]$ die Äquivalenzklasse aller zu ihr isomorphen Gruppe bezeichnet, so induziert die Zuordnung:

$$G \overset{s.o.}{\cong} \mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_k} \;\mapsto\; (d_1, \ldots, d_k)$$

eine Bijektion zwischen den folgenden Mengen:

$$\{\, [G] \mid G \text{ abelsche Gruppe der Ordnung } n \,\}$$
$$\downarrow$$
$$\{\, (d_1, \ldots, d_k) \mid k \in \mathbb{N},\ d_i > 1,\ d_i \mid d_{i+1},\ d_1 \cdot \ldots \cdot d_k = n \,\}. \qquad \square$$

BEWEIS.
Ist G eine abelsche Gruppe, so wird G durch folgende skalare Multiplikation zu einem $\mathbb{Z}$-Modul:

$$\bullet\colon \mathbb{Z} \times G \longrightarrow G \quad \text{mit} \quad z \bullet g := g^n.$$

Ist G eine endliche Gruppe mit $n := |G|$, so ist dieser offensichtlich endlich erzeugt als Modul über dem Hauptidealring $\mathbb{Z}$, und aus Lemma 1.2.7 und dem Satz von Lagrange 1.2.20 folgt sofort die Aussage:

$$g^n = e_G \text{ für alle } g \in G,$$

so daß dann G ein $\mathbb{Z}$-Torsionsmodul ist, d.h. $G = G_{\text{Tor}}$.
Nach dem Klassifikationssatz 5.2.31 für endlich erzeugte Moduln über Hauptidealringen gibt es dann eindeutig bestimmte Zahlen $d_1, \ldots, d_k \in \mathbb{N}$ mit $d_i > 1$ und $d_i \mid d_{i+1}$, so daß gilt:

$$G = G_{\text{Tor}} \cong \mathbb{Z}/(d_1)_{\mathbb{Z}} \times \ldots \times \mathbb{Z}/(d_k)_{\mathbb{Z}} = \mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_k}.$$

Des weiteren gilt:

$$|\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_k}| = d_1 \cdot \ldots \cdot d_k \quad \Longrightarrow \quad d_1 \cdot \ldots \cdot d_k = n.$$

Es bleibt zu zeigen, daß für $G \cong \mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_k}$ die Zuordnung

$$\Psi_n\colon [G] \mapsto (d_1, \ldots, d_k)$$

eine Bijektion zwischen den folgenden Mengen ist:

$$\{\, [G] \mid G \text{ abelsche Gruppe der Ordnung } n \,\}$$
$$\downarrow$$
$$\{\, (d_1, \ldots, d_k) \mid k \in \mathbb{N},\ d_i > 1,\ d_i \mid d_{i+1},\ d_1 \cdot \ldots \cdot d_k = n \,\}.$$

Ψ_n wohldefiniert: Für zwei endliche abelsche Gruppen G und H gelte $[G] = [H]$. Dann sind die beiden Gruppen nach der Definition der Äquivalenzrelation isomorph: $G \cong H$.
Nach obiger Klassifikation endlicher abelscher Gruppen gibt es eindeutig bestimmte Elemente $a_1, \ldots, a_k \in \mathbb{N}$ und $b_1, \ldots, b_r \in \mathbb{N}$ mit $a_i \mid a_{i+1}$ und $b_i \mid b_{i+1}$ sowie:

$$\mathbb{Z}_{a_1} \times \ldots \times \mathbb{Z}_{a_k} \cong G \cong H \cong \mathbb{Z}_{b_1} \times \ldots \times \mathbb{Z}_{b_r},$$

woraus dann

$$\mathbb{Z}_{a_1} \times \ldots \times \mathbb{Z}_{a_k} \cong \mathbb{Z}_{b_1} \times \ldots \times \mathbb{Z}_{b_r},$$

folgt, welches wegen der Eindeutigkeitsaussage aus der Klassifikation endlicher abelscher Gruppen sofort liefert:

$$k = r \quad \text{und} \quad a_1 = b_1, \ldots, a_k = b_k.$$

Damit ist die Abbildung Ψ_n wohldefiniert wegen:

$$\Psi_n\big([G]\big) = (a_1, \ldots, a_k) = (b_1, \ldots, b_r) = \Psi_n\big([H]\big).$$

Ψ_n injektiv: Es seien G, H endliche abelsche Gruppen mit:

$$\Psi_n\big([G]\big) = (d_1, \ldots, d_k) = \Psi_n\big([H]\big).$$

Dann gilt nach der Definition von Ψ_n:

$$G \cong \mathbb{Z}_{d_1} \times \ldots \times Z_{d_k} \cong H \quad \Longrightarrow \quad G \cong H \quad \Longrightarrow \quad [G] = [H].$$

Ψ_n surjektiv: Für $G := \mathbb{Z}_{d_1} \times \ldots \times \mathbb{Z}_{d_k}$ mit $d_i \mid d_{i+1}$ gilt per Definition:

$$\Psi_n(G) = (d_1, \ldots, d_k).$$ □

Beispiel 5.2.35.

i.) Sei G eine endlich erzeugte abelsche Gruppe mit einer endlichen Präsentation:

$$N \xrightarrow{\psi} P \xrightarrow{\varphi} G.$$

Weiter sei A eine Matrizendarstellung von ψ mit einer Smith-Normalform:

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

Dann folgt mit Lemma 5.2.32:

$$G \cong \mathbb{Z}^2 \times \mathbb{Z}_2 \times \mathbb{Z}_4.$$

ii.) Die Anzahl aller abelschen Gruppen (bis auf Isomorphie) der Ordnung 24 ist nach Satz 5.2.34 gegeben durch die Anzahl der möglichen Tupel:

$$(d_1, \ldots, d_k) \quad \textit{mit} \quad d_1 > 1,\ d_1 \cdot \ldots \cdot d_k = 24,\ d_i \mid d_{i+1}.$$

Alle Möglichkeiten dazu sind:

$$(24),\ (2, 12),\ (2, 2, 6).$$

Somit ist eine abelschen Gruppen der Ordnung 24 isomorph zu einer der folgenden Gruppen:

$$\mathbb{Z}_{24}, \quad \mathbb{Z}_2 \times \mathbb{Z}_{12}, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6.$$ □

5.3. Konjugationsklassen quadratischer Matrizen

Bemerkung 5.3.1.

i.) Sei K ein Körper und V ein endlich-dimensionaler K-Vektorraum. Für ein $\varphi \in \mathrm{End}_K(V)$ liefert folgende Definition einer skalaren Multiplikation eine $K[t]$-Modulstruktur auf V:

$$\bullet\colon K[t] \times V \longrightarrow V \quad \textit{mit} \quad p(t) \bullet v := p(\varphi)(v).$$

Diese $K[t]$-Modulstruktur auf V kann auch beschrieben werden durch folgenden Ringhomomorphismus:

$$\Psi_\varphi\colon K[t] \longrightarrow \mathrm{End}_K(V) \quad \textit{mit} \quad p \mapsto p(\varphi).$$

ii.) Sei K ein Körper und $A \in \mathrm{Mat}_n(K)$. Dann ist die folgende Abbildung ein Ringhomomorphismus:

$$\Phi_A\colon K[t] \longrightarrow \mathrm{Mat}_n(K) \quad \textit{mit} \quad p \mapsto p(A).$$

iii.) Sei K ein Körper und $A \in \mathrm{Mat}_n(K)$. Auf dem K-Vektorraum $K^{[n]}$ ist durch folgende Definition einer skalaren Multiplikation eine $K[t]$-Modulstruktur definiert:

$$\bullet\colon K[t] \times K^{[n]} \longrightarrow K^{[n]} \quad \textit{mit} \quad p(t) \bullet x := p(A) \cdot x.$$

Weiter sei Φ der folgende Ringisomorphismus aus Satz 3.1.20:

$$\Phi\colon \mathrm{Mat}_n(K) \longrightarrow \mathrm{End}_K(K^{[n]}) \quad \textit{mit} \quad A \mapsto \varphi_A.$$

Dann ist folgendes Diagramm von Ringhomomorphismen kommutativ:

$$\begin{array}{ccc} K[t] & \xrightarrow{\Phi_A} & \mathrm{Mat}_n(K) \\ & \searrow^{\Psi_{\varphi_A}} & \downarrow \Phi \\ & & \mathrm{End}_K(K^{[n]}) \end{array} \qquad \textit{mit} \quad \Psi_{\varphi_A} = \Phi \circ \Phi_A.$$

Die obige $K[t]$-Modulstruktur auf $K^{[n]}$ bzgl. A entspricht dabei der durch Ψ_{φ_A} gegebenen $K[t]$-Modulstruktur, d.h es gilt:

$$p \bullet x \overset{(K[t]\text{-Mod. durch } A)}{=} p(A) \cdot x = p(\varphi_A)(x) \overset{(K[t]\text{-Mod. durch } \Psi_{\varphi_A})}{=} p \bullet x.$$

Entscheidend dabei ist, daß durch den Ringisomorphismus $A \mapsto \varphi_A$ offensichtlich folgende Gleichung gilt:

$$\varphi_{p(A)} = p(\varphi_A).$$ □

Definition 5.3.2. *Sei K ein Körper und V ein endlich-dimensionaler K-Vektorraum. Für ein $\varphi \in \mathrm{End}_K(V)$ sei denn die in Bemerkung 5.3.1 auf V durch den Ringhomomorphismus:*

$$\Psi_\varphi\colon K[t] \longrightarrow \mathrm{End}_K(V) \quad \textit{mit} \quad p(t) \mapsto p(\varphi)$$

definierte $K[t]$-Modulstruktur mit V_φ bezeichnet.
Für eine Matrix $A \in \mathrm{Mat}_n(K)$ sei die in Bemerkung 5.3.1 auf $K^{[n]}$ durch den Ringhomomorphismus:

$$\Psi_{\varphi_A}\colon K[t] \longrightarrow \mathrm{End}_K(K^{[n]}) \quad \textit{mit} \quad p(t) \mapsto p(\varphi_A)$$

definerte $K[t]$-Modulstruktur mit $K_A^{[n]}$ bezeichnet. □

Bemerkung 5.3.3.

i.) Es gilt für $A \in \mathrm{Mat}_n(K)$ nach Bemerkung 5.3.1:

$$K_A^{[n]} = (K^{[n]})_{\varphi_A}.$$

ii.) Sei K ein Köper und V ein endlich-dimensionaler K-Vektorraum. Für einen Endomorphismus $\varphi \in \mathrm{End}_K(V)$ ist der Ringhomomorphismus:

$$\Psi_\varphi\colon K[t] \longrightarrow \mathrm{End}_K(V) \quad \textit{mit} \quad p(t) \mapsto p(\varphi)$$

auch K-linear, d.h. ein Vektorraumhomomorphismus zwischen den K-Vektorräumen $K[t]$ und $\mathrm{End}_K(V)$.

Für $A \in \mathrm{Mat}_n(K)$ ist der Ringhomomorphismus:

$$\Phi_A\colon K[t] \longrightarrow \mathrm{Mat}_n(K) \quad \textit{mit} \quad A \mapsto p(A)$$

auch K-linear, d.h. ein Vektorraumhomomorphismus zwischen den K-Vektorräumen $K[t]$ und $\mathrm{Mat}_n(K)$. □

LEMMA 5.3.4. *Sei K ein Körper und V ein endlich-dimensionaler K-Vektorraum. Für ein $\varphi \in \mathrm{End}_K(V)$ ist der Ringhomomorphismus:*

$$\Psi_\varphi \colon K[t] \longrightarrow \mathrm{End}_K(V) \quad \textit{mit} \quad p(t) \mapsto p(\varphi)$$

nicht injektiv, und V_φ ist ein endlich erzeugter $K[t]$-Torsionsmodul.
Für $A \in \mathrm{Mat}_n(K)$ ist der folgende Ringhomomorphismus nicht injektiv:

$$\Phi_A \colon K[t] \longrightarrow \mathrm{Mat}_n(K) \quad \textit{mit} \quad p(t) \mapsto p(A). \qquad \square$$

BEWEIS.
Eine injektive lineare Abbildung zwischen Moduln bildet linear unabhängige Systeme auf linear unabhängige Systeme ab (Hauptsatz über linerare Abbildungen und Basen 2.2.31). Die beiden Abbildungen Ψ_φ und Φ_A sind nach Bemerkung 5.3.3 auch lineare Abbildungen, und beide bilden den unendlich-dimensionalen K-Vektorraum $K[t]$ in einen endlich-dimensionalen K-Vektorraum ab, denn es gilt:

$$\dim_K \big(\mathrm{End}_K(V)\big) = \big(\dim_K(V)\big)^2 \quad \text{und} \quad \dim_K \big(\mathrm{Mat}_n(K)\big) = n^2.$$

Somit können Ψ_φ und Φ_A nicht injektiv sein, da in den Zielräumen das Bild der unendlichen Basis und damit des linear unabhängigen Systems $(1, t, \ldots, t^i, \ldots)$ unter diesen Abbildungen aus dimensionsgründen nicht linear uanbhängig sein kann.
Zu zeigen ist noch, daß V_φ ein endlich erzeugter $K[t]$-Modul ist. Da Ψ_φ nicht injektiv ist, gibt es ein $p \in \ker(\Psi_\varphi)$ mit $p \neq 0$. Die durch Ψ_φ auf V induzierte $K[t]$-Modulstruktur (siehe Bemerkung 5.3.1) liefert dann für alle $v \in V_\varphi$:

$$p \bullet v = \underbrace{\Psi_\varphi(p)}_{\text{Nullabb. } \bar{0}}(v) = \bar{0}(v) = 0,$$

und v ist somit ein Torsionselement und $V_\varphi = (V_\varphi)_{\mathrm{Tor}}$.
Wegen $K \subseteq K[t]$ ist außerdem jede K-Basis von V ein $K[t]$-Erzeugendensystem von V_φ, so daß V_φ auch endlich erzeugt ist. $\square$

BEMERKUNG 5.3.5. *Da für einen Körper K der Polynomring $K[t]$ ein Hauptidealring ist, wird ein Ideal $I \subseteq K$ darin von einen Element erzeugt: $I = (p)_{K[t]}$. Für jede Einheit $\alpha \in \big(K[t]\big)^* = K^*$ ist dann offensichtlich auch αp ein Erzeuger von I, so daß ein $I \neq \{0\}$ ein normiertes Polynom als Erzeuger besitzt.*
Sind $p, \widetilde{p}$ normierte Polynome, die $I \neq \{0\}$ erzeugen, so ist jedes dieser Polynome per Definition ein Vielfaches des anderen. Damit folgt sofort:

$$p = q\widetilde{p},\ \widetilde{p} = \widetilde{q}p \quad \Longrightarrow \quad p = (q\widetilde{q})p \quad \Longrightarrow \quad q\widetilde{q} \in \big(K[t]\big)^*.$$

Dann gilt $p = \varepsilon\widetilde{p}$ mit einer Einheit $\varepsilon \in (K[t])^* = K^*$, und es folgt $\varepsilon = 1$, da beide Polynome normiert sind.
Somit hat ein $I \neq \{0\}$ einen eindeutig bestimmten normierten Erzeuger. $\square$

DEFINITION 5.3.6. *Sei K ein Körper und V ein endlich-dimensionaler K-Vektorraum. Für $\varphi \in \mathrm{End}_K(V)$ heißt dann der eindeutig bestimmte Erzeuger des Hauptideals $\ker(\Psi_\varphi) \subseteq K[t]$ (siehe Lemma 5.3.4 und Bemerkung 5.3.5) das Mininalpolynom von φ und wird mit μ_φ bezeichnet.*
Ist $A \in \mathrm{Mat}_n(K)$, so heißt der nach Lemma 5.3.4 und Bemerkung 5.3.5 eindeutig bestimmte Erzeuger des Hauptideals $\ker(\Phi_A) \subseteq K[t]$ das Mininalpolynom von A und wird mit μ_A bezeichnet. $\square$

BEMERKUNG 5.3.7. *Für $A \in \mathrm{Mat}_n(K)$ gilt: $\mu_A = \mu_{\varphi_A}$.* □

LEMMA 5.3.8. *Sei V ein n-dimensioaler K-Vektorraum und $\varphi \in \mathrm{End}_K(V)$. Dann gilt für den $K[t]$-Modul V_φ und seine durch $\Psi_\varphi\colon K[t] \longrightarrow \mathrm{End}_K(V)$ gegebene $K[t]$-Modulstruktur:*

$$\ker(\Psi_\varphi) = \mathrm{Ann}_{K[t]}(V_\varphi).$$

Ist $v_1, \ldots, v_n$ eine K-Basis von V und damit ein $K[t]$-Erzeugendensystem von V_φ, und gilt $\mathrm{Ann}_{K[t]}(v_i) = (p_i)_{K[t]}$ so folgt:

$$\mathrm{Ann}_{K[t]}(V_\varphi) = \big(\mathrm{kgV}(p_1, \ldots, p_n)\big)_{K[t]} \quad \textit{und damit:} \quad \mu_\varphi = \mathrm{kgV}(p_1, \ldots, p_n).$$

Dazu muß der kgV *der p_i evt. normiert werden. Ein p_i läßt sich bestimmen durch die kleinste nicht-triviale Relation,*

$$\sum_{j=1}^{k} \alpha_j \varphi^j(v_i) = 0,$$

die sich ergibt, ein minimales k zu finden, so daß die Vektoren

$$v_i, \varphi(v_i), \varphi^2(v_i), \ldots, \varphi^k(v_i)$$

linear abhängig werden. Dann ist insbesondere $\alpha_k \neq 0$ und

$$p_i := \frac{1}{\alpha_k} \sum_{j=1}^{k} \alpha_j t^j$$

ein normierter Erzeuger von $\mathrm{Ann}_{K[t]}(v_i)$.
Ist $A \in \mathrm{Mat}_n(K)$, so gilt $\mu_A = \mu_{\varphi_A}$, und μ_A kann nach obgien Schema bestimmt werden, indem für eine Basis $x_1, \ldots, x_n$ des $K^{[n]}$ jeweils $\mathrm{Ann}_{K[t]}(x_i) = (p_i)_{K[t]}$ bestimmt wird durch die Suche eines minimalen k, so daß

$$x_i, Ax_i, A^2x_i, \ldots, A^kx_i$$

linear abhängig wird. Es gilt dann analog $\mu_A = \mathrm{kgV}(p_1, \ldots, p_n)$. □

SATZ 5.3.9. *Sei V ein n-dimensionaler K-Vektorraum, und seien $\varphi, \psi \in \mathrm{End}_K(V)$. Dann sind folgende Aussagen äquivalent:*

$$\varphi \textit{ und } \psi \textit{ sind konjugiert} \iff \begin{array}{l} V_\varphi \textit{ und } V_\psi \textit{ sind isomorphe} \\ K[t]\textit{-Moduln.} \end{array}$$

Dabei gilt sogar spezieller:

$$\psi = \xi \circ \varphi \circ \xi^{-1} \textit{ mit } \xi \in \mathrm{GL}_K(V) \iff \begin{array}{l} \xi\colon V_\varphi \longrightarrow V_\psi \textit{ ist ein} \\ K[t]\textit{-Modulisomorphismus.} \end{array}$$

Für eine Matrix $A \in \mathrm{Mat}_n(K)$ und Basis $\mathcal{D}$ von V sind folgende Aussagen äquivalent:

$$A = [\varphi]_{\mathcal{D},\mathcal{D}} \iff \begin{array}{l} [\,\cdot\,]_{\mathcal{E}_n,\mathcal{D}}\colon V_\varphi \longrightarrow K_A^{[n]} \textit{ ist ein} \\ K[t]\textit{-Modulisomorphismus.} \end{array}$$

Für zwei Matrizen $A, B \in \mathrm{Mat}_n(K)$ gilt:

$$A \textit{ und } B \textit{ sind konjugiert} \iff \begin{array}{l} K_A^{[n]} \textit{ und } K_B^{[n]} \textit{ sind isomorphe} \\ K[t]\textit{-Moduln.} \end{array}$$

□

BEMERKUNG 5.3.10. *In der Situtation von Satz 5.3.9 sind die auftretenden $K[t]$-Moduln V_φ, V_ψ, $K_A^{[n]}$ und $K_B^{[n]}$ nach Lemma 5.3.4 alles endlich erzeugte Torsionsmoduln über den Hauptidealring $K[t]$, so daß sie nach dem Klassifikationssatz 5.2.31 alle isomorph sind zu jeweils einem Modul der Form:*

$$\prod_{i=1}^{k} K[t]/(\alpha_i)_{K[t]},$$

wobei $\alpha_1, \ldots, \alpha_k \in K[t]$ eindeutig bestimmte normierte Nicht-Einheiten sind mit $\alpha_i \mid \alpha_{i+1}$. Dabei gilt dann:

$$\prod_{i=1}^{k} K[t]/(\alpha_i)_{K[t]} \cong \prod_{i=1}^{r} K[t]/(\beta_i)_{K[t]} \quad \Longleftrightarrow \quad k = r \text{ und } \alpha_1 = \beta_1, \ldots, \alpha_k = \beta_k.$$

Sind dann z.B. für die beiden $K[t]$-Moduln $K_A^{[n]}$ und $K_B^{[n]}$ die Größen $\alpha_1, \ldots, \alpha_k$ und $\beta_1, \ldots, \beta_r$ aus obigen Zerlegungen bekannt, so sind A und B genau dann konjugiert, wenn $k = r$ und jeweils $\alpha_i = \beta_i$ gilt.
$\alpha_1, \ldots, \alpha_k$ können nach Lemma 5.2.32 aus einer endlichen Präsentation von $K_A^{[n]}$ gewonnen werden. □

SATZ 5.3.11. *Sei K ein Körper und $A \in \mathrm{Mat}_n(K)$. Dann ist eine endliche Präsentation des $K[t]$-Moduls $K_A^{[n]}$ gegeben durch folgende Kette von $K[t]$-Modulhomomorphismen:*

$$\big(K[t]\big)^n \xrightarrow{\psi} \big(K[t]\big)^n \xrightarrow{\varphi} K_A^{[n]}$$

mit

$$\psi\colon \begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix} \mapsto \underbrace{(t \cdot E_n - A)}_{\in \mathrm{Mat}_n(K[t])} \cdot \begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix} \quad \text{und} \quad \varphi\colon \begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix} \mapsto \sum_{i=1}^{n} p_i \bullet e_i.$$

Insbesondere gilt dann: Sind $p_1, \ldots, p_k$ die Nicht-Einheiten unter den Elementarteilern von $t \cdot E_n - A$, so existiert ein $K[t]$-Modulisomorphismus

$$K_A^{[n]} \cong \prod_{i=1}^{k} K[t]/(p_i)_{K[t]}.$$ □

DEFINITION 5.3.12. *Sei K ein Körper und $A \in \mathrm{Mat}_n(K)$. Die eindeutig bestimmten Nicht-Einheiten $p_1, \ldots, p_k \in K[t]$ der Elementarteiler von $t \cdot E_n - A \in \mathrm{Mat}_n\big(K[t]\big)$ heißen die Polynominvarianten von A.* □

BEMERKUNG 5.3.13. *Ist $A \in \mathrm{Mat}_n(K)$, so hat $t \cdot E_n - A$ die Smith-Normalform der quadratischen die Form:*

$$t \cdot E_n - A \overset{SNF}{\rightsquigarrow} \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & p_1 & \\ & & & & \ddots \\ & & & & & p_k \end{pmatrix}$$

mit $p_i \in K[t]$ normiert und $p_i \mid p_{i+1}$ für $1 \leq i < k$,

denn würden auf der Diagonalen Nullen auftreten, hätte der $K[t]$-Modul $K_A^{[n]}$ einen freien Untermodul (Satz 5.3.11 und Lemma 5.2.32) - er ist nach Lemma 5.3.4 aber ein Torsionsmodul.
Mit der Anzahl der Nicht-Einheiten unter den Elementarteilern von $t \cdot E_n - A$ ist dann auch die Anzahl der Einsen auf der Diagonalen eindeutig bestimmt.
Die Polynominvarianten von A sind dann:

$$p_1, p_2, \ldots, p_k.$$

□

LEMMA 5.3.14. *Sei K ein Körper, und seien $A, B \in \mathrm{Mat}_n(K)$. Dann gelten folgende Äquivalenzen:*

$$\begin{aligned} & A \text{ und } B \text{ sind konjugiert} \\ \iff\ & A \text{ und } B \text{ haben die gleichen Polynominvarianten} \\ \iff\ & t \cdot E_n - A \text{ und } t \cdot E_n - B \text{ haben die gleichen Elemetarteiler.} \end{aligned}$$

□

DEFINITION 5.3.15. *Sei R ein kommutativer Ring mit Eins und $p \in R[t]$ normiert mit:*

$$p := t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0.$$

Dann ist die Begleitmatrix von p die folgende Matrix:

$$A_p := \begin{pmatrix} 0 & & & -a_0 \\ 1 & 0 & & -a_1 \\ & \ddots & \ddots & \vdots \\ & & 1 & 0 & -a_{n-2} \\ & & & 1 & -a_{n-1} \end{pmatrix} \in \mathrm{Mat}_n(R).$$

□

LEMMA 5.3.16. *Sei K ein Körper und $p \in K[t]$ ein normiertes Polyom n-ten Grades. Dann hat die Begleitmatrix A_p von p nur die Polynominvarante p, d.h. es gilt:*

$$t \cdot E_n - A_p \overset{SNF}{\rightsquigarrow} \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & p \end{pmatrix} \in \mathrm{Mat}_n\left(K[t]\right).$$

Insbesondere gilt dann nach Lemma 5.3.14: Hat eine Matrix $B \in \mathrm{Mat}_n(K)$ nur die Polynominvariante p, so ist sie zu der Begleitmatrix A_p konjugiert. □

DEFINITION 5.3.17. *Sei K ein Körper. Eine Matrix $A \in \mathrm{Mat}_n(K)$ hat rationale Normalform, falls sie eine Blockdiagonalmatrix ist mit Diagonalblöcken:*

$$A_{p_1}, \ldots, A_{p_k},$$

wobei A_{p_i} die Begleitmatrix zu einem normierten Polynom $p_i \in K[t]$ ist, und für die Polynome $p_1, \ldots, p_k$ gilt:

$$p_i \mid p_{i+1} \quad \text{für} \quad 1 \leq i < k.$$

Damit hat A also dann die Gestalt:

$$A = \begin{pmatrix} A_{p_1} & & \\ & \ddots & \\ & & A_{p_k} \end{pmatrix} \quad \textit{mit} \quad A_{p_i} = \begin{pmatrix} 0 & & & -a_0 \\ 1 & \ddots & & \vdots \\ & \ddots & 0 & -a_{n-2} \\ & & 1 & -a_{n-1} \end{pmatrix} \quad \textit{für} \quad p_i = t^n + \sum_{i=0}^{n-1} a_i t^i.$$

Es wird für die rationale Normalform bzgl. der normierten Polynome $p_1, \ldots, p_k$ mit $p_i \mid p_{i+1}$ auch abkürzend geschrieben: $A(p_1, \ldots, p_k)$. □

Satz 5.3.18. *(Klassifikation der Konjugationsklassen quadratischer Matrizen) Sei K ein Körper und $A \in \mathrm{Mat}_n(K)$. Dann gibt es genau eine rationale Normalform $A(p_1, \ldots, p_k)$ (Definition 5.3.17), zu der A konjugiert ist, und die Polynome $p_1, \ldots, p_k$ entsprechen den Polynominvarianten von A. Weiter existiert ein $K[t]$-Modulisomorphismus:*

$$K_A^{[n]} \cong \prod_{i=1}^{k} K[t]/(p_i)_{K[t]}.$$

Sind $A, B \in \mathrm{Mat}_n(K)$, so gelten folgende Äquivalenzen:

$$\begin{aligned} & A \text{ und } B \text{ sind konjugiert} \\ \iff\ & A \text{ und } B \text{ haben die gleichen Polynominvarianten} \\ \iff\ & A \text{ und } B \text{ haben die gleiche rationale Normalform} \\ \iff\ & t \cdot E_n - A \text{ und } t \cdot E_n - B \text{ haben die gleichen Elementarteiler} \\ \iff\ & t \cdot E_n - A \text{ und } t \cdot E_n - B \text{ haben die gleiche Smith-Normalform.} \end{aligned}$$

Wird für $A \in \mathrm{Mat}_n(K)$ mit $[A]$ seine Konjugationsklasse bezeichnet, so induziert die Zuordnung:

$$A \overset{Pol.Inv.}{\longrightarrow} (p_1, \ldots, p_k)$$

eine Bijektion der folgenden Mengen:

$$\begin{array}{c} \{\, [A] \mid A \in \mathrm{Mat}_n(K) \,\} \\ \downarrow \\ \{\, (p_1, \ldots, p_k) \mid p_i \in K[t] \text{ normiert}, \ p_i \mid p_{i+1}, \ \sum_{i=1}^{k} \mathrm{grad}(p_i) = n \,\}. \end{array}$$ □

Satz 5.3.19. *Sei K ein Körper und $A \in \mathrm{Mat}_n(K)$ mit den Polynominvarianten $p_1, \ldots, p_k$. Dann gelten folgende Aussagen:*

i.) p_k ist das Minimalpolynom μ_A von A.

ii.) Das Produkt der Polynominvarianten $p_1, \ldots, p_k$ ist das charakteristische Polynom χ_A von A:

$$p_1 \cdot \ldots \cdot p_k = \chi_A.$$

iii.) $\mu_A \mid \chi_A$.

iv.) Für ein Primpolynom $p \in K[t]$ gilt:

$$p \mid \mu_A \quad \Longleftrightarrow \quad p \mid \chi_A,$$

d.h. das Minimalpolyonom und das charakteristische Polynom von A enthalten die gleichen Primfaktoren (jedoch i.a. in unterschiedlicher Vielfachheit).

v.) Es gilt folgende Äquivalenz:

$$\mu_A \text{ zerfällt in Linearfaktoren} \quad \Longleftrightarrow \quad \chi_A \text{ zerfällt in Linearfaktoren.}$$

vi.) Die Eigenwerte von A entsprechen den Nullstellen des Minimalpolynoms μ_A. □

BEMERKUNG 5.3.20. *Die in Satz 5.3.19 enthaltene Aussage, daß μ_A ein Teiler von χ_A ist, findet sich in der Literatur als Satz von Cayley-Hamilton. Daraus folgt sofort, daß $\chi_A(A)$ die Nullmatrix ist, da $\mu_A(A)$ dies ja per Definition von μ_A erfüllt. Die Folgerung $\chi_A(A) = \bar{0}$ ist eine allgemeinere Tatsache, denn sie gilt auch für Matrizen über einem kommutativen Ring mit Eins, wo evt. gar kein Minimalpolynom von A existiert. Auch die allgemeinere Fassung „$\chi_A(A) = 0$“ findet sich in der Literatur als Satz von Cayley-Hamilton.* □

Literaturverzeichnis

[BlAn1] Christian Blatter, *Analysis 1*, Springer Verlag, 1991, vierte Auflage.

[BrLAI] Egbert Brieskorn, *Lineare Algebra und analytische Geometrie I*, Vieweg, 1983.

[BrLAII] Egbert Brieskorn, *Lineare Algebra und analytische Geometrie II*, Vieweg, 1985.

[FAn1] Otto Forster, *Analysis 1*, Vieweg, 1976.

[GMZ] H.-D. Ebbinghaus et al., *Zahlen*, Grundwissen Mathematik 1, Springer-Verlag, 1983.

[LaMR] T. Y. Lam, *Lectures on Modules and Rings*, Springer, 1999.

[MAC] Georg Cantor, *Beiträge zu Begründung der transfiniten Mengenlehre*, Mathematische Annalen, Volume 46 Nummer 4, 1895, Seite 481–512.

[PanDM] Alois Panholzer, *Diskrete Methoden*, Vorlesungsskript Sommersemester 2011, TU Wien.

[RALA] Steven Roman, *Advanced Linear Algebra*, Springer Verlag, Graduate Texts in Mathematics 135, 1992.

[RSV] H.-J. Reiffen, G. Scheja, U. Vetter, *Algebra*, B.I. Wissenschaftsverlag, 1984, 2te Auflage.

[SSAlg1] G. Scheja, U. Storch, *Lehrbuch der Algebra Teil 1*, B. G. Teubner Stuttgart, 1980.

[SSAlg2] G. Scheja, U. Storch, *Lehrbuch der Algebra Teil 2*, B. G. Teubner Stuttgart, 1988.

[SSAlg3] G. Scheja, U. Storch, *Lehrbuch der Algebra Teil 2*, B. G. Teubner Stuttgart, 1981.

[WAn1] Rolf Walter, *Einführung in die Analysis 1*, de Gruyter, 2007.