

# Lineare Algebra II Skript

Prof. Vogel

21. Mai 2020

## Inhaltsverzeichnis

<b>I</b>	<b>Unitäre Räume</b>	<b>2</b>
0	Unitäre Räume und der Spektralsatz	2
<b>II</b>	<b>Ringe</b>	<b>9</b>
1	Ringe und Ideale	9
2	Teilbarkeit	19
3	Euklidische Ringe	22
<b>III</b>	<b>Normalformen und Endomorphismen</b>	<b>31</b>
4	Invarianten-und Determinantenteiler	32

## Teil I

## Unitäre Räume

Ziel: Entwicklung einer analogen Theorie zur reellen Theorie der euklidischen VR für  $\mathbb{C}$ -VR

## 0 Unitäre Räume und der Spektralsatz

Notation: In diesem Abschnitt sei  $V$  stets ein endlicher  $\mathbb{C}$ -VR.

**Definition 0.1.**  $h : V \times V \rightarrow \mathbb{C}$  heißt eine **Sesquilinearform** auf  $V$

$\stackrel{\text{Def}}{:=} \Leftrightarrow$

(S1)  $h$  ist linear im ersten Argument, d.h.

- $h(v_1 + v_2, w) = h(v_1, w) + h(v_2, w),$
- $h(\lambda v, w) = \lambda h(v, w),$

$$\forall v_1, v_2, w \in V, \lambda \in \mathbb{C}.$$

(S2)  $h$  ist semilinear im zweiten Argument, d.h.

- $h(v, w_1 + w_2) = h(v, w_1) + h(v, w_2)$
- $h(v, \lambda w) = \bar{\lambda} h(v, w)$

$$\forall v, w_1, w_2 \in V, \lambda \in \mathbb{C}.$$

**Anmerkung.** sesqui = 1,5. In der Literatur sind (S1) und (S2) gelegentlich vertauscht.

**Beispiel 0.2.**  $\mathbb{C}, h(x, y) = x^t \bar{y}$  ist eine Sesquilinearform auf  $\mathbb{C}^n$  :

$$\begin{aligned} (x_1 + x_2)^t y &= x_1^t y + x_2^t y, \\ (\lambda x)^t y &= \lambda (x^t y), \\ x^t (\bar{y}_1 + \bar{y}_2) &= x^t \bar{y}_1 + x^t \bar{y}_2, \\ x^t \bar{\lambda y} &= \bar{\lambda} x^t y. \end{aligned}$$

für  $x_1, x_2, y, y_1, y_2 \in \mathbb{C}^n$ .

$h$  ist für  $n > 0$  keine Bilinearform:

$$h\left(\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, i \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}\right) = (1, \dots, 0) \begin{pmatrix} -i \\ 0 \\ \vdots \\ 0 \end{pmatrix} = -i \neq ih\left(\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}\right) = i.$$

**Definition 0.3.** Sei  $V$  ein  $\mathbb{C}$ -VR,  $h$  Sesquilinearform auf  $V$ .  $h$  heißt **hermitisch**  $\stackrel{\text{Def}}{\Leftrightarrow} h(w, v) = \overline{h(v, w)}$  für alle  $v, w \in V$ .

**Anmerkung.** In diesem Fall ist  $h(v, v) = \overline{h(v, v)}$  für alle  $V \in V$ , d.h.  $h(v, v) \in \mathbb{R}$  für alle  $v \in V$ .

**Beispiel 0.4.**  $h(x, y) = x^t \bar{y}$  aus Bsp. 0.2 ist hermitesch, denn es ist  $h(y, x) = \underbrace{y^t \bar{x}}_{\in \mathbb{C}} = (y^t \bar{x})^t = \overline{x^t (y^t)^t} = \overline{x^t y} = x^t \bar{y} = h(x, y).$

Hier ist  $h(x, x) = x^t \bar{x} = (x_1, \dots, x_n) \begin{pmatrix} \bar{x}_1 \\ \vdots \\ \bar{x}_n \end{pmatrix} = x_1 \bar{x}_1 + \dots + x_n \bar{x}_n = |x_1|^2 + \dots + |x_n|^2 \in \mathbb{R}.$

**Definition 0.5.** Sei  $h : V \times V \longrightarrow \mathbb{C}$  eine Sesquilinearform,  $B = (v_1, \dots, v_n)$  Basis von  $V$ .

$$M_B = (h(v_i, v_j))_{1 \leq i, j \leq n} \in M_{n,n}(\mathbb{C})$$

heißt die **Fundamentalmatrix** von  $h$  bzgl.  $B$ . (Darstellungsmatrix)

**Beispiel 0.6.** Für  $h(x, y) = x^t \bar{y}$  aus Bsp. 0.2, ist

$$M_B(h) = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} = E_n$$

**Definition 0.7.** Sei  $M \in M_{n,n}(\mathbb{C})$ .  $M^* := \overline{M}^t$  heißt die zu  $M$  **adjungierte Matrix**.  $M$  heißt **hermitesch**  $\stackrel{\text{Def.}}{\Leftrightarrow} M = M^*$

**Anmerkung.** Nicht verwechseln mit der adjunkten Matrix!

**Satz 0.8.** Sei  $B = (v_1, \dots, v_n)$  eine Basis von  $V$ .

$\text{Sesq}(V) := \{h : V \times V \longrightarrow \mathbb{C} \mid h \text{ ist Sesquilinearform}\}$  ist ein  $\mathbb{C}$ -VR. (UVR von  $\mathbb{C}$ -VR  $\text{Abb}(V \times V, \mathbb{C})$ ). Die Abbildung

$$M_B = \text{Sesq}(V) \longrightarrow M_{n,n}(\mathbb{C}), h \mapsto M_B(h)$$

ist ein Isomorphismus von  $\mathbb{C}$ -VR mit Umkehrabbildung

$$h_B : M_{n,n}(\mathbb{C}) \longrightarrow \text{Sesq}(V), A \mapsto h_B(A) \text{ mit } h_B(A) : V \times V \longrightarrow \mathbb{C},$$

$$\left( \sum_{i=1}^n x_i v_i, \sum_{j=1}^n y_j v_j \right) \mapsto x^t A \bar{y} \text{ mit } x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

Es gilt:  $h$  hermitesch  $\Leftrightarrow M_B(h)$  hermitesch.

*Beweis.*

- $h_B$  ist wohldefiniert:  $h_B(A)$  ist Sesquilinearform analog zur Rechnung in Bsp. 0.2.
- $M_B, h_B$  sind  $\mathbb{C}$ -linear: klar.
- $M_B \circ h_B = id$ , denn: Sei  $A = (a_{ij}) \in M_{n,n}(\mathbb{C}) \Rightarrow h_B(A)(v_i, v_j) = e_i^t A \bar{e}_j = a_{ij}$ , d.h. Darstellungsmatrix von  $h_B(A)$  bzgl.  $B$  ist  $A$ .
- $h_B \circ M_B = id$ , denn: Sei  $h \in \text{Sesq}(V) \Rightarrow h_B(M_B(h))(v_i, v_j) = e_i^t M_B(h) \bar{e}_j = h(v_i, v_j) \Rightarrow h_B(M_B(h)) = h$ . Für  $h \in \text{Sesq}(V)$  ist

$$\begin{aligned} h \text{ hermitesch} &\Leftrightarrow h(w, v) = \overline{h(v, w)} \text{ für alle } v, w \in V \\ &\Leftrightarrow h(v_j, v_i) = \overline{h(v_i, v_j)} \text{ für alle } i = 1, \dots, n \\ &\Leftrightarrow M_B(h)^t = \overline{M_B(h)} \\ &\Leftrightarrow M_B(h) = \overline{M_B(h)}^t = M_B(h)^* \end{aligned}$$

□

**Satz 0.9.**  $A, B$  Basen von  $V$ ,  $h$  Sesquilinearform auf  $V$ . Dann gilt

$$M_B(h) = (T_A^B)^t M_A(h) \overline{T_A^B}, \text{ wobei } T_A^B = M_A^B(id_V).$$

*Beweis.* analog zum reellen Fall

□

**Definition 0.10.** Sei  $h$  hermitesche Form.  $h$  heißt positiv definit  $\stackrel{\text{Def:}}{\Leftrightarrow} h(v, v) > 0, \forall v \in V, v > 0$ . Eine positiv definite hermitesche Sesquilinearform nennt man auch ein komplexes **Skalarprodukt**.

**Beispiel 0.11.**  $V = \mathbb{C}^n, \langle \cdot, \cdot \rangle : \mathbb{C}^n \times \mathbb{C}^n, \langle x, y \rangle := x^t \bar{y}$  ist ein Skalarprodukt (Standartskalarprodukt auf  $\mathbb{C}^n$ ) denn:

$$\langle x, x \rangle = |x_1|^2 + \dots + |x_n|^2 > 0, \forall x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{C}^n, x \neq 0.$$

**Definition 0.12.** Ein unitärer Raum ist ein Paar  $(V, h)$  bestehend aus einem endlichdimensionalen  $\mathbb{C}$ -VR  $V$  und einem Skalarprodukt  $h$  auf  $V$ .

**Definition 0.13.** Sei  $(V, h)$  unitärer Raum,  $v \in V$ .

$$\|v\| := \sqrt{\langle v, v \rangle} \text{ heißt die Norm von } V.$$

**Satz 0.14.** Sei  $(V, h)$  ein unitärer Raum. Dann gilt:

1.  $\|x + y\| \leq \|x\| + \|y\|, \forall x, y \in V$  (Dreiecksungleichung)
2.  $|h(x, y)| \leq \|x\| \cdot \|y\|, \forall x, y \in V$  (Cauchy-Schwarz-Ungleichung)

*Beweis.*

2. Seien  $x, y \in V$ . Falls  $x = 0$ , dann

$$h(x, y) = h(0, y) = h(0 \cdot 0, y) = 0 \cdot h(0, y) = 0 = \|0\| \cdot \|y\|.$$

Im Folgenden sei  $x \neq 0$ . Setze

$$\begin{aligned} \alpha &:= \frac{h(x, y)}{\|x\|^2}, w := y - \alpha x \Rightarrow h(w, x) = h(y - \alpha x, x) = h(y - \frac{h(y, x)}{\|x\|^2} x, x) \\ &= h(y, x) - \frac{h(y, x)}{\|x\|^2} \underbrace{h(x, x)}_{\|x\|^2} = 0 \\ &\Rightarrow \|y\|^2 = \|w + \alpha x\|^2 = h(w + \alpha x, w + \alpha x) = \|w\|^2 + \alpha \cdot \bar{\alpha} h(x, x) \\ &= \|w\|^2 + |\alpha|^2 \|x\|^2 \\ &\Rightarrow \|y\| \geq |\alpha| \|x\| = \frac{|h(y, x)|}{\|x\|^2} \|x\| = \frac{|h(x, y)|}{\|x\|} \\ &\Rightarrow \|y\| \|x\| \geq |h(x, y)| \end{aligned}$$

1.

$$\begin{aligned} \|x + y\|^2 &= h(x + y, x + y) = \|x\|^2 + \|y\|^2 + h(x, y) + h(y, x) \\ &= \|x\|^2 + \|y\|^2 + 2 \operatorname{Re} h(x, y) \\ &\leq \|x\|^2 + \|y\|^2 + 2|h(x, y)| \\ &\leq \|x\|^2 + \|y\|^2 + 2\|x\|\|y\| \\ &= (\|x\| + \|y\|)^2 \end{aligned}$$

□

**Definition 0.15.** Sei  $(v_1, \dots, v_n)$  eine Basis von  $V$ .  $(v_1, \dots, v_n)$  heißt eine

**Orthogonalbasis** von  $V \stackrel{\text{Def.}}{\Leftrightarrow} h(v_i, v_j) = 0 \text{ für } i \neq j.$

**Orthonormalbasis** von  $V \stackrel{\text{Def.}}{\Leftrightarrow} h(v_i, v_j) = \delta_{ij} \text{ für alle } 1 \leq i, j \leq n.$

**Satz 0.16.** Sei  $(V, h)$  ein unitärer Raum. Dann hat  $V$  eine ONB.

*Beweis.* gzz.:  $(V, h)$  hat eine OB (normieren der Basisvektoren liefert dann ONB) Beweis per Induktion nach  $n = \dim(V)$ .

$n = 0, 1$  : trivial

- $n \geq 2$ : Wähle  $v_1 \in V, v_1 \neq 0$  Setze  $H := \{w \in V | h(w, v_1) = 0\}$ .

Die Abbildung  $\phi : V \rightarrow \mathbb{C}, w \mapsto h(w, v_1)$  ist Linearform mit  $\ker \phi = H$   
 $\Rightarrow \dim H = \dim \ker \phi = \dim V - \dim \text{im } \phi \in \{n, n-1\}$   
 $\in \{0, 1\}$

Wegen  $h(v_1, v_1) > 0$  ist  $v_1 \notin H$ ; somit  $\dim H = n-1$

$(H, h|_{H \times H})$  ein unitärer Raum der Dimension  $n-1$

$\Rightarrow H$  hat OB  $(v_2, \dots, v_n)$

$\Rightarrow (v_1, v_2, \dots, v_n)$  ist OB von  $V$

□

**Anmerkung.** Gram-Schmidt-Verfahren (wie über  $\mathbb{R}$ ) liefert Algorithmus zur Bestimmung einer ONB.

**Definition 0.17.** Sei  $(V, h)$  ein unitärer Raum,  $U \subset V$  ein Untervektorraum.  $U^\perp = \{v \in V | h(v, u) = 0 \text{ für alle } u \in U\}$  heißt das **orthogonale Komplement** zu  $U$ .  $U, W$  sind Untervektorräume von  $V$  mit  $V = U \oplus W$  und  $h(u, w) = 0$  für alle  $u \in U, w \in W$ . Dann heißt  $V$  die **orthogonale direkte Summe** von  $U$  und  $W$ . Notation:  $V = U \hat{\oplus} W$ .

**Satz 0.18.** Sei  $(V, h)$  ein unitärer Raum,  $U \subset V$  ein Untervektorraum. Dann gilt:

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

*Beweis.* 1.

Beh.:  $V = U + U^\perp$

Sei  $(u_1, \dots, u_m)$  ONB von  $U$ .

Sei  $v \in V$ . Setze  $v' := v - \sum_{j=1}^m h(v, u_j) u_j$

Für  $i = 1, \dots, m$  ist  $h(v', u_i) = h(v, u_i) - \sum_{j=1}^m h(v, u_j) \underbrace{h(u_j, u_i)}_{=\delta_{ij}} = h(v, u_i) - h(v, u_i) = 0$

$\Rightarrow v' \in U^\perp$

$v = \underbrace{v'}_{\in U^\perp} + \underbrace{\sum_{j=1}^m h(v, u_j) u_j}_{\in U} \in U + U^\perp$

2.  $U \cap U^\perp = 0$ , denn:  $u \in U \cap U^\perp \Rightarrow h(u, u) = 0 \Rightarrow u = 0$ .

3. Wegen 1. und 2. ist  $V = U \hat{\oplus} U^\perp$ , außerdem ist  $h(u, u') = 0$  für  $u \in U, u' \in U^\perp$ , somit  $V = U \hat{\oplus} U^\perp$ .

□

**Definition 0.19.** Seien  $(V, h_v), (W, h_w)$  unitäre Räume,  $\varphi : V \rightarrow W$  eine lineare Abbildung.  $\varphi$  heißt **unitär**  $\Leftrightarrow h_w(\varphi(v_1), \varphi(v_2)) = h_v(v_1, v_2)$  für alle  $v_1, v_2 \in V$ .

**Anmerkung:** Ist  $\varphi \in \text{End}(V)$  ein unitärer Endomorphismus, dann ist  $\varphi$  ein Isomorphismus, denn:

- $\varphi$  ist injektiv, wegen  $\varphi(v) = 0 \Rightarrow 0 = h(\varphi(v), \varphi(v)) = h(v, v) \Rightarrow v = 0$
- wegen  $\dim V < \infty$  folgt  $\varphi$  surjektiv.

**Bemerkung 0.20.** Sei  $(V, h)$  unitärer Raum,  $B = (v_1, \dots, v_n)$  ONB von  $(V, h)$ . Dann ist die Abbildung

$$(\mathbb{C}^n, \langle \cdot, \cdot \rangle) \rightarrow (V, h), e_i \mapsto v_i$$

ein unitärer Isomorphismus, d.h.  $(V, h)$  ist unitär isomorph zu  $(\mathbb{C}^n, \langle \cdot, \cdot \rangle)$ .

*Beweis.*  $h(\varphi(e_i), \varphi(e_j)) = h(v_i, v_j) = \delta_{ij} = \langle e_i, e_j \rangle$

□

**Definition 0.21.** Sei  $A \in M_{n,n}(\mathbb{C})$ .

- $A$  heißt **unitär**  $\stackrel{\text{Def}}{\Leftrightarrow} A^* A = E_n$
- $U(n) := \{A \in M_{n,n}(\mathbb{C}) \mid A \text{ ist unitär} \}$
- $U(n)$  ist eine Gruppe bzgl. " $\cdot$ ", die **unitäre Gruppe** vom Rang  $n$ .
- $SU(n) := \{A \in U(n) \mid \det(A) = 1\}$  ist eine Untergruppe von  $U(n)$ , die **spezielle unitäre Gruppe**.

**Bemerkung 0.22.** Sei  $A \in M_{n,n}(\mathbb{C})$ . Dann sind äquivalent:

- $A$  ist unitär
- Die Abbildung  $(\mathbb{C}^n, \langle \cdot, \cdot \rangle) \rightarrow (\mathbb{C}^n, \langle \cdot, \cdot \rangle), x \mapsto Ax$  ist unitär. Hierbei ist  $\langle \cdot, \cdot \rangle$  das Standard-skalarprodukt.

*Beweis.*  $\langle Ax, Ay \rangle = (Ax)^t \overline{Ay} = x^t A^t \overline{A} \overline{y}$

Somit ist die Abbildung aus (ii) unitär

$$\Leftrightarrow x^t A^t \overline{A} \overline{y} = \langle x, y \rangle = x^t \overline{y} \text{ für alle } x, y \in \mathbb{C}^n$$

$$\Leftrightarrow h_{(e_1, \dots, e_n)}(A^t, \overline{A}) = h_{(e_1, \dots, e_n)}(E_n) \text{ (vgl. Satz 0.7)}$$

$$\stackrel{0.7}{=} A^t A = E_n \Leftrightarrow \overline{A}^t (A^t)^t = E_n \Leftrightarrow \overline{A}^t A = A^* A = E_n \Leftrightarrow A \text{ ist unitär}$$

□

**Bemerkung 0.23.** Sei  $(V, h)$  ein unitärer Raum und  $f \in \text{End}(V)$ . Dann existiert genau ein  $f^* \in \text{End}(V)$  mit

$$h(f(x), y) = h(x, f^*(y)), \forall x, y \in V$$

$f^*$  heißt die **zu  $f$  adjungierte Abbildung**. Ist  $B$  eine ONB von  $(V, h)$ , dann ist

$$M_B(f^*) = M_B(f)^*$$

*Beweis.* analog zu LA1, 19/20; Def. + Lemma 5.48

□

**Definition 0.24.** Sei  $(V, h)$  ein unitärer Raum,  $f \in \text{End}(V)$ ,  $A \in M_{n,n}(\mathbb{C})$ .

- $f$  heißt **selbstadjungiert**  $\stackrel{\text{Def.}}{\Leftrightarrow} f^* = f$
- $f$  heißt **normal**  $\stackrel{\text{Def.}}{\Leftrightarrow} f^* \circ f = f \circ f^*$
- $A$  heißt **selbstadjungiert**  $\stackrel{\text{Def.}}{\Leftrightarrow} A^* = A$
- $A$  heißt **normal**  $\stackrel{\text{Def.}}{\Leftrightarrow} A^* A = A A^*$

**Anmerkung.**  $A$  ist selbstadjungiert  $\Leftrightarrow A$  ist hermitisch.

**Bemerkung 0.25.** Sei  $(V, h)$  ein unitärer Raum,  $f \in \text{End}(V)$ . Dann gilt:

- (a)  $f$  unitär  $\Rightarrow f$  normal
- (b)  $f$  selbstadjungiert  $\Rightarrow f$  normal

Für  $A \in M_{n,n}(\mathbb{C})$  gilt:  $A$  unitär  $\Rightarrow A$  normal,  $A$  selbstadjungiert  $\Rightarrow A$  normal

*Beweis.* (a) Seien  $v, w \in V$

$$\begin{aligned} &\Rightarrow h(v, f^{-1}(w)) = h(f(v), f(f^{-1}(w))) = h(f(v), w) \\ &\text{\small } f \text{ Isomorphismus, da unitär} \quad \text{\small } f \text{ unitär} \\ &\stackrel{0.23}{\Rightarrow} f^* = f^{-1} \Rightarrow f^* \circ f = f^{-1} \circ f = \text{id}_V = f \circ f^{-1} = f \circ f^* \end{aligned}$$

- (b)  $f$  selbstadjungiert  $\Rightarrow f^* = f \Rightarrow f^* \circ f = f \circ f = f \circ f^*$

□

**Ziel.**  $f$  normal  $\Rightarrow (V, h)$  besitzt eine ONB aus Eigenvektoren von  $f$  (Spektralsatz)

**Bemerkung 0.26.** Sei  $(V, h)$  ein unitärer Raum,  $f \in \text{End}(V)$ . Dann gilt:

- (a)  $U \subset V$  UVR mit  $f(U) \subset U \Rightarrow f^*(U^\perp) \subset U^\perp$
- (b)  $f$  normal. Dann:  $v \in V$  Eigenvektoren von  $f$  zum Eigenwert  $\lambda \in \mathbb{C} \Leftrightarrow v$  ist Eigenvektor von  $f^*$  zum Eigenwert  $\bar{\lambda}$
- (c)  $f$  selbstadjungiert  $\Rightarrow$  Alle Eigenwerte von  $f$  sind reell.  $h(f^*(v), u) = \overline{h(u, f^*(v))} = \overline{h(\underbrace{f(u), v}_{\in U})} = 0 \Rightarrow f^*(v) \in U^\perp$
- (d) Sei  $f$  normal. Setze  $g := \lambda \text{id}_V - f$

*Beweis.* 1. Sei  $v \in V^\perp, u \in U$  es ist

- (a) Beh.:  $g^* = \bar{\lambda} \text{id}_V - f^*$

$$\begin{aligned} \text{denn: } h((\lambda \text{id}_V - f)(x), y) &= \lambda h(x, y) - h(f(x), y) = h(x, \bar{\lambda} y) - h(x, f^*(y)) \\ h(x, \bar{\lambda} y - f^*(y)) &= h(x, (\bar{\lambda} \text{id}_V - f^*(y))) \text{ für alle } x, y \in V \end{aligned}$$

- (b) Beh.:  $g^* \circ g = g \circ g^*$ , d.h.  $g$  ist normal denn:  $g \circ g^* = (\lambda \text{id}_V - f) \circ (\bar{\lambda} \text{id}_V - f^*) = f^* \circ f \stackrel{f \text{ normal}}{=} (\bar{\lambda} \text{id}_V - f^*) \circ (\lambda \text{id}_V - f) = g^* \circ g$

- (c) Sei  $v \in V, v \neq 0$

Dann:  $v$  Eigenvektor zum Eigenwert  $\lambda$  von  $f$   
 $v$  Eigenvektoren zum Eigenwert  $\bar{\lambda}$



- (d) Sei  $f$  selbstadjungiert,  $\lambda \in \mathbb{C}$  ein Eigenwert von  $f$ ,  $v$  Eigenvektor zum Eigenwert  $\lambda \Rightarrow f$  normal, nach (b) ist  $v$  Eigenvektor zum Eigenwert  $\bar{\lambda}$  von  $f^* = f \Rightarrow \lambda = \bar{\lambda} \Rightarrow \lambda \in \mathbb{R}$

□

**Satz 0.27** (Spektralsatz für normale Operatoren). Sei  $(V, h)$  ein unitärer Raum,  $f \in \text{End}(V)$  normal. Dann existiert eine ONB von  $(V, h)$  aus Eigenvektoren von  $f$ .

*Beweis.* Beweis per Induktion nach  $n = \dim V$ .

- $n = 0, 1$ : trivial
- $n > 1$ : charakteristisches Polynom  $\chi_f \in \mathbb{C}[t]$  hat nach dem Fundamentalsatz der Algebra eine Nullstelle in  $\mathbb{C}$ .  
 $\Rightarrow f$  hat einen Eigenwert, etwa  $\lambda$ . Sei  $v \in V$  ein Eigenvektor zu  $\lambda$  mit  $\|v\| = 1$ . Setze  $L := \mathbb{C}v$ . Es ist  $f^*(v) = \bar{\lambda}v$ , also  $f^*(L) \subset L \xrightarrow{0.26(a)} (f^*)^* L^\perp \subset L^\perp \Rightarrow f$  induziert einen normalen Endomorphismus des unitären Raums  $(L^\perp, h|_{L^\perp \times L^\perp})$ . Nach Induktionsvoraussetzung existiert eine ONB  $(v_2, \dots, v_n)$  von  $L^\perp$  aus Eigenvektoren zu  $f|_{L^\perp} \Rightarrow (v, v_2, \dots, v_n)$  ist ONB von  $V = L \hat{\oplus} L^\perp$  aus Eigenvektoren von  $f$ .

□

**Anmerkung.** • Es gilt sogar die Umkehrung: Wenn ONB von  $(V, h)$  aus Eigenvektoren von  $f$  existiert, dann ist  $f$  normal.

- Für jeden selbstadjungierten/unitären Endomorphismus eines unitären Vektorraums existiert eine ONB von  $(V, h)$  aus Eigenvektoren.

**Lemma 0.28.** Sei  $A \in M_{n,n}(\mathbb{C})$  normal. Dann existiert eine unitäre Matrix  $U \in U(n)$ , so dass  $U^*AU$  eine Diagonalmatrix ist.

*Beweis.* Wende Spektralsatz 0.27 auf  $(\mathbb{C}^n, \langle \cdot, \cdot \rangle) \rightarrow (\mathbb{C}^n, \langle \cdot, \cdot \rangle), x \mapsto Ax$  an. (Basiswechselmatrix unitär, da ONB von Eigenvektoren). Erhalte  $U \in U(n, \mathbb{C})$  mit  $U^{-1}AU$  Diagonalmatrix,  $U^{-1} = U^*$  wegen  $U$  unitär. □

**Anmerkung.** Jede reelle orthogonale Matrix ist über  $\mathbb{C}$  diagonalisierbar (aber: Es gibt orthogonale Matrizen, die über  $\mathbb{R}$  nicht diagonalisierbar sind, z.B.  $\det \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$  (Drehung um  $\frac{\pi}{2}$ ))

## Teil II

# Ringe

## 1 Ringe und Ideale

Erinnerung an LA 1 Definition:

**Definition 1.1.** Ein **Ring** ist ein Tupel  $(R, +, \cdot, 0_R)$  bestehend aus einer Menge  $R$  mit zwei Verknüpfungen

$$+, \cdot : R \times R \rightarrow R$$

und einem ausgezeichnetem Element  $0_R$ , so dass gilt:

(R1)  $(R, +, 0_R)$  ist eine abelsche Gruppe

(R2) Assoziativität der Multiplikation:  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$  für alle  $a, b, c \in R$

(R3) Distributivität:  $a(b + c) = ab + ac$ ,  $(a + b) \cdot c = ac + bc$  für alle  $a, b, c \in R$

Ein **Ring mit Eins (Unitärer Ring)** ist ein Ring, in dem ein Element  $1_R$  existiert, für das gilt

(R4)  $1_R \cdot a = a = a \cdot 1_R$  für alle  $a \in R$

Ein Ring heißt **kommutativ**, wenn die Multiplikation kommutativ ist, d.h. heißt wenn gilt:

(R5)  $a \cdot b = b \cdot a$  für alle  $a, b \in R$

**Konvention:** In der LA2 interessieren wir uns für kommutative Ringe mit eins. Deswegen verwenden wir ab jetzt folgende Sprechweise: **Ring:=Kommutativer Ring mit Eins**

**Beispiel 1.2.** Beispiele für Ringe:

- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
- $\mathbb{Z}/n\mathbb{Z}$
- Nullring:  $\{0\}$ . Hierbei  $0_R = 0 = 1_R$ . Häufig schreibt man kurz 0 für den Nullring.

In diesem Abschnitt seien  $R$  und  $S$  stets Ringe.

**Definition 1.3.** Sei  $J \subseteq R$ .  $J$  heißt **Ideal** in  $R$   $\stackrel{\text{Def.}}{\Leftrightarrow}$  Die folgenden Bedingungen sind erfüllt:

(J1)  $0 \in J$

(J2)  $a, b \in J \implies a + b \in J$

(J3)  $r \in R, a \in J \implies ra \in J$

**Beispiel 1.4.** (a)  $\{0\}, R$  sind Ideale in  $R$ .

(b) Für  $n \in \mathbb{Z}$  ist  $n\mathbb{Z} := \{na \mid a \in \mathbb{Z}\}$  ist ein Ideal in  $\mathbb{Z}$

**Ziel.** Jedes Ideal in  $\mathbb{Z}$  ist von der Form  $n\mathbb{Z}$ .

**Bemerkung 1.5** (Division mit Rest). Seien  $a, b \in \mathbb{Z}, b \neq 0$ . Dann existieren  $q, r \in \mathbb{Z}$  mit

$$a = qb + r \text{ und } 0 \leq r < |b|$$

$r$  heißt **Rest** der Division von  $a$  durch  $b$ .

*Beweis.* Setze  $R := \{a - \tilde{q}b \mid \tilde{q} \in \mathbb{Z}\} \cap \mathbb{N}_0 \implies R$  ist nichtleere Teilmenge von  $\mathbb{N}_0$ , insbesondere besitzt  $R$  kleinstes Element, etwa  $r$ . Sei  $q \in \mathbb{Z}$  mit  $a - qb = r \implies a = qb + r$  Annahme:  $r \geq |b| \implies 0 \leq r - |b| = a - qb - \text{sgn}(b)b = \underbrace{a - (q + \text{sgn}(b))b}_{\in R} < r$  Das ist ein Widerspruch zur

Minimalität von  $r$ .  $\square$

**Anmerkung.**  $q, r$  wie in Bemerkung 1.5 sind eindeutig bestimmt.

**Bemerkung 1.6.** Sei  $J \subseteq \mathbb{Z}$  ein Ideal. Dann existiert ein  $n \in \mathbb{Z}$  mit  $J = n\mathbb{Z}$

*Beweis.* • Falls  $J = \{0\} = 0\mathbb{Z}$ , dann fertig.

- Im Folgenden sei  $J \neq \{0\}$ . Dann existiert ein Element  $a \in J, a \neq 0$ . Mit  $a \in J$  ist auch  $(-1)a = -a \in J$ , somit  $J \cap \mathbb{N} \neq \emptyset \implies J \cap \mathbb{N}$  besitzt ein kleinstes Element, etwa  $n$ .  
Behauptung:  $J = n\mathbb{Z}$

(i) " $\supseteq$ ": Sei  $x \in n\mathbb{Z} \implies$  Es existiert ein  $q \in \mathbb{Z}$  mit  $x = \underbrace{nq}_{\in J} \xrightarrow{J \text{ Ideal}} x \in J$

(ii) " $\subseteq$ ": Sei  $x \in J \xrightarrow{\text{Division mit Rest}} \text{Es existieren } q, r \in \mathbb{Z} \text{ mit } x = qn + r, 0 \leq r < n \implies r = \underbrace{n}_{\in J} - \underbrace{qn}_{\in J} \in J$ . Wegen der Minimalität von  $n$  in  $J \cap \mathbb{N}$  folgt  $r = 0 \implies x = qn \in \mathbb{Z}$

$\square$

**Definition 1.7.** Sei  $\varphi : R \longrightarrow S$  eine Abbildung.  $\varphi$  heißt ein **Ringhomomorphismus**  $\xrightarrow{\text{Def:}}$   
Die folgenden Bedingungen sind erfüllt:

(RH1)  $\varphi(a + b) = \varphi(a) + \varphi(b)$  für alle  $a, b \in R$

(RH2)  $\varphi(ab) = \varphi(a)\varphi(b)$  für alle  $a, b \in R$

(RH3)  $\varphi(1_R) = 1_S$

**Bemerkung 1.8.** Sei  $\varphi : R \longrightarrow S$  ein Ringhomomorphismus. Dann gilt:

- (a)  $J \subseteq S \text{ Ideal} \implies (\varphi)^{-1}(J) \subseteq R \text{ Ideal}$
- (b)  $\ker \varphi := \{a \in R \mid \varphi(a) = 0\} \subseteq R \text{ Ideal}$
- (c)  $\varphi$  injektiv  $\Leftrightarrow \ker \varphi = \{0\}$
- (d)  $J \subseteq R \text{ Ideal}$  und  $\varphi$  surjektiv  $\implies \varphi(J) \subseteq S \text{ Ideal}$
- (e)  $\text{im } \varphi := \varphi(R)$  ist ein Unterring von  $S$

*Beweis.* (a) (J1)  $0 \in \varphi^{-1}(J)$ , denn:  $\varphi(0) = \varphi(0 + 0) = \varphi(0) + \varphi(0) \implies \varphi(0) = 0 \in J \implies 0 \in \varphi^{-1}(J)$

(J2)  $a, b \in \varphi^{-1}(J) \implies \varphi(a), \varphi(b) \in J \xrightarrow{J \text{ Ideal}} \underbrace{\varphi(a) + \varphi(b)}_{=\varphi(a+b)} \in J \implies a + b \in \varphi^{-1}(J)$

(J3)  $r \in R, a \in \varphi^{-1}(J) \implies \varphi(a) \in J \xrightarrow{J \text{ Ideal}} \underbrace{\varphi(r)\varphi(a)}_{=\varphi(ra)} \in J \implies ra \in \varphi^{-1}(J)$

(b) aus (a) wegen  $\ker \varphi = \varphi^{-1}(\{0\}), \{0\} \subseteq S \text{ Ideal}$ .

(c) nachrechnen

(d) nachrechnen

(e) nachrechnen

$\square$

**Anmerkung.** (d) wird falsch, wenn man die Voraussetzung  $\varphi$  surjektiv weglässt. Die kanonische Inklusion  $i: \mathbb{Z} \rightarrow \mathbb{Q}, x \mapsto x$  ist ein Ringhomomorphismus,  $\mathbb{Z}$  ein Ideal in  $\mathbb{Z}$ ,  $\mathbb{Z} = i(\mathbb{Z})$  ist kein Ideal in  $\mathbb{Q}$  (denn:  $\frac{1}{3} \cdot 2 = \frac{2}{3} \notin \mathbb{Z}$ ).  $\mathbb{Z}$  ist aber ein Unterring in  $\mathbb{Q}$ .

**Bemerkung 1.9.** Sei  $J \subseteq R$  ein Ideal. Dann ist durch  $r_1 \sim r_2 \stackrel{\text{Def.}}{\iff} r_1 - r_2 \in J$  eine Äquivalenzrelation auf  $R$ , welche die zusätzliche Eigenschaft

$$r_1 \sim r_2, s_1 \sim s_2 \implies r_1 + s_1 \sim r_2 + s_2, r_1 s_1 \sim r_2 s_2$$

(Kongruenzrelation) hat, definiert. Die Äquivalenzklasse von  $r \in R$  ist durch

$$\bar{r} := r + J := \{r + a \mid a \in J\}$$

gegeben und heißt die **Restklasse** von  $r$  modulo  $J$ . Die Menge der Restklassen bezeichnen wir mit  $R/J$ .

*Beweis.* (1.) " $\sim$ " ist eine Äquivalenzrelation:

- $\sim$  reflexiv:  $r \sim r$ , denn  $r - r = 0 \in J$
- $\sim$  symmetrisch: Seien  $r, s \in R$  mit  $r \sim s \implies r - s \in J \implies (-1)(r - s) \in J \implies s - r \in J \implies s \sim r$
- $\sim$  transitiv: Seien  $r, s, t \in R$  mit  $r \sim s, s \sim t \implies r - s \in J, s - t \in J \implies r - t \in J \implies r \sim t$

(2.) Verträglichkeit mit  $+, \cdot$ : Sei  $r_1 \sim r_2, s_1 \sim s_2 \implies r_1 - r_2 \in J, s_1 - s_2 \in J$

$$(r_1 + s_1) - (r_2 + s_2) = \underbrace{(r_1 - r_2)}_{\in J} + \underbrace{(s_1 - s_2)}_{\in J} \implies r_1 + s_1 \sim r_2 + s_2$$

Außerdem:

$$r_1 s_1 - r_2 s_2 = r_1 \underbrace{(s_1 - s_2)}_{\in J} + s_2 \underbrace{(r_1 - r_2)}_{\in J} \implies r_1 s_1 \sim r_2 s_2$$

□

**Bemerkung 1.10.** Sei  $J \subseteq R$  ein Ideal. Dann wird  $R/J$  mit der Addition

$$+ : R/J \times R/J \longrightarrow R/J, \bar{r} + \bar{s} := \overline{r + s}$$

und der Multiplikation

$$\cdot : R/J \times R/J \longrightarrow R/J, \bar{r} \cdot \bar{s} := \overline{r \cdot s}$$

zu einem Ring, dem **Faktorring (Restklassenring)**  $R/J$ . Die Abbildung  $\pi : R \rightarrow R/J, r \mapsto \bar{r}$  ist ein surjektiver Ringhomomorphismus mit  $\ker \pi = J$ .  $\pi$  heißt die **kanonische Projektion** von  $R$  nach  $R/J$ .

*Beweis.* • Wohldefiniertheit von  $+, \cdot$ : nach 1.9 ist für  $r_1, r_2, s_1, s_2 \in R$  mit  $r_1 \sim r_2, s_1 \sim s_2$  auch  $r_1 + s_1 \sim r_2 + s_2, r_1 s_1 \sim r_2 s_2$

- Ringeigenschaften vererben sich aufgrund der vertreterweisen Definition
- $\pi$  ist ein Ringhomomorphismus nach Konstruktion:  $\pi(a + b) = \overline{a + b} = \bar{a} + \bar{b} = \pi(a) + \pi(b)$ , analog für  $\cdot$ ,  $\pi(1) = \bar{1}$
- $\pi$  ist surjektiv nach Konstruktion
- $\ker \pi = \{r \in R \mid \bar{r} = \bar{0}\} = \{r \in R \mid r \sim 0\} = \{r \in R \mid r - 0 \in J\} = J$

□

**Anmerkung.** Insbesondere sind die Ideale in  $R$  genau die Kerne von Ringhomomorphismen, die von  $R$  ausgehen.

**Beispiel 1.11.** Ist  $R = \mathbb{Z}, J = n\mathbb{Z}$ , dann erhält man die aus der LA1 bekannten Restklassenringe:  $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \dots, \bar{n-1}\}$  mit den Verknüpfungen  $\bar{a} + \bar{b} := \overline{a + b}, \bar{a} \cdot \bar{b} = \overline{a \cdot b}$ .

**Satz 1.12** (Homomorphiesatz für Ringhomomorphismen). Sei  $\varphi : R \rightarrow S$  ein Ringhomomorphismus. Dann gibt es einen Ringhomomorphismus

$$\phi : R/\ker\varphi \rightarrow \text{im } \varphi, \bar{r} = r + \ker\varphi \mapsto \varphi(r).$$

- Beweis.* 1. Wohldefiniertheit von  $\phi$ : Seien  $r_1, r_2 \in R$  mit  $\bar{r}_1 = \bar{r}_2 \implies r_1 - r_2 \in \ker\varphi \implies \varphi(r_1 - r_2) = 0 \implies \varphi(r_1) = \varphi(r_2)$
2.  $\phi$  ist ein Ringhomomorphismus:  $\phi(\bar{r}_1 + \bar{r}_2) = \phi(\overline{r_1 + r_2}) = \varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2) = \phi(\bar{r}_1) + \phi(\bar{r}_2)$ , analog für " $\cdot$ ",  $\phi(1) = \varphi(1) = \bar{1}$
3.  $\phi$  ist injektiv: Sei  $r \in R$  mit  $\phi(\bar{r}) = 0 \implies \varphi(r) = 0 \implies r \in \ker\varphi \implies r - 0 \in \ker\varphi \implies \bar{r} = \bar{0}$ , d.h.  $\ker\phi = \{\bar{0}\}$
4.  $\phi$  ist surjektiv: Nach Konstruktion

□

**Beispiel 1.13.** Seien  $K$  ein Körper,  $R = K[t]$ ,  $\varphi : K[t] \rightarrow K, f \mapsto f(0)$ .  $\varphi$  ist ein Ringhomomorphismus,  $\text{im } \varphi = K, \ker\varphi = \{f \in K[t] \mid f(0) = 0\} = \{tg \mid g \in K[t]\} = tK[t]$ . Wir erhalten einen Ringhomomorphismus

$$\phi : K[t]/tK[t] \xrightarrow{\cong} K, f + tK[t] \mapsto f(0)$$

**Bemerkung 1.14.** Seien  $J \subseteq R$  ein Ideal,  $\pi : R \rightarrow R/J$  die kanonische Projektion. Dann sind die Abbildungen

$$\begin{aligned} \{\text{Ideale in } R/J\} &\xleftrightarrow{\quad} \{\text{Ideale } \tilde{J} \text{ in } R \text{ mit } \tilde{J} \supseteq J\} \\ J &\longmapsto \pi^{-1}(J) \\ J &\longmapsto \pi(J) \end{aligned}$$

zueinander inverse, inklusionserhaltende Abbildungen.

*Beweis. Übung*

□

**Definition 1.15.**  $x \in R$  heißt eine **Einheit**  $\stackrel{\text{Def}}{\iff}$  Es existiert ein  $y \in R$  mit  $xy = 1_R$ .  $R^\times := \{x \in R \mid x \text{ ist Einheit}\}$  bildet eine abelsche Gruppe bzgl. " $\cdot$ ", die **Einheitengruppe** von  $R$ .

**Anmerkung.** • vgl. LA1 Lemma 1.11

- $R$  ist Körper  $\iff R^\times = R \setminus \{0\}$
- häufig wird die alternative Notation  $R^*$  statt  $R^\times$  benutzt.

**Beispiel 1.16.** (a)  $\mathbb{Z}^\times = \{-1, 1\}$ , denn  $1 \cdot 1 = 1$  und  $(-1)(-1) = 1$  Sind  $a, b \in \mathbb{Z}$  und  $ab = 1 \implies a = b = 1$  oder  $a = b = -1$

(b)  $K$  Körper,  $(K[t])^\times = K^\times$

**Bemerkung 1.17.** Sei  $R \neq 0$ . Dann sind äquivalent:

- (i)  $R$  ist ein Körper
- (ii)  $\{0\}$  und  $R$  sind die einzigen Ideale in  $R$
- (iii) Jeder Ringhomomorphismus  $\varphi : R \rightarrow S$  in einen Ringhomomorphismus  $S \neq 0$  ist injektiv

*Beweis.* • (i)  $\Rightarrow$  (ii) Sei  $R$  ein Körper. Sei  $J \subseteq R$  ein Ideal,  $J \neq \{0\}$ . Es existiert ein  $a \in J, a \neq 0 \Rightarrow 1 = \underbrace{a}_{\in J} a^{-1} \in J \Rightarrow$  ist  $b \in R$ , dann ist  $b = b \cdot \underbrace{1}_{\in J} \in J$ , d.h.  $J = R$

- (ii)  $\Rightarrow$  (iii) Sei  $\varphi : R \rightarrow S$  ein Ringhomomorphismus mit  $S \neq 0$ . Nach 1.8 (a) ist  $\ker \varphi \subseteq R$  ein Ideal, d.h. wegen (ii) ist  $\ker \varphi = \{0\}$  oder  $\ker \varphi = R$ . Es ist  $\ker \varphi \neq R$ , denn  $\varphi(1_R) = 1_S$  und  $1_S \neq 0_S$  (Wäre  $1_S = 0_S$ , dann ist für Jedes  $a \in S: a = a \cdot 1_S = a \cdot 0_S = 0_S$ , d.h.  $S = 0$  *Widerspruch*)  $\Rightarrow \ker \varphi = \{0\}$ , d.h.  $\varphi$  ist injektiv.
- (iii)  $\Rightarrow$  (i) Sei  $a \in R \setminus R^\times$ , insbesondere existiert kein  $b \in R$  mit  $ab = 1_R \Rightarrow aR := \{ar | r \in R\} \subsetneq R$ , und  $aR$  ist ein Ideal in  $R$ .  $\Rightarrow R/aR$  ist nicht der Nullring (denn: Wenn  $R/aR = 0$ , dann  $1_R + aR = 0_R + aR$ , also  $1 \in aR$  *Widerspruch*)  $\xrightarrow{(iii)}$  Die kanonische Projektion  $\pi : R \rightarrow S = R/aR$  ist injektiv, d.h.  $\ker \pi = \{0\}$ , andererseits ist  $\ker \pi = aR$  nach 1.10, also:  $\underbrace{a \cdot 1_R}_{\in aR} = \{0\} \Rightarrow a = 0$ , d.h.  $R$  ist Körper.

□

**Definition 1.18.**  $x \in R$  heißt **Nullteiler**  $\stackrel{\text{Def:}}{\Leftrightarrow}$  Es existiert ein  $y \in R, y \neq 0_R$  mit  $xy = 0_R$ .  $R$  heißt **nullteilerfrei**  $\Leftrightarrow R \neq 0$  und  $0 \in R$  ist der einzige Nullteiler in  $R$  (**Integritätsbereich**).

**Anmerkung.** •  $R \neq 0 \Rightarrow 0_R$  ist ein Nullteiler in  $R$  (wegen  $0_R \cdot 1_R = 0_R, 0_R \neq 1_R$ ) (Achtung: Unterschiedliche Notation in Literatur)

- Im Nullring ist 0 kein Nullteiler (aber: Nullring ist nicht nullteilerfrei)

**Beispiel 1.19.** (a)  $\mathbb{Z}$  ist nullteilerfrei

(b)  $\bar{2} \in \mathbb{Z}/6\mathbb{Z}$  ist Nullteiler wegen  $\bar{2} \cdot \underbrace{\bar{3}}_{\neq 6} \neq 6 = \bar{0}$  in  $\mathbb{Z}/6\mathbb{Z}$

(c) Sei  $K$  Körper, dann ist  $K[t]$  nullteilerfrei

**Definition 1.20.** Seien  $a_1, \dots, a_n \in R, J \subseteq R$  ein Ideal.

$(a_1, \dots, a_n) := \left\{ \sum_{i=1}^n a_i r_i \mid r_1, \dots, r_n \in R \right\} \subseteq R$  heißt das **von  $a_1, \dots, a_n$  erzeugte Ideal**

$J$  heißt **Hauptideal**  $\stackrel{\text{Def:}}{\Leftrightarrow}$  Es existiert  $a \in R$  mit  $J = (a) = \{ra \mid r \in R\} =: Ra (= aR)$ .

$R$  heißt ein **Hauptidealring (HIR)**  $\stackrel{\text{Def:}}{\Leftrightarrow} R$  ist nullteilerfrei und jedes Ideal in  $R$  ist ein Hauptideal.

**Anmerkung.**  $(a_1, \dots, a_n)$  ist ein Ideal in  $R$  (leicht nachzurechnen)

- Beispiel 1.21.** (a)  $K$  Körper  $\implies K$  ist HIR (denn:  $K$  Körper  $\xrightarrow{1.17} \{0\}, R$  sind die einzigen Ideale in  $R$ ,  $\{0\} = (0), R = (1) = \{1 \cdot r | r \in R\}$  und  $K$  ist nullteilerfrei (vgl LA1, Lemma 1.15))
- (b)  $\mathbb{Z}$  ist ein HIR, denn:  $\mathbb{Z}$  ist nullteilerfrei und jedes Ideal in  $\mathbb{Z}$  ist von der Form  $n\mathbb{Z} = (n)$  (das ist Bemerkung 1.6)
- (c)  $\mathbb{Z}[t]$  ist kein HIR, denn: Es gibt kein  $f \in \mathbb{Z}[t]$  mit  $(2, t) = (f)$

*Beweis.* Annahme: Es existiert ein  $f \in \mathbb{Z}[t]$  mit  $(f) = (2, t)$ , dann existiert  $h \in \mathbb{Z}[t]$  mit  $z = hf \implies \deg h = \deg f = 0$ , d.h.  $f$  ist konstant (?), etwa  $f = a$  für ein  $a \in \mathbb{Z}$ . Außerdem existiert ein  $\tilde{h} \in \mathbb{Z}[t]$  mit  $t = \tilde{h}f = \tilde{h}a \xrightarrow{t \text{ normiert}} a = 1 \implies f = 1$ , aber:  $1 \notin (2, t)$ , denn anderenfalls existieren  $u, v \in \mathbb{Z}[t]$  mit  $1 = 2 \cdot u + t \cdot v \xrightarrow{t=0} 1 = 2 \cdot u(0) + 0 \cdot v(0) = 2 \cdot 1(0)$   
*Widerspruch*  $\square$

**Definition 1.22.** Sei  $J \subseteq R$  ein Ideal.  $J$  heißt

**Primideal**  $\stackrel{\text{Def:}}{\iff} J \neq R$  und für alle  $x, y \in R$  gilt:  $xy \in J \implies x \in J$  oder  $y \in J$ .

**maximales Ideal**  $\stackrel{\text{Def:}}{\iff} J \neq R$  und es existiert kein Ideal  $I \subseteq R$  mit  $J \subsetneq I \subsetneq R$

(d.h.  $J$  ist maximal bezüglich " $\subseteq$ " unter allen Idealen  $\neq R$  in  $R$ )

**Bemerkung 1.23.** Sei  $J \subseteq R$  ein Ideal. Dann gilt:

- (a)  $J$  ist Primideal  $\iff R/J$  nullteilerfrei
- (b)  $J$  maximales Ideal  $\iff R/J$  Körper

*Beweis.* (a) Die Bedingung  $xy \in J \implies x \in J$  oder  $y \in J$  ist äquivalent zu  $\bar{x} \cdot \bar{y} = \bar{0} \implies \bar{x} = \bar{0}$  oder  $\bar{y} = \bar{0}$  in  $R/J$ .  $J \neq R$  ist äquivalent zu  $R/J \neq 0$ . D.h.  $J$  Primideal ist äquivalent zur Nullteilerfreiheit von  $R/J$ .

- (b) Bemerkung 1.16: Ideale  $I \subseteq R$  mit  $J \subsetneq I \subsetneq R$  entsprechen genau den Idealen in  $R/J$ , die  $\neq \{0\}$  und  $\neq R/J$  sind. Nach Bemerkung 1.17 ist  $R/J$  genau dann ein Körper, wenn es solche Ideale nicht gibt.  $\square$

**Folgerung.** Sei  $J \subseteq R$  ein maximales Ideal. Dann ist  $J$  ein Primideal:

*Beweis.* Folgt aus 1.23, da jeder Körper nullteilerfrei ist (LA1, Lemma 1.15)  $\square$

**Frage.** Primideale/maximale Ideale in  $\mathbb{Z}$ ?

**Bemerkung 1.24.** Sei  $n \in \mathbb{N}$ . Dann sind äquivalent:

- (i)  $n$  ist Primzahl
- (ii)  $\mathbb{Z}/n\mathbb{Z}$  ist nullteilerfrei
- (iii)  $\mathbb{Z}/n\mathbb{Z}$  ist ein Körper

*Beweis.* • (i)  $\Leftrightarrow$  (iii): LA1, Lemma 1.16, Bemerkung 1.17

• (iii)  $\Rightarrow$  (ii): Körper sind nullteilerfrei. LA 1; Lemma 1.15

• (ii)  $\Rightarrow$  (i): Beweis durch vollständige Induktion:

1. Falls  $n = 1$ , dann  $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\mathbb{Z} = 0$  nicht nullteilerfrei

2. Falls  $n > 1$ , Keine Primzahl, dann  $n = ab$  mit  $1 < a, b < n \Rightarrow \bar{0} = \bar{n} = \bar{a} \cdot \bar{b} \Rightarrow \mathbb{Z}/n\mathbb{Z}$  nicht nullteilerfrei.

□

**Folgerung.** • Primideale in  $\mathbb{Z}:(0), (p)$  für  $p$  Primzahl.

• Maximale Ideale in  $\mathbb{Z}:(p)$  für  $p$  Primzahl

*Beweis.* Für  $n < 0$  ist  $(-n) = (n)$ . Rest aus 1.25

□

**Ziel.** Jeder Ring  $\neq 0$  hat ein maximales Ideal.

**Anmerkung.** Dafür benötigen wir ein Axiom aus der Mengenlehre, das **Auswahlaxiom**. Ist  $I$  eine Menge und  $(A_i)_{i \in I}$  eine Familie von nichtleeren Mengen, dann gibt es eine Abbildung

$$\gamma : I \longrightarrow \bigcup_{i \in I} (A_i) \text{ mit } \gamma(i) \in A_i, \forall i \in I \text{ (Auswahlfunktion)}$$

Das Auswahlaxiom ist äquivalent zu folgenden Aussagen:

- Zornsches Lemma (1.32)
- Jeder Vektorraum hat eine Basis
- Jeder Ring  $\neq 0$  hat ein maximales Ideal.

**Definition 1.25.** Sei  $M$  eine Menge,  $\sim$  eine Relation auf  $M$ .

•

$\sim$  heißt **antisymmetrisch**  $\stackrel{\text{Def:}}{\Leftrightarrow}$  Für alle  $a, b \in M$  gilt :  $a \sim b$  und  $b \sim a \Rightarrow a = b$

**total**  $\stackrel{\text{Def:}}{\Leftrightarrow}$  Für alle  $a, b \in M$  gilt :  $a \sim b$  oder  $b \sim a$

•

$\sim$  heißt **Halbordnung** auf  $M$   $\stackrel{\text{Def:}}{\Leftrightarrow} \sim$  reflexiv, antisymmetrisch und transitiv

**Totalordnung** auf  $M$   $\stackrel{\text{Def:}}{\Leftrightarrow} \sim$  ist eine Halbordnung und  $\sim$  ist total

In diesen Fällen sagt man auch: Das Tupel  $(M, \sim)$  ist eine halbgeordnete bzw. totalgeordnete Menge.

**Beispiel 1.26.** (a)  $\leq$  ist auf  $\mathbb{N}$  eine Totalordnung

(b) Sei  $M = \mathbb{P}(\{1, 2, 3\})$ ,  $\subseteq$  auf  $M$  eine Halbordnung, aber keine Totalordnung. Es ist zum Beispiel weder  $\{1\} \subset \{3\}$  noch  $\{3\} \subset \{1\}$ .

**Definition 1.27.** Sei  $(M, \leq)$  eine halbgeordnete Menge,  $a \in M$ .  $a$  heißt ein **maximales Element** vom  $M$   $\stackrel{\text{Def:}}{\Leftrightarrow}$  Für alle  $x \in M$  gilt  $a \leq x \Rightarrow x = a$

**Anmerkung.** Für ein maximales Element  $a \in M$  gilt nicht notwendig  $x \leq a$  für  $x \in M$ . Im allgemeinen existieren maximale Elemente nicht unbedingt.

**Beispiel 1.28.** (a) In  $(\{\{1\}, \{2\}, \{3\}, \{1, 2\}, \{2, 3\}, \{1, 3\}, \subseteq\})$  sind  $\{1, 2\}, \{2, 3\}, \{1, 3\}$  maximale Elemente.

(b) maximale Ideale im Ring  $R$  sind maximale Elemente von  $\{I \not\subseteq R \mid I \text{ ist Ideal}\}$  bezüglich  $\subseteq$ .



**Definition 1.29.** Sei  $(M, \leq)$  eine halbgeordnete Menge.  $(M, \leq)$  heißt **induktiv geordnet**  $\stackrel{\text{Def:}}{\Leftrightarrow}$  Jede Teilmenge von  $T \in M$ , für die  $(T, \leq)$  totalgeordnet ist, besitzt eine obere Schranke, d.h. es existiert ein  $S \in M$  mit  $t \leq S$  für alle  $t \in T$ .

**Satz 1.30** (Zornsches Lemma). Jede induktiv geordnete nichtleere Menge  $(M, \leq)$  besitzt ein maximales Element.

**Anmerkung.** Das zornsche Lemma ist äquivalent zum Auswahlaxiom.

**Satz 1.31.** Sei  $R \neq 0$ . Dann besitzt  $R$  ein maximales Ideal.

*Beweis.* Sei  $X := \{I \not\subseteq R \mid I \text{ Ideal}\}$

- $X$  ist bzgl.  $\subseteq$  halbgeordnet
- $X \neq \emptyset$  wegen  $\{0\} \in X$
- Sei  $\{I_\lambda \mid \lambda \in 1\}$  totalgeordnete Teilmenge von  $X$  (d.h. für  $\lambda, \mu \in 1 : I_\lambda \subseteq I_\mu$  oder  $I_\mu \subseteq I_\lambda$ )  
Behauptung:  $\{I_\lambda \mid \lambda \in 1\}$  besitzt eine obere Schranke in  $X$ , d.h. es existiert ein  $J \in X$  mit  $I_\lambda \subseteq J$  für alle  $\lambda \in 1$  denn: Setze  $I := \bigcap_{\lambda \in 1} I_\lambda$

1.  $I$  ist ein Ideal, denn:  $0 \in I$  wegen  $0 \in I_\lambda$  für alle  $\lambda \in 1$

(J2)  $a, b \in I \implies$  Es existiert  $\lambda, \mu$  mit  $a \in I_\lambda, b \in I_\mu$ , ohne Einschränkungen gelte  
 $I_\lambda \subseteq I_\mu \implies \underbrace{a}_{\in I_\lambda \subseteq I_\mu} + \underbrace{b}_{\in I_\mu} \in I_\mu \subseteq I$

(J2)  $a \in I, r \in R \implies$  Es existiert  $\lambda \in 1$  mit  $a \in I_\lambda \implies ra \in I_\lambda \subseteq I$

2.  $I \not\subseteq R$ , denn  $i \subseteq R$  und  $I \neq R$  wegen  $1 \neq I_\lambda$  für alle  $\lambda \in 1$ , (d.h.  $I \in (X)$ )

3.  $I_\lambda \subset I$  für alle  $\lambda \in 1$ .

Zornsches Lemma:  $(X)$  besitzt maximales Element  $I$  bzgl.  $\subseteq \implies I$  ist maximales Ideal in  $R$ .

□

**Folgerung.** Es gilt:

(a) Jedes Ideal  $I \not\subseteq R$  ist einem Ideal von  $R$  enthalten.

(b) Jedes  $x \in R \setminus R^\times$  ist einem Ideal von  $R$  enthalten.

*Beweis.* (a)  $J \not\subseteq R \text{ Ideal} \implies R/I \neq 0$ , also besitzt  $R/I$  ein maximales Ideal  $\stackrel{1.14}{\implies} R$  besitzt ein maximales Ideal, das  $I$  enthält.

(b) Sei  $x \in R \setminus R^\times \implies (x) \not\subseteq R$ , denn  $1 \notin (x)$ . Behauptung folgt aus (a)

□

**Ziel.** Formulierung und Beweis des chinesischen Restsatzes.

**Definition 1.32.** Seien  $I, J \subseteq R$  Ideale. Dann sind

$$I + J := \{a + ba \in I, b \in J\}$$

$$I \cdot J := \left\{ \sum_{i=1}^n a_i b_i \mid n \in \mathbb{N}_0, a_1, \dots, a_n \in I, b_1, \dots, b_n \in J \right\}$$

und  $I \cap J$  Ideale in  $R$ . Analog für endliche Familien von Idealen, insbesondere  $I^n := \underbrace{I \cdot \dots \cdot I}_{n\text{-mal}}$

für  $n \in \mathbb{N}$ . Konvention:  $I^0 := R$ .  $I, J$  heißen **relativ prim**  $\stackrel{\text{Def:}}{\Leftrightarrow} I + J = R = (1)$

**Anmerkung.** • Das dies tatsächlich Ideale sind, rechnet man nach

- Offenbar ist Multiplikation bzw. Addition von Idealen assoziativ, Klammerung ist nicht notwendig

- $(a_1, \dots, a_n) = (a_1) + \dots + (a_n)$

**Beispiel 1.33.** Seien  $R = \mathbb{Z}, I = (2), J = (3)$

- $I + J = (1)$ , denn:  $1 = \underbrace{(-1) \cdot 2}_{\in I} + \underbrace{1 \cdot 3}_{\in J} \in I + J$

- $I \cap J = (6)$

- $IJ = (6)$

**Anmerkung.** Für  $R = \mathbb{Z}$  ist  $(m) + (n) = (m, n)$ ,  $(m) \cap (n) = (\text{kgV}(m, n))$ ,  $(m)(n) = (mn)$

**Bemerkung 1.34.**  $I, J \subseteq R$  Ideale. Dann gilt:

(a)  $I(J + K) = IJ + IK$

(b)  $(I \cap J)(I + J) \subseteq IJ \subseteq I \cap J$

(c)  $I + J = (1) \implies I \cap J = IJ$

*Beweis.* Übung. □

**Bemerkung 1.35.** Seien  $I_1, \dots, I_n \subseteq R$  paarweise relative Primideale. Dann gilt:

$$I_1 \cdot \dots \cdot I_n = I_1 \cap \dots \cap I_n$$

*Beweis.* Beweis durch Induktion nach  $n$ :

- $n = 2$ : aus 1.37 (c)

- $n \geq 3$ : Behauptung sei wahr für alle  $k < n$ . Setze  $J := I - I_1 \cdot \dots \cdot I_{n-1} \stackrel{IV}{=} I_1 \cap \dots \cap I_{n-1}$   
Behauptung:  $J + I_n = (1)$ . Denn: Nach Voraussetzung ist  $I_j + I_n = (1)$  für  $j = 1, \dots, n-1$

$$\implies \text{Für alle } j \in \{1, \dots, n-1\} \text{ existieren } x_j \in I_j, y_j \in I_n \text{ mit } x_j + y_j = 1$$

$$\implies x_1 \cdot \dots \cdot x_{n-1} - 1 = (1 - y_1) \cdot \dots \cdot (1 - y_{n-1})$$

$$\implies x_1 \cdot \dots \cdot x_{n-1} = 1 + y \text{ für ein } y \in I_n$$

$$\implies 1 = \underbrace{x_1 \cdot \dots \cdot x_{n-1}}_{\in I_1 \cdot \dots \cdot I_{n-1} = J} + \underbrace{(-1)y}_{\in I_n} \in J + I_n, \text{ d.h. } J + I_n = (1)$$

$$\text{Somit: } I_1 \cdot \dots \cdot I_n = J \cdot I_n = J \cap I_n = (I_1 \cap \dots \cap I_{n-1}) \cap I_n = I_1 \cap \dots \cap I_n.$$

□

**Definition 1.36.** Sei  $(R_i)_{i \in I}$  eine Familie von Ringen. Das kartesische Produkt  $\prod_{i \in I} R_i$  wird durch komponentenweise Addition und Multiplikation zu einem Ring. Diesen bezeichnet man als das **direkte Produkt** über die Familie  $(R_i)_{i \in I}$ .

**Satz 1.37** (Chinesischer Restsatz). Seien  $I_1, \dots, I_n \in R$  Ideale,  $\varphi : R \longrightarrow \prod_{j=1}^n R/I_j, r \mapsto (r + I_1, \dots, r + I_n)$  (ist Ringhomomorphismus). Dann gilt:

(a)  $\varphi$  ist surjektiv  $\Leftrightarrow$  Die Ideale  $I_1, \dots, I_n$  sind paarweise relativ prim.

(b)  $\ker \varphi = \bigcap_{j=1}^n I_j$

(c)  $\varphi$  ist injektiv  $\Leftrightarrow \bigcap_{j=1}^n I_j = \{0\}$

Insbesondere erhalten wir unter der Voraussetzung, dass  $I_1, \dots, I_n$  paarweise relativ prim sind, einen Ringisomorphismus

$$R / \prod_{j=1}^n I_j \cong R/I_1 \times \dots \times R/I_n$$

*Beweis.* Das Nullelement in  $R/I_j$  ist  $I_j$  und das Einselement ist  $1 + I_j$ . Für die bessere Lesbarkeit des Beweises bezeichnen wir diese (unabhängig von  $j$ ) jeweils mit  $\bar{0}, \bar{1}$ .

(a) " $\Rightarrow$ ": Sei  $\varphi$  surjektiv, seien  $i, j \in \{1, \dots, n\}, i \neq j$ .

Behauptung:  $I_i + I_j = (1)$ . Wegen  $\varphi$  surjektiv existiert ein  $x \in R$  mit

$$\varphi(x) = (\bar{0}, \dots, \bar{0}, \underbrace{\bar{1}}_{i\text{-te Stelle}}, \bar{0}, \dots, \bar{0}) \implies x \in I_j.$$

Außerdem:

$$\begin{aligned} \varphi(1-x) &= \varphi(1) - \varphi(x) \\ &= (\bar{1}, \dots, \bar{1}) - (\bar{0}, \dots, \bar{0}, \underbrace{\bar{1}}_{i\text{-te Stelle}}, \bar{0}, \dots, \bar{0}) = (\bar{1}, \dots, \bar{1}, \underbrace{\bar{1}}_{i\text{-te Stelle}}, \bar{0}, \dots, \bar{0}) \\ &\implies 1-x \in I_i \\ &\implies 1 = \underbrace{(1-x)}_{\in I_i} + \underbrace{x}_{\in I_j} \in I_i + I_j \implies I_i + I_j = (1) \end{aligned}$$

(b) " $\Leftarrow$ ": Seien  $I_1, \dots, I_n$  paarweise relativ prim.

(a) Behauptung:  $(\bar{0}, \dots, \bar{0}, \underbrace{\bar{1}}_{i\text{-te Stelle}}, \bar{0}, \dots, \bar{0}) \in \Im \varphi$  für  $i = 1, \dots, n$ . Sei  $I \in \{1, \dots, n\}$  fixiert.

Für  $j \neq i$  ist  $I_i + I_j = (1)$

$\implies$  Es existieren  $u_j \in I_i, v_j \in I_j$  mit  $u_j + v_j = 1$

Setze  $x := v_1 \cdot \dots \cdot v_{i-1} \cdot v_{i+1} \cdot \dots \cdot v_n$

$\implies x \in I_j$  für  $j \neq i$  und  $x$

$$= (1 - u_1) \cdot \dots \cdot (1 - u_{i-1}) (1 - u_{i+1} \cdot \dots \cdot (1 - u_n))$$

$$= 1 + z \text{ für ein } z \in I_i$$

$$\implies \varphi(x) = (\bar{0}, \dots, \bar{0}, \underbrace{\bar{1}}_{i\text{-te Stelle}}, \bar{0}, \dots, \bar{0})$$

(b)

Sei  $y = (r_1 + I_1, \dots, r_n + I_n)$

$$\begin{aligned} \implies \varphi(r_1 + I_1, \dots, r_n + I_n) &= \varphi(r_1)\varphi(e_1) + \dots + \varphi(r_n)\varphi(e_n) \\ &= (r_1 + I_1, \bar{0}, \dots, \bar{0}) + \dots + (\bar{0}, \dots, \bar{0}, r_n + I_n) \\ &= (r_1 + I_1, \dots, r_n + I_n) = y \end{aligned}$$

(c)  $\ker \varphi = \{r \in R \mid r + I_1 = I_1, \dots, r + I_n = I_n\} = I_1 \cap \dots \cap I_n$

(d) aus (b)

Der Rest folgt aus dem Homomorphiesatz. □

**Beispiel 1.38.** Seien  $R = \mathbb{Z}, I_1 = 2\mathbb{Z}, I_2 = 3\mathbb{Z}$ . Dann ist

$$\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, a \mapsto (a + 2\mathbb{Z}, a + 3\mathbb{Z})$$

surjektiv wegen  $2\mathbb{Z} + 3\mathbb{Z} = (1)$  (vgl. Beispiel 1.36).  $\ker \varphi = 2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$ . D.h.  $\varphi$  induziert einen Ringisomorphismus

$$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

## 2 Teilbarkeit

**Ziel.** Verallgemeinerung des Konzepts, der Teilbarkeit auf  $\mathbb{Z}$  und damit verbundene Bedirfflichkeit (z.B. Primzahl, ggT) auf nullteilerfreie Ringe. Wir zeigen, dass in jedem Hauptidealring ein Analogon des Satzes über die eindeutige Primfaktorzerlegung in  $\mathbb{Z}$ . *Notation:* In diesem Abschnitt sei  $R$  stets ein nullteilerfreier Ring.

**Definition 2.1.** Seien  $a, b \in R$ .

- $b$  heißt ein **Teiler** von  $a$  (Notation:  $b|a$ )  $\stackrel{\text{Def.}}{\Leftrightarrow}$  Es existiert ein  $c \in R$  mit  $a = bc$ .
- $a, b$  heißen **assoziiert** (Notation:  $a \hat{=} b$ )  $\stackrel{\text{Def.}}{\Leftrightarrow} a|b$  und  $b|a$

**Beispiel 2.2.**  $R = \mathbb{Z}, a \in \mathbb{Z} \Rightarrow a \hat{=} -a$

**Bemerkung 2.3.** Seien  $a, b \in R$ . Dann sind äquivalent:

- (i)  $a \hat{=} b$
- (ii) Es existiert ein  $e \in R^\times$  mit  $a = be$
- (iii)  $(a) = (b)$

*Beweis.* • (i)  $\Rightarrow$  (ii): Sei  $a \hat{=} b \Rightarrow a|b$  und  $b|a \Rightarrow$  Es existieren  $c, d \in R$  mit  $b = ac$  und  $a = bd \Rightarrow b = ac = bdc \Rightarrow b(1 - dc) = 0$

1. Erster Fall:  $b = 0 \Rightarrow a = 0$ . Setze  $e := 1$ . Fertig.

2. Zweiter Fall:  $b \neq 0 \xRightarrow{R \text{ nullteilerfrei}} 1 - dc = 0 \Rightarrow cd = 1 \Rightarrow c, d \in R^\times$ . Setze  $e := d$ , dann  $a = be$  mit  $e \in R^\times$

- (ii)  $\Rightarrow$  (iii): Sei  $a = be$  mit  $e \in R^\times \Rightarrow a \in (b) \Rightarrow (a) \subseteq (b)$ . Wegen  $e \in R^\times$  ist  $b = e^{-1}a \Rightarrow b \in (a) \Rightarrow (b) \subseteq (a)$
- (iii)  $\Rightarrow$  (i): Sei  $(a) = (b) \Rightarrow a \in (b) \Rightarrow$  Es existiert  $c \in R$  mit  $a = bc \Rightarrow b|a$ . Analog:  $a|b$ . Also:  $a \hat{=} b$ .

□

**Definition 2.4.** Seien  $a_1, \dots, a_n \in R$ .  $d \in R$  heißt ein **gtößter gemeinsamer Teiler** von  $a_1, \dots, a_n$   $\stackrel{\text{Def.}}{\Leftrightarrow}$  Die folgenden Bedingungen sind erfüllt:

(GGT1)  $d|a_1, \dots, d|a_n$

(GGT2)  $c|a_1, \dots, c|a_n \Rightarrow c|d$

Wir bezeichnen die Menge der größten gemeinsamen Teiler von  $a_1, \dots, a_n$  mit  $\text{GGT}(a_1, \dots, a_n)$

**Anmerkung.** • Sind  $d_1, d_2 \in \text{GGT}(a_1, \dots, a_n)$ , dann folgt  $d_1|d_2$  und  $d_2|d_1$ , also  $d_1 \hat{=} d_2$

- Ist  $d \in \text{GGT}(a_1, \dots, a_n)$  und  $d' \hat{=} d$ , dann ist  $d' \in \text{GGT}(a_1, \dots, a_n)$
- Ohne zusätzliche Vorraussetzung an  $R$  kann man im Allgemeinen nicht erwarten, dass  $\text{GGT}(a_1, \dots, a_n) \neq \emptyset$  (z.B. in  $R = \mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} | a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$  ist  $\text{GGT}(4, 2(1 + \sqrt{-3})) = \emptyset$ )

**Bemerkung 2.5.** Sei  $R$  ein HIR und  $a_1, \dots, a_n \in R$ . Dann gilt:

- (a)  $\text{GGT}(a_1, \dots, a_n) \neq \emptyset$
- (b)  $d \in \text{GGT}(a_1, \dots, a_n) \Leftrightarrow (d) = (a_1, \dots, a_n)$

*Beweis.* (a)  $R$  HIR  $\implies$  Es existiert  $\tilde{d} \in R$  mit  $(a_1, \dots, a_n) = (\tilde{d})$  Behauptung:  $\tilde{d} \in \text{GGT}(a_1, \dots, a_n)$ . denn:

(GGT1)  $a_i \in (a_1, \dots, a_n) = (\tilde{d}) \implies \tilde{d} | a_i$  für  $i = 1, \dots, n$

(GGT2) Sei  $c \in R$  mit  $c | a_1, \dots, c | a_n$ . Wegen  $\tilde{d} \in (a_1, \dots, a_n)$  existieren  $r_1, \dots, r_n \in R$  mit  $\tilde{d} = r_1 a_1 + \dots + r_n a_n$ . Somit folgt  $c | (r_1 a_1 + \dots + r_n a_n)$ , d.h.  $c | \tilde{d}$ .

(b) " $\Rightarrow$ ": Sei  $d \in \text{GGT}(a_1, \dots, a_n) \xrightarrow{\text{Ann. 2.4}} d \hat{=} \tilde{d} \xrightarrow{2.3} (d) = (\tilde{d}) = (a_1, \dots, a_n)$

(c) " $\Leftarrow$ ": Sei  $(d) = (a_1, \dots, a_n) \implies d \in \text{GGT}(a_1, \dots, a_n)$  mit selben Argument wie im Beweis von (a). □

**Anmerkung.** • Im Fall  $R = \mathbb{Z}$ ,  $a_1, \dots, a_n \in \mathbb{Z}$  ist  $\text{GGT}(a_1, \dots, a_n) \cap \mathbb{N}_0 = \{d\}$  für ein  $d \in \mathbb{N}_0$ . (beachte:  $\mathbb{Z}^\times = \{-1, 1\}$ .) Man nennt dann  $d$  den größten gemeinsamen Teiler von  $a_1, \dots, a_n$ :

$$d =: \text{ggT}(a_1, \dots, a_n)$$

- Im Fall  $F = K[t]$  (wobei  $K$  Körper, in §3: dies ist ein HIR),  $f_1, \dots, f_n \in K[t]$ , nicht alle  $f_i = 0$ , dann existiert ein eindeutig bestimmtes Polynom  $d \in K[t]$  mit  $d \in \text{GGT}(f_1, \dots, f_n)$  (beachte:  $(K[t])^\times = K^\times$ ). Man nennt

$$d =: \text{ggT}(f_1, \dots, f_n)$$

den größten gemeinsamen Teiler von  $f_1, \dots, f_n$ . (Und man setzt  $\text{ggT}(0, \dots, 0) := 0$ .)

**Folgerung.** Sei  $R$  ein HIR,  $a, b \in R, d \in \text{GGT}(a, b)$ . Dann existieren  $u, v \in R$  mit  $d = ua + vb$

*Beweis.* aus 2.5:  $d \in (d) = (a, b)$  □

**Definition 2.6.** Sei  $p \in R \setminus (R^\times \cup \{0\})$

$p$  heißt **irreduzibel**  $\stackrel{\text{Def:}}{\iff}$  Aus  $p = ab$  mit  $a, b \in R$  folgt stets  $a \in R^\times$  oder  $b \in R^\times$

$p$  heißt **Primelement**  $\stackrel{\text{Def:}}{\iff}$  Aus  $p | ab$  mit  $a, b \in R$  folgt stets  $p | a$  oder  $p | b$   
 $\iff (p)$  ist ein Primideal

**Anmerkung.**  $p$  irreduzibel bzw. Primelement,  $p' \hat{=} p \implies p'$  irreduzibel bzw. Primelement.

**Beispiel 2.7.**

irreduzible Elemente in  $\mathbb{Z} =$  Primzahlen aus  $\mathbb{N}$  sowie deren Negative  
 $=$  Primelemente in  $\mathbb{Z}$

**Frage.** Zusammenhang zwischen irreduziblen Elementen und Primelementen in  $R$ ?

**Bemerkung 2.8.** Sei  $p \in R \setminus (R^\times \cup \{0\})$  ein Primelement. Dann ist  $p$  irreduzibel.

*Beweis.* Sei  $p = ab$  mit  $a, b \in R \implies p | ab \xrightarrow[p \text{ Primideal}]{\implies} p | a \text{ oder } p | b$ . Gelte ohne Einschränkung:  $p | a$ . Außerdem:  $a \nmid p$ , somit  $p \hat{=} a$ . Nach 2.3 existiert ein  $w \in R^\times$  mit  $a = ep \implies p = ab = epb \implies p(1 - eb) = 0 \xrightarrow[p \neq 0]{R \text{ nullteilerfrei}} 1 - eb = 0 \implies eb = 1$ , d.h.  $b \in R^\times$  □

**Anmerkung.** Es gibt Beispiele für irreduzible Elemente, die kein Primelement sind (vgl. Übungen)

**Bemerkung 2.9.** Sei  $R$  ein HIR,  $p \in R \setminus (R^\times \cup \{0\})$ . Dann sind äquivalent:

- (i)  $p$  ist irreduzibel
- (ii)  $p$  ist Primelement

*Beweis.* • (ii)  $\implies$  (i) aus 2.9

- (i)  $\implies$  (ii) Sei  $p$  irreduzibel.
  1.  $(p)$  ist maximales Ideal in  $R$ , denn: Sei  $I \subseteq R$  Ideal mit  $(p) \subsetneq I$ . Wegen  $R$  HIR existiert  $a \in R$  mit  $I = (a) \xRightarrow{p \in I}$  Es existiert  $c \in R$  mit  $p = ac \implies a \in R^\times$  oder  $c \in R^\times$ . Falls  $c \in R^\times$ , dann  $8p) = (a) = I$  nach 2.3. Also  $a \in R^\times$ , d.h.  $I = (a) = R$  *Widerspruch*
  2. Wegen 1. und 1.24 ist  $(p)$  Primideal, d.h.  $p$  ist Primelement.

□

**Anmerkung.** Beweis hat gezeigt: In HIR gilt für  $p \in R \setminus (R^\times \cup \{0\})$  :  $p$  irreduzibel  $\Leftrightarrow (p)$  maximales Ideal.

**Frage.** Wann gilt in  $R$  ein Analogon des Satzes über die eindeutige Primfaktorzerlegung in  $\mathbb{Z}$ ?

**Definition 2.10.**  $R$  heißt **faktoriell**  $\xRightarrow{\text{Def.}}$  Jedes  $a \in R \setminus (R^\times \cup \{0\})$  lässt sich eindeutig bis auf Reihenfolge und Assoziierbarkeit als Produkt von irreduziblen Elementen aus  $R$  schreiben, d.h. es existieren irreduzible Elemente  $p_1, \dots, p_r \in R$  mit

$$a = p_1 \cdot \dots \cdot p_r$$

und sind  $q_1, \dots, q_s$  irreduzible Elemente mit  $a = q_1 \cdot \dots \cdot q_s$ , so ist  $r = s$  und nach Umm nummerieren ist  $p_i \hat{=} q_i$  für  $i = 1, \dots, r$

**Ziel.** Jeder HIR ist faktoriell.

**Definition 2.11.**  $R$  heißt **noethersch**  $\xLeftrightarrow{\text{Def.}}$  Für jede aufsteigende Kette  $I_1 \subseteq I_2 \subseteq \dots$  von Idealen in  $R$  existiert ein  $n \in \mathbb{N}$  mit  $I_k = I_n$  für alle  $k \geq n$ .

**Bemerkung 2.12.** Sei  $R$  ein HIR. Dann ist  $R$  noethersch.

*Beweis.* Sei  $I_1 \subseteq I_2 \subseteq \dots$  eine aufsteigende Kette von Idealen aus  $R$ . Setze  $I := \bigcup_{k \geq 1} I_k$

1.  $I$  ist ein Ideal in  $R$ , denn:
  - (J1)  $0 \in I_k$  für alle  $k \geq 1 \implies 0 \in I$
  - (J2) Seien  $a, b \in I \implies$  Es existieren  $k, l \in \mathbb{N}$  mit  $a \in I_k, b \in I_l$ . Mit  $m := \max\{k, l\}$  ist  $a, b \in I_m \implies a + b \in I_m \subseteq I$
  - (J3) Seien  $a \in I, r \in R \implies$  Es existiert ein  $k \in \mathbb{N}$  mit  $a \in I_k \implies ra \in I_k \subseteq I$
2. Wegen 1. und  $R$  HIR existiert ein  $a \in R$  mit  $I = (a)$ , insbesondere  $a \in I \implies$  Es existiert ein  $N \in \mathbb{N}$  mit  $a \in I_N \implies (a) \subseteq I_N \subseteq I = (a) \implies I_N = I \implies I_k = I_N$  für alle  $k \geq N$ .

□

**Satz 2.13.** Sei  $R$  ein HIR. Dann ist  $R$  faktoriell.

*Beweis.* 1. Existenz von Zerlegung in irreduzible Elemente. Setze  $M := \{(a) \mid a \in R \setminus (R^\times \cup \{0\}) \text{ besitzt keine Faktorisierung in irreduzible Elemente}\}$ .

- Annahme:  $M \neq \emptyset$ . Es existiert ein bezüglich  $\subseteq$  maximales Element  $j \in M$ , denn: Andernfalls existiert zu jedem  $I \in M$  ein  $I' \in M$  mit  $I \subsetneq I'$ , das liefert eine unendlich strikt aufsteigende Kette von Idealen in  $R$ . *Widerspruch* zu  $R$  noethersch. Es existiert ein  $a \in R$  mit  $J = (a)$ .  $a$  ist nicht irreduzibel, denn für  $a$  irreduzibel wäre  $a$  selbst eine Faktorisierung in irreduzible Elemente  $\implies J = (a) \notin M$  *Widerspruch*  $\implies$  Es existieren  $a_1, a_2 \in R \setminus (R^\times \cup \{0\})$  mit  $a = a_1 a_2 \implies (a) \subseteq (a_1), (a) \subseteq (a_2)$ . Wäre  $(a) = (a_1)$ , dann existiert ein  $b \in R^\times$  mit  $a = a_1 b = a_1 a_2 \implies a_1(a_2 - b) = 0 \xRightarrow{R \text{ nullteilerfrei}} a_2 = b \in R^\times$  *Widerspruch*. Also:  $(a) \subsetneq (a_1)$ , analog  $(a) \subsetneq (a_2) \implies (a_1), (a_2) \notin M \implies a_1, a_2$  haben Faktorisierung in irreduzible Elemente, also auch  $a = a_1 a_2$  *Widerspruch*. Also:  $M \neq \emptyset \implies$  Existenz.

2. Eindeutigkeit der Zerlegung: Sei  $a = p_1 \cdot \dots \cdot p_r = q_1 \cdot \dots \cdot p_r = q_1 \cdot \dots \cdot q_s$  mit  $p_1, \dots, p_r, p_1, \dots, p_s$  irreduzibel. Beweis per Induktion nach  $r$ :

- Induktionsanfang:  $r = 0 \implies a = 1 \implies s = 0$  (sonst  $q_1, \dots, q_s \in R^\times$  Widerspruch)
- Induktionsannahme: Die Behauptung sei für  $0, \dots, r-1$  bewiesen.
- Induktionsschritt:  $p_1 | p_1 \cdot \dots \cdot p_r = q_1 \cdot \dots \cdot q_s \xrightarrow{p_1 \text{ Primelement}} \text{Es existiert ein } j \in \{1, \dots, s\}$  mit  $p_1 | q_j$ . Nach Ummummern sei  $j = 1$ , also  $p_1 | q_1$ , etwa  $q_1 = cp_1$  mit  $c \in R$ . Da  $q_1$  irreduzibel ist, folgt  $c \in R^\times$ , also  $p_1 \hat{=} q_1 \implies p_1 \cdot \dots \cdot p_r = cp_1 q_2 \cdot \dots \cdot q_s \implies p_1(p_2 \cdot \dots \cdot p_r - cq_2 \cdot \dots \cdot q_s) = 0 \xrightarrow{R \text{ nullteilerfrei}} p_2 \cdot \dots \cdot p_r (cq_2) q_3 \cdot \dots \cdot q_s$ . Wegen  $c \in R^\times$  ist  $cq_2$  irreduzibel  $\xrightarrow{IV} r-1 = s-1 (\implies r = s)$  und nach Ummummern ist  $p_2 \hat{=} cq_2 \hat{=} q_2, p_3 \hat{=} q_3, \dots, p_r \hat{=} q_r$

□

### 3 Euklidische Ringe

*Notation:* In diesem Abschnitt sei  $R$  stets ein Ring.

**Definition 3.1.**  $R$  heißt **euklidischer Ring**  $\stackrel{\text{Def.}}{\iff} R$  ist nullteilerfrei und es existiert eine Abbildung  $\delta : R \setminus \{0\} \longrightarrow \mathbb{N}_0$ , so dass gilt: Für alle  $f, g \in R, g \neq 0$  existieren  $q, r \in R$  mit  $f = qg + r$  und  $(\delta(r) < \delta(g) \text{ oder } r = 0)$ .  $\delta$  heißt eine **Normabbildung** auf  $R$ .

**Beispiel 3.2.** 1.  $R = \mathbb{Z}$  mit  $\delta = |\cdot|$  ist ein euklidischer Ring (Bem. 1.5)

2.  $K$  Körper  $\implies R = K[t]$  mit  $\delta = \deg$  ist ein euklidischer Ring
3.  $K$  Körper mit  $\delta : K \setminus \{0\} \longrightarrow \mathbb{N}_0, x \mapsto 1$  ist ein euklidischer Ring (hier ist  $f = fg^{-1}g + 0$ , hier ist  $r = 0$ )
4.  $R = \mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$  ist ein euklidischer Ring mit  $\delta(x + iy) = x^2 + y^2$  (Ring mit ganzen Gaußschen Zahlen) (vgl. Übungen)

**Satz 3.3.** Sei  $R$  ein euklidischer Ring. Dann ist  $R$  ein Hauptidealring.

*Beweis.* Sei  $I \subseteq R$  ein Ideal,  $I \neq 0$ . Es ist  $\emptyset \neq \{\delta(a) | a \in I \setminus \{0\}\} \subseteq \mathbb{N}_0$ . Wähle  $a \in I \setminus \{0\}$ , so dass  $\delta(a)$  minimal. Behauptung:  $I = (a)$ , denn:

- " $\supseteq$ ": Wegen  $a \in I$  ist  $(a) \subseteq I$
- " $\subseteq$ ": Sei  $f \in I \implies$  Es existiert  $a, r \in R$  mit  $f = qa + r$  und  $(\delta(r) < \delta(a) \text{ oder } r = 0) \implies r = f - qa \in I$ . Wegen  $\delta(a)$  minimal folgt  $r = 0 \implies f = qa \in (a)$

□

**Anmerkung.** Es gibt Hauptidealringe, die nicht euklidisch sind (siehe Beispieldatenbank)

**Folgerung.** Sei  $R$  ein euklidischer Ring. Dann ist  $R$  faktoriell.

*Beweis.*  $R$  euklidisch  $\xrightarrow{3.3} R$  Hauptidealring  $\xrightarrow{2.14} R$  faktoriell. □

**Folgerung.** Sei  $K$  ein Körper,  $f \in K[t], f \neq 0$ . Dann besitzt  $f$  eine bis auf Reihenfolge der Faktoren eindeutige Darstellung:

$$f = c p_1^{e_1} \cdot \dots \cdot p_r^{e_r}$$

mit  $c \in K^\times, r \geq 0, e_1, \dots, e_r \in \mathbb{N}$  und paarweise verschiedenen normierten irreduziblen Polynomen  $p_1, \dots, p_r$ .

*Beweis.* nach 3.2 ist  $K[t]$  euklidisch, nach 3.4 also faktoriell. □

**Satz 3.4** (Euklidischer Algorithmus). Sei  $R$  ein euklidischer Ring mit Normabbildung  $\delta, a, b \in R \setminus \{0\}$ . Wir betrachten eine Folge  $a_0, a_1, \dots$  von Elementen aus  $R$ , die induktiv wie folgt gegeben ist:

$$\begin{aligned}
 a_0 &:= a \\
 a_1 &:= b \\
 a_0 &:= q_0 a_1 + a_2 \text{ mit } \delta(a_2) < \delta(a_1) \text{ oder } a_2 = 0 \\
 \text{Falls } a_2 \neq 0 : a_1 &:= q_1 a_2 + a_3 \text{ mit } \delta(a_3) < \delta(a_2) \text{ oder } a_3 = 0 \\
 &\vdots \\
 \text{Falls } a_i \neq 0 : a_{i-1} &:= q_{i-1} a_i + a_{i+1} \text{ mit } \delta(a_{i+1}) < \delta(a_i) \text{ oder } a_{i+1} = 0 \\
 &\vdots
 \end{aligned}$$

Dann existiert ein eindeutig bestimmter Index  $n \in \mathbb{N}$  mit  $a_n \neq 0, a_{n+1} = 0$ . Es ist dann

$$d := a_n \in \text{GGT}(a, b)$$

Durch Rückwärtseinsetzen lässt sich  $d$  als Linearkombination von  $a, b$  darstellen:

$$d = a_n = a_{n-2} - q_{n-2} a_{n-1} = \dots = ua + vb \text{ mit } u, v \in R$$

(erweiterter euklidischer Algorithmus)

**Beispiel 3.5.**  $R = \mathbb{Z}, a = 24, b = 15$

$$\begin{aligned}
 24 &= 1 \cdot 15 + 9 \\
 15 &= 1 \cdot 9 + 6 \\
 9 &= 1 \cdot 6 + 3 \\
 6 &= 2 \cdot 3 + 0
 \end{aligned}$$

$$\implies \text{ggT}(24, 15) = 3$$

Es ist

$$3 = 9 - 1 \cdot 6 = 9 - (15 - 1 \cdot 9) = 2 \cdot 9 - 1 \cdot 15 = 2 \cdot (24 - 1 \cdot 15) - 15 = 2 \cdot 24 - 3 \cdot 15.$$

*von 3.6.* Falls  $a_i \neq 0$  für alle  $i \in \mathbb{N}$ , dann wäre  $\delta(a_1) > \delta(a_2) > \dots$  eine streng monoton fallende unendliche Folge in  $\mathbb{N}_0$ . *Widerspruch.*  $\implies$  Es existiert ein eindeutig bestimmtes  $n \in \mathbb{N}$  mit  $a_n \neq 0, a_{n+1} = 0$ . Wir betrachten die Gleichungen:

$$\begin{aligned}
 (G_0) \quad a_0 &= q_0 a_1 + a_2 \\
 &\vdots \\
 (G_{n-2}) \quad a_{n-2} &= q_{n-2} a_{n-1} + a_n \\
 (G_{n-1}) \quad a_{n-1} &= q_{n-1} a_n
 \end{aligned}$$

Dann gilt:  $a_n | a_{n-1} \xrightarrow{(a_{n-2})} a_n | (q_{n-2} a_{n-1} + a_n) = a_{n-2} \implies \dots \implies a_n | a_1$  und  $a_n | a_0$ . Sei  $c \in R$  mit  $c | a_0$  und  $c | a_1 \xrightarrow{(a_0)} c | (a_0 - q_0 a_1) = a_2 \implies \dots \implies c | a_n$ . Also:  $a_n \in \text{GGT}(a_0, a_1) = \text{GGT}(a, b)$ . Es ist

$$\begin{aligned}
 a_n &= a_{n-2} - q_{n-2} a_{n-1} \xrightarrow{G_{n-3}} a_{n-2} - q_{n-2} (a_{n-3} - q_{n-3} a_{n-2}) \\
 &= (1 + q_{n-2} q_{n-3}) a_{n-2} - q_{n-2} a_{n-3} = \dots = ua + vb
 \end{aligned}$$

(mit geeigneten  $u, v \in R$ ) □



**Satz 3.6** (Gauß-Diagonalisierung von Matrizen). Sei  $R$  ein euklidischer Ring,  $A \in M_{n,n}(R)$ . Dann gilt:  $A$  lässt sich durch wiederholtes Anwenden von elementaren Zeilen- und Spaltenoperationen vom Typ

- Addition des  $\lambda$ -fachen einer Zeile/Spalte zu einer anderen Zeile bzw. Spalte
- Zeilen-/Spaltenvertauschung

in eine Matrix der Gestalt

$$\left( \begin{array}{ccc|c} c_1 & & & \\ & c_2 & & \\ & & \ddots & \\ & & & c_r \\ \hline & & & 0 \end{array} \right)$$

mit  $c_1, \dots, c_r \in R \setminus \{0\}, c_1 | c_2 | \dots | c_r$  überführen.

*Beweis.* Falls  $A = 0$ , dann fertig. Im Folgenden sei  $A = (a_{ij}) \neq 0$ . Sei  $\delta$  eine Normabbildung auf  $R$ .

1. Durch Zeilen- und Spaltenvertauschen erreichen wir  $a_{11} \neq 0$  und  $\delta(a_{11}) \leq \delta(a_{ij})$  für alle  $i, j$  mit  $a_{ij} \neq 0$ .
2. Ziel: Bringe  $A$  auf die Form

$$\left( \begin{array}{c|c} * & 0 \\ \hline 0 & * \end{array} \right)$$

, wobei links oben Element  $\neq 0$  mit minimalen  $\delta$

- 1. Fall: In der ersten Spalte/Zeile stehen keine Elemente  $\neq 0$  außer  $a_{11}$ ; dann fertig
- 2. Fall: In der ersten Spalte/Zeile stehen noch Elemente  $\neq 0$ , ohne Einschränkung  $a_{21} \neq 0 \implies$  Es existiert ein  $a \in R$  mit  $a_{21} = qa_{11}$  oder  $\delta(a_{21} - qa_{11}) < \delta(a_{11})$ . Addiere das  $(-q)$ -fache der 1. Zeile zur 2. Zeile (\*\*).  $\implies$  Erhalte Matrix  $A' = (a'_{ij})$  mit  $a'_{21} \neq 0$  oder  $\delta(a'_{21}) < \delta(a_{11})$ . Erhalte durch Zeilen/Spaltenvertauschen eine Matrix

$$A'' = (a''_{ij}) \text{ mit } a''_{11} \neq 0, \delta(a''_{11}) \leq \delta(a''_{ij}) \text{ für alle } i, j \text{ mit } a''_{ij} \neq 0$$

und  $\delta(a''_{11}) \leq \delta(a_{11})$  (–" nur, wenn obige Division aufgefangen und  $\delta(a_{11})$  nach (\*\*)) immer noch minimal). Iteriere dies, dieser Prozess bricht nach endlich vielen Iterationen ab. Erhalte eine Matrix der Form

$$D = \left( \begin{array}{c|c} d_{11} & \\ \hline 0 & * \end{array} \right)$$

mit  $d_{11} \neq 0, \delta(d_{11}) \leq \delta(d_{ij})$  falls  $d_{ij} \neq 0, \delta(d_{11}) \leq \delta(a_{11})$

3. Erreiche  $d_{11} | d_{ij}$  für alle  $i, j$ .

- 1. Fall: Es gilt bereits  $d_{11} | d_{ij}$  für alle  $i, j$  dann fertig
- 2. Fall: Es existieren  $i, j$  mit  $d_{11}$  nicht Teiler von  $d_{ij} \implies$  Es existiert ein  $q \in R$  mit  $d_{ij} - qd_{11} \neq 0$  und  $\delta(d_{ij} - qd_{11}) < \delta(d_{11})$ . Addiere erste Zeile von  $D$  zur  $i$ -ten Zeile

von  $D$ , erhalte

$$\left( \begin{array}{c|cccc} d_{11} & 0 & \dots & 0 & \dots & 0 \\ \hline 0 & & & * & & \\ \vdots & & & & & \\ d_{11} & d_{i2} & \dots & d_{ij} & \dots & d_{in} \\ 0 & & & & & \\ \vdots & & & * & & \\ 0 & & & & & \end{array} \right)$$

. Subtrahiere das  $q$ -fache der ersten Spalte von der  $j$ -ten Spalte dieser Matrix, erhalte

$$D' = (d'_{ij}) = \left( \begin{array}{c|cccc} d_{11} & 0 & \dots & 0 & -qd_{11} & 0 & \dots & 0 \\ \hline 0 & & & & * & & & \\ \vdots & & & & & & & \\ 0 & & & & & & & \\ d_{11} & * & & d_{ij} - qd_{11} & & & * & \\ 0 & & & & & & & \\ \vdots & & & & & & & \\ 0 & & & & * & & & \end{array} \right)$$

mit  $d'_{ij} = d_{ij} - qd_{11}$ ,  $\delta(d'_{ij}) < \delta(d_{11}) \leq \delta(a_{11})$ . Wiederhole die gesamte bisherige Prozedur für die Matrix  $D'$ . Dieser Prozess bricht nach endlich vielen Schritten ab. Wir erhalten eine Matrix

$$C = \left( \begin{array}{c|c} c_{11} & D \\ \hline 0 & C' \end{array} \right)$$

mit  $c_{11} \neq 0$ ,  $\delta(c_{11}) \leq \delta(a_{11})$  und  $c_{11}|c_{ij}$  für alle  $i, j$ .

4. Wende das Verfahren auf  $C'$  an (und iteriere dies). Operationen an  $C'$  erhalten die Teilbarkeit durch  $c_{11}$ , d.h. wir können die Matrix auf die Gestalt

$$\left( \begin{array}{c|c} * & 0 \\ \hline 0 & * \end{array} \right)$$

mit  $c_1|c_2|c_3|\dots|c_r$  bringen.

□

**Beispiel 3.7.** (a)  $R = \mathbb{Z}$  mit  $\delta = |\cdot|$ .

$$\begin{aligned} A &= \begin{pmatrix} 4 & 3 \\ 6 & 5 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 3 & 4 \\ 5 & 6 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 3 & 1 \\ 5 & 1 \end{pmatrix} \\ &\rightsquigarrow \begin{pmatrix} 1 & 3 \\ 1 & 5 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix} \mid \Pi - \text{I} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \end{aligned}$$

(b)  $R = \mathbb{Q}[t]$  mit  $\delta = \deg$ .

$$A = \begin{pmatrix} t-1 & 0 \\ -1 & t-1 \end{pmatrix} \begin{matrix} \leftarrow \square \\ \leftarrow \square \end{matrix} \rightsquigarrow \begin{pmatrix} -1 & t-1 \\ t-1 & 0 \end{pmatrix} \mid \Pi + (t-1)\text{I} \rightsquigarrow \begin{pmatrix} -1 & t-1 \\ 0 & (t-1)^2 \end{pmatrix} \rightsquigarrow \rightsquigarrow \begin{pmatrix} -1 & 0 \\ 0 & (t-1)^2 \end{pmatrix}$$

**Erinnerung an LA1**

- Zeilen-/bzw. Spaltenoperationene wie in 3.8 lassen sich durch Multiplikation mit Elementarmatrizen

$$E_{ij} = \begin{pmatrix} 1 & & \\ & \ddots & \\ \lambda & & 1 \end{pmatrix}$$

$$P_{ij} = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & 0 & & & 1 \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 & 0 \\ & & 1 & & & & & & 1 \\ & & & & & & & & & \ddots \\ & & & & & & & & & & 1 \end{pmatrix}$$

von links bzw. rechts beschreiben.

- Determinanten lassen sich auch von quadratischen Matrizen mit Einträgen in  $R$  bilden (via Leibnizformel). Es ist  $A\tilde{A} = \tilde{A} = \det(A)E_n$ , wobei  $\tilde{A}$  adjungte Matrix zu  $A$ . Insbesondere:  $A \in M_{n,n}(R)$  invertierbar (d.h. es existiert  $B \in M_{n,n}(R)$  mit  $AB = BA = E_n$ )  $\Leftrightarrow \det(A) \in R^\times$  (vgl. LA1 Def. 4.63)

### Definition 3.8.

$$\text{GL}(R) = \{A \in M_{n,n}(R) | A \text{ ist invertierbar} \} = \{A \in M_{n,n}(R) | \det(A) \in R^\times \}$$

ist eine Gruppe bzgl. Multiplikation, die **allgemeine lineare Gruppe** über  $R$  von Rang  $n$ .

**Definition 3.9.**  $A$  heißt **äquivalent** z  $B$  ( $A \sim B$ )  $\stackrel{\text{Def.}}{\Leftrightarrow}$  Es existieren  $S \in \text{GL}_n(R), T \in \text{GL}_n(R)$  mit  $B = SAT^{-1}$ . Falls  $m = n$ , so heißt  $A$  **ähnlich** zu  $B$  ( $A \approx B$ )  $\stackrel{\text{Def.}}{\Leftrightarrow}$  Es existiert  $S \in \text{GL}_n(R)$  mit  $B = SAS^{-1}$

**Anmerkung.** •  $\sim, \approx$  sind Äquivalenzrelationen auf  $M_{m,n}(K)$ , nzw.  $M_{n,n}(K)$

- $K$  Körper,  $A, B \in M_{n,n}(K), C$  Basis von  $K^n, D$  Basis von  $K^m, f : K^n \rightarrow K^m$  lineare Abbildung mit  $M_D^C(f) = A$ . Dann:  $A \sim B \Leftrightarrow$  Es existieren Basen  $C', D'$  von  $K^n$  bzw.  $K^m$  mit  $M_{D'}^{C'}(f) = B$  (d.h.  $A, B$  beschreiben bzgl. geeigneter Basen dieselbe lineare Abbildung)

**Frage.** Gibt es innerhalb einer Äquivalenzklasse bzgl.  $\sim$  einen besonders schönen Vertreter?

**Folgerung.** Sei  $R$  ein euklidischer Ring,  $A \in M_{m,n}(R)$ . Dann existieren  $c_1, \dots, c_r \in R \setminus \{0\}$  mit  $c_1 | c_2 | \dots | c_r$  und

$$A \sim \left( \begin{array}{ccc|c} c_1 & & 0 & 0 \\ & \ddots & & \\ 0 & & c_r & \\ \hline & & 0 & 0 \end{array} \right)$$

*Beweis.* Umformungen in 3.8 korrespondieren zur Multiplikation mit Elementarmatrizen von links bzw. rechts mit Determinante  $\in \{-1, 1\}$  (diese sind also invertierbar)  $\square$

**Anmerkung.** Um durch Zeilen- bzw. Spaltenoperationen zu

$$A \sim \left( \begin{array}{ccc|c} c_1 & & 0 & 0 \\ & \ddots & & \\ 0 & & c_r & \\ \hline & & 0 & 0 \end{array} \right)$$

zu gelangen, darf man auch Zeilen bzw. Spalten mit  $\lambda \in R^\times$  multiplizieren

$$\begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & \lambda & & \\ & & & & 1 & \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix}$$

(invertierbar für  $\lambda \in R^\times$ ) d.h.: Im Allgemeinen zu 3.8 ist diese Operation jetzt auch erlaubt.

**Erinnerung.** Sei  $K$  ein Körper,  $A \in M_{n,n}(K)$ . Dann gelten:

- $\text{Rang } A = r \implies$

$$A \sim \left( \begin{array}{c|c} E_r & 0 \\ \hline 0 & 0 \end{array} \right)$$

- $S \in \text{GL}_n(K), T \in \text{GL}_n(K) \implies \text{Rang}(SAT^{-1}) = \text{Rang}(A)$

Es folgt für  $A, B \in M_{m,n}(K)$ :

$$A \sim B \Leftrightarrow \text{Rang } A = \text{Rang } B$$

**Ziel.** Klassifikation von Matrizen aus  $M_{m,n}(R)$ ,  $R$  euklidischer Ring, bis auf Äquivalenz.

**Definition 3.10.** Sei  $A \in M_{m,n}(R)$ ,  $1 \leq k \leq m$ ,  $1 \leq l \leq n$ .

- $B \in M_{k,l}(R)$  heißt eine **Untermatrix von A**  $\stackrel{\text{Def.}}{\Leftrightarrow}$   $B$  entsteht aus  $A$  durch Streichen  $m - k$  Zeilen und  $n - l$  Spalten.
- Ist  $B \in M_{l,l}(R)$  eine quadratische Untermatrix von  $A$  mit  $(l \leq \min\{m, n\})$ , dann heißt  $\det(B)$  ein **Minor  $l$ -ter Stufe** von  $A$ .
- $\text{Fit}_l(A) = (\det(B) | B \text{ ist } l \times l - \text{Untermatrix von } A) \subseteq R$  (d.h. das von allen Minoren  $l$ -ter Stufe von  $A$  erzeugte Ideale in  $R$ ) heißt das  **$l$ -te Fittingideal** von  $A$ .

**Beispiel 3.11.**

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

- $\text{Fit}_1(A) = (\det(1), \det(2), \det(3), \det(4)) = (1, 2, 3, 4) = (1) = \mathbb{Z}$

•

$$\text{Fit}_2(A) = \left( \det \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \right) = (-2) = 2\mathbb{Z}$$

**Satz 3.12** (Fittings Lemma). Seien  $A \in M_{m,n}(R)$ ,  $S \in \text{GL}_m(R)$ ,  $T \in \text{GL}_n(R)$ ,  $l \leq \min\{m, n\}$ . Dann gilt:

$$\text{Fit}_l(A) = \text{Fit}_l(SA) = \text{Fit}_l(AT)$$

*Beweis.* 1.  $\text{Fit}_l(SA) \subseteq \text{Fit}_l(A)$ , denn:

$$A = (a_{ij}) \in M_{m,n}(R), S = (s_{ij}) \in \text{GL}_m(R), SA = (b_{ij}) \in M_{m,n}(R).$$

Seien  $A \leq i_1 < i_2 < \dots < i_l \leq m$ ,  $1 \leq j_1 < j_2 < \dots < j_l \leq n$ . Wir betrachten die  $l \times l$ -Untermatrix

$$B = \begin{pmatrix} b_{i_1, j_1} & \dots & b_{i_1, j_l} \\ \vdots & & \vdots \\ b_{i_l, j_1} & \dots & b_{i_l, j_l} \end{pmatrix}$$

von  $SA$

$$\begin{aligned}
 \Rightarrow \det(B) &= \det \begin{pmatrix} \sum_{r_1=1}^m s_{i_1, r_1} a_{r_1, j_1} & \dots & \sum_{r_1=1}^m s_{i_1, r_1} a_{r_1, j_l} \\ b_{i_2, j_1} & \dots & b_{i_2, j_l} \\ \vdots & & \vdots \\ b_{i_l, j_1} & \dots & b_{i_l, j_l} \end{pmatrix} \\
 &= \sum_{r_1=1}^m s_{i_1, r_1} \cdot \det \begin{pmatrix} a_{r_1, j_1} & \dots & a_{r_1, j_l} \\ b_{i_2, j_1} & \dots & b_{i_2, j_l} \\ \vdots & & \vdots \\ b_{i_l, j_1} & \dots & b_{i_l, j_l} \end{pmatrix} \\
 &= \sum_{r_1=1}^m \dots \sum_{r_l=1}^m s_{i_1, r_1} \cdot \dots \cdot s_{i_l, r_l} \underbrace{\det \begin{pmatrix} a_{r_1, j_1} & \dots & a_{r_1, j_l} \\ \vdots & & \vdots \\ a_{i_l, j_1} & \dots & a_{i_l, j_l} \end{pmatrix}}_{\substack{0, \text{ falls } i \neq j \text{ existieren mit } r_i = r_j \\ \pm \text{ein Minor } l\text{-ter Stufe von } A}} \in \text{Fit}_l(A) \\
 &= \begin{cases} 0, & \text{falls } i \neq j \text{ existieren mit } r_i = r_j \\ \pm \text{ein Minor } l\text{-ter Stufe von } A \end{cases}
 \end{aligned}$$

$$\Rightarrow \text{Fit}_l(SA) \subseteq \text{Fit}_l(A).$$

2. Wende 1. auf  $S^{-1} \in \text{GL}_m(R), SA \in M_{m,n}(R)$  an

$$\Rightarrow \text{Fit}_l(S^{-1}(SA)) \subseteq \text{Fit}_l(SA), \text{ also } \text{Fit}_l(A) \subseteq \text{Fit}_l(SA)$$

3.  $\text{Fit}_l(A) = \text{Fit}_l(A^t)$ , also  $\text{Fit}_l(AT) = \text{Fit}_l((AT)^t) = \text{Fit}_l(T^t A^t) \stackrel{2.}{=} \text{Fit}_l(A^t) = \text{Fit}_l(A)$

□

**Folgerung.** Seien  $A, B \in M_{m,n}(R)$  mit  $A \sim B$ . Dann gilt:  $\text{Fit}_l(A) = \text{Fit}_l(B)$  für alle  $l \leq \min\{m, n\}$

*Beweis.*  $A \sim B \Rightarrow$  Es existieren  $S \in \text{GL}_m(R), T \in \text{GL}_n(R)$  mit  $B = SAT^{-1} \Rightarrow \text{Fit}_l(B) = \text{Fit}_l(SAT^{-1}) \stackrel{3.15}{=} \text{Fit}_l(AT^{-1}) \stackrel{3.15}{=} \text{Fit}_l(A)$  □

**Bemerkung 3.13.** Sei  $R$  ein nullteilerfreier Ring,

$$A = \left( \begin{array}{ccc|c} c_1 & & & 0 \\ & c_2 & & \vdots \\ & & \ddots & \\ & & & c_r \\ \hline 0 & \dots & 0 & 0 \end{array} \right) \in M_{m,n}(R)$$

, mit  $c_1, \dots, c_r \in R \setminus \{0\}, c_1 | c_2 | \dots | c_r$ . Dann gilt :

$$\text{Fit}_l(A) = \begin{cases} (c_1 \cdot \dots \cdot c_l) & , \text{ falls } 1 \leq l \leq r \\ (0) & , \text{ falls } r < l \leq \min\{m, n\} \end{cases}$$

Insbesondere gilt:  $\text{Fit}_r(A) \subseteq \text{Fit}_{r-1}(A) \subseteq \dots \subseteq \text{Fit}_1(A)$

*Beweis.* • Für  $l > r$  erhält jede  $l \times l$ -Untermatrix von  $A$  stets eine Nullzeile, d.h.  $\text{Fit}_l(A) = (0)$

•  $l \leq r$ : Die einzigen  $l \times l$ -Untermatrizen von  $A$ , die keine Nullzeile/-spalte enthalten, sind von der Form

$$\begin{pmatrix} c_{i_1} & & 0 \\ & \ddots & \\ 0 & & c_{i_l} \end{pmatrix}$$

mit  $1 \leq i_1 < i_2 < \dots < i_l \leq r$

$$\implies \text{Fit}_l(A) = (c_{i_1} \cdot \dots \cdot c_{i_l}) | 1 \leq i_1 < i_2 < \dots < i_l \leq r$$

$$\implies (c_1 \cdot \dots \cdot c_l) \subseteq \text{Fit}_l(A)$$

Umgekehrt folgt wegen  $1 \leq i_1 < i_2 < \dots < i_l \leq r : i_1 \geq 1, i_2 \geq 2, \dots, i_l \geq l$

$$\implies c_1 | c_{i_1}, \dots, c_l | c_{i_l} \implies c_1 \cdot \dots \cdot c_l | c_{i_1} \cdot \dots \cdot c_{i_l} \implies (c_{i_1} \cdot \dots \cdot c_{i_l}) \subseteq (c_1 \cdot \dots \cdot c_l)$$

$$\implies \text{Fit}_l(A) \subseteq (c_1 \cdot \dots \cdot c_l)$$

□

**Satz 3.14** (Elementarteilersatz über euklidischen Ringen). Sei  $R$  ein euklidischer Ring,  $A \in M_{m,n}(R)$ . Dann existieren  $c_1, \dots, c_r \in R \setminus \{0\}$  mit  $c_1 | c_2 | \dots | c_r$ , so dass

$$A \sim \left( \begin{array}{ccc|c} c_1 & & & 0 \\ & c_2 & & \vdots \\ & & \ddots & \\ & & & c_r \\ \hline 0 & \dots & 0 & 0 \end{array} \right)$$

$r$  ist eindeutig bestimmt,  $c_1, \dots, c_r$  sind eindeutig bestimmt bis auf Assoziiertheit.  $c_1, \dots, c_r$  heißen **Elementarteiler von A**

*Beweis.* 1. Existenz aus 3.12

2. Eindeutigkeit von  $r$ : Sei

$$A \sim \left( \begin{array}{ccc|c} c_1 & & & 0 \\ & c_2 & & \vdots \\ & & \ddots & \\ & & & c_r \\ \hline 0 & \dots & 0 & 0 \end{array} \right)$$

und

$$A \sim \left( \begin{array}{ccc|c} d_1 & & & 0 \\ & d_2 & & \vdots \\ & & \ddots & \\ & & & d_s \\ \hline 0 & \dots & 0 & 0 \end{array} \right)$$

mit  $c_1, \dots, c_r, d_1, \dots, d_s \in R \setminus \{0\}$  mit  $c_1 | c_2 | \dots | c_r, d_1 | d_2, \dots, | d_s$ ,

$$\xrightarrow[3.17]{3.16} \text{Fit}_l(A) = \begin{cases} (c_1 \cdot \dots \cdot c_l) & l \leq r \\ (0) & \text{sonst} \end{cases} = \begin{cases} (d_1 \cdot \dots \cdot d_l) & \\ (0) & \text{sonst} \end{cases}$$

für alle  $l \in \{1, \dots, \min\{m, n\}\}$

$$\implies r = \max\{l \in \{1, \dots, \min\{m, n\}\} | \text{Fit}_l(A) \neq (0)\} = s$$

3.  $c_l \hat{=} d_l$  für  $l = 1, \dots, r$  per Induktion nach  $l$ :

- IA:  $\text{Fit}_1(A) = (c_1) = (d_1) \xrightarrow{2.3} c_1 \hat{=} d_1$

- IS:  $\text{Fit}_l(A) = (c_1 \cdot \dots \cdot c_l) = (d_1 \cdot \dots \cdot d_l) \implies c_1 \cdot \dots \cdot c_l \hat{=} d_1 \cdot \dots \cdot d_l$ , außerdem ist nach IV.

$$c_1 \hat{=} d_1, \dots, c_{l-1} \hat{=} d_{l-1} \implies c_1 \cdot \dots \cdot c_l = \underbrace{d_1 \cdot \dots \cdot d_{l-1}}_{c_1 \cdot \dots \cdot c_{l-1} f \text{ für ein } f \in R^\times} d_l \cdot e \text{ für ein } e \in R^\times$$

$$\implies \underbrace{c_1 \cdot \dots \cdot c_{l-1}}_{\neq 0} (c_l - d_l e f) = 0 \implies c_l = d_l e f \implies c_l \hat{=} d_l$$

□

**Satz 3.15.** Sei  $R$  ein euklidischer Ring,  $A, B \in M_{m,n}(R)$ . Dann sind äquivalent:

- (i)  $A \sim B$
- (ii) Die Elementarteiler von  $A$  und  $B$  stimmen bis auf Assoziiertheit überein
- (iii)  $\text{Fit}_l(A) = \text{Fit}_l(B)$  für alle  $1 \leq l \leq \min\{m, n\}$

*Beweis.* • (i)  $\implies$  (iii): aus 3.16

- (iii)  $\implies$  (ii): Seien  $c_1, \dots, c_r, d_1, \dots, d_s$  die Elementarteiler von  $A$  bzw.  $B$ . Insbesondere

$$A \sim \left( \begin{array}{cccc|c} c_1 & & & & 0 \\ & c_2 & & & \vdots \\ & & \ddots & & \\ & & & c_r & 0 \\ \hline 0 & \dots & & 0 & 0 \end{array} \right)$$

und

$$B \sim \left( \begin{array}{cccc|c} d_1 & & & & 0 \\ & d_2 & & & \vdots \\ & & \ddots & & \\ & & & d_r & 0 \\ \hline 0 & \dots & & 0 & 0 \end{array} \right)$$

Argumentiere nun wie im Beweis von 3.18 in 2. und 3.

- (ii)  $\implies$  (i) Sei

$$A \sim \left( \begin{array}{cccc|c} c_1 & & & & 0 \\ & c_2 & & & \vdots \\ & & \ddots & & \\ & & & c_r & 0 \\ \hline 0 & \dots & & 0 & 0 \end{array} \right)$$

und

$$B \sim \left( \begin{array}{cccc|c} d_1 & & & & 0 \\ & d_2 & & & \vdots \\ & & \ddots & & \\ & & & d_r & 0 \\ \hline 0 & \dots & & 0 & 0 \end{array} \right)$$

mit  $c_1 \hat{=} d_1, \dots, c_r \hat{=} d_r$ , etwa  $d_1 = \lambda_1 c_1, \dots, d_r = \lambda_r c_r$  mit  $\lambda_1, \dots, \lambda_r \in R^\times$

$$\begin{aligned} \Rightarrow \left( \begin{array}{cccc|c} d_1 & & & & 0 \\ & d_2 & & & \vdots \\ & & \ddots & & \\ & & & d_r & 0 \\ \hline 0 & \dots & & 0 & 0 \end{array} \right) &= \left( \begin{array}{cccc|c} \lambda_1 c_1 & & & & 0 \\ & \lambda_2 c_2 & & & \vdots \\ & & \ddots & & \\ & & & \lambda_r c_r & 0 \\ \hline 0 & \dots & & 0 & 0 \end{array} \right) \\ &= \underbrace{\left( \begin{array}{cccc|c} \lambda_1 & & & & \\ & \ddots & & & \\ & & \lambda_r & & \\ & & & 1 & \\ & & & & \ddots \\ & & & & & 1 \end{array} \right)}_{\in \text{GL}(m, R)} \left( \begin{array}{cccc|c} c_1 & & & & 0 \\ & c_2 & & & \vdots \\ & & \ddots & & \\ & & & c_r & 0 \\ \hline 0 & \dots & & 0 & 0 \end{array} \right) \end{aligned}$$

$$A \sim \left( \begin{array}{cccc|c} c_1 & & & & 0 \\ & c_2 & & & \vdots \\ & & \ddots & & \\ & & & c_r & 0 \\ \hline 0 & \dots & & 0 & 0 \end{array} \right) \sim \left( \begin{array}{cccc|c} d_1 & & & & 0 \\ & d_2 & & & \vdots \\ & & \ddots & & \\ & & & d_r & 0 \\ \hline 0 & \dots & & 0 & 0 \end{array} \right) \sim B$$

□

**Anmerkung.** Satz 3.19 beinhaltet Insbesondere den Fall, das  $R = K$  ein Körper ist. Die Elementarteiler von  $A \in M_{m,n}(K)$  sind bis auf Assoziiertheit:  $\underbrace{1, \dots, 1}_{r \text{ Stück}}, 0, \dots, 0$  (mit  $r = \text{Rang } A$ ). D.h.

$$A \sim B \Leftrightarrow \text{Rang } A = \text{Rang } B$$

**Beispiel 3.16.**

$$A = \begin{pmatrix} 6 & -2 \\ -2 & 2 \end{pmatrix}, B = \begin{pmatrix} 4 & 8 \\ 4 & 6 \end{pmatrix} \in M_{2,2}(\mathbb{Z})$$

$$\text{Fit}_1(A) = (6, -2, -2, 2) = (2),$$

$$\text{Fit}_2(A) = (\det A) = (8)$$

$$\text{Fit}_1(B) = (4, 8, 4, 6) = (2)$$

$$\text{Fit}_2(B) = (\det B) = (-8) = (8)$$

$\Rightarrow A \sim B$  Es ist  $(c_1) = \text{Fit}_1(A), (c_1, c_2) = \text{Fit}_2(A) = (8) = (2)$  D.h.:  $c_1 = 2, c_2 = 4$  sind Elementarteiler von  $A$  (bzw. von  $B$ ), Insbesondere sind

$$A, B \sim \begin{pmatrix} 2 & 0 \\ 0 & 4 \end{pmatrix}$$

## Teil III

# Normalformen und Endomorphismen

**Frage.** Sei  $K$  ein Körper,  $V$  euklidischer  $K$ -VR und  $\varphi \in \text{End}(V)$ . Wie einfach kann man  $M_B(\varphi)$  bekommen durch geeignete Wahl einer Basis  $B$ ? In Termen von MAtrixen: Suche möglichst einfache Vertreter der Äquivalenzklassen bezüglich " $\approx$ ".



## 4 Invarianten-und Determinantenteiler

**Notation 1.** In diesem Abschnitt sei  $K$  stets ein Körper und  $n \in \mathbb{N}$ .

**Frage.** Seien  $A, B \in M_{n,n}(K)$ . Wann ist  $A \approx B$ ?

**Definition 4.1.** Sei  $A \in M_{n,n}(K)$ .

$P_A := tE_n - A \in M_{n,n}(K[t])$  heißt die **charakteristische Matrix** von  $A$

**Anmerkung.** Insbesondere ist  $\chi_A^{\text{char}} = \det(P_A)$ . Hierbei bezeichnet  $\chi_A^{\text{char}}$  das charakteristische Polynom von  $A$ .

**Satz 4.2** (Satz von Frobenius). Seien  $A, b \in M_{n,n}(K)$ . Dann sind äquivalent:

- (i)  $A \approx B$  (in  $M_{n,n}(K)$ )
- (ii)  $P_A \sim P_B$  (in  $M_{n,n}(K[t])$ )

*Beweis.* (i)  $\implies$  (ii): Sei  $A \approx B \implies$  Es existiert ein  $S \in \text{GL}_n(K)$  mit  $B = SAS^{-1}$

$$\implies P_B = tE_n - B = tE_n - SAS^{-1} = StE_nS^{-1} - SAS^{-1} = S \underbrace{tE_n - A}_{P_A} S^{-1}$$

$$\implies P_B \approx P_A \implies P_B \sim P_A$$

(ii)  $\implies$  (i): Sei  $P_A \sim P_B$ .

(a) Wir konstruieren  $R \in M_{n,n}(K)$  mit  $AR = RB$ . Nach Voraussetzung existieren  $S, T \in \text{GL}_n(K[t])$  mit  $P_A = SP_B T^{-1}$ , d.h.  $SP_B = P_A T$

$$\implies S(tE_n - B) = (tE_n - A)T(*)$$

Wir schreiben  $S, T$  in der folgenden Form:

$$S = \sum_{i=0}^m t^i S_i, T = \sum_{i=0}^m t^i T_i \quad \text{mit } S_i, T_i \in M_{n,n}(K)$$

$$\begin{aligned}
 \implies S(tE_n - B) &= \sum_{i=0}^m t^i S_i (zE_n - B) \\
 &= \sum_{i=0}^m (t^{i+1} S_i - t^i S_i B) \\
 &= \sum_{i=1}^{m+1} t^i S_{i-1} - \sum_{i=0}^m t^i S_i B \\
 &= \sum_{i=0}^{m+1} (S_{i-1} - S_i B) t^i \text{ mit } S_{i-1}, S_{m+1} := 0. \\
 (tE_n - B) &= (tE_n - A) \sum_{i=0}^m t^i T_i \\
 &= \sum_{i=0}^m i = 0^m (t^{i+1} T_i - t^i A T_i) \\
 &= \sum_{i=0}^{m+1} (T_{i-1} - A T_i) t^i \\
 &\stackrel{(*)}{\implies} \sum_{i=0}^{m+1} (S_{i-1} - S_i B) t^i = \sum_{i=0}^{m+1} (T_{i-1} - A T_i) z^i \\
 &\implies S_{i-1} - S_i B = T_{i-1} A T_i \text{ für } 0 \leq i \leq m+1 \\
 &\implies A_i S_{i-1} - A^i S_i B = A^i T_{i-1} - A^{i+1} T_i \text{ für } 0 \leq i \leq m+1 \\
 \implies \sum_{i=0}^{m+1} (A^i S_{i-1} - A^i S_i B) &= \sum_{i=0}^{m+1} (A^i T_{i-1} - A^{i+1} T_i) \\
 &= (A T_{i-1} - A T_0) + (A T_0 - A^2 T_1) \\
 &\quad + \dots + (A^{m+1} T_m - A^{m+2} T_{m+1}) \\
 &= A T_{i-1} - A^{m+2} T_{m+1} = 0. \\
 \implies \sum_{i=0}^{m+1} A^i S_{i-1} &= \sum_{i=0}^{m+1} A^i S_i B \\
 \stackrel{S_{m+1}=0}{\stackrel{S_{-1}=0}{\implies}} \sum_{i=0}^{m+1} A^i S_{i-1} &= \sum_{i=0}^m A^i S_i B \\
 \implies A \left( \sum_{i=0}^m A^i S_i \right) &= \left( \sum_{i=0}^m A^i S_i \right) B
 \end{aligned}$$

Setze  $R := \sum_{i=0}^m A^i S_i$ , dann  $AR = RB$ .

(b) Wir zeigen:  $R \in \text{GL}_n(K)$  (wegen  $AR = RB$  folgt dann  $A = RBR^{-1}$ , also  $A \approx B$ , fertig.) Nach Voraussetzung ist  $S \in \text{GL}_n(K[t])$ .

Es existiert  $M \in \text{GL}_n(K[t])$  mit  $SM = E_n$ ,  $M = \sum_{i=0}^m t^i M_i$  mit  $M_i \in \text{M}_{n,n}(K)$ ,

ohne Einschränkung  $m$  wie vorhin.

Behauptung: Mit  $N := \sum_{j=0}^m RB^j M_j \in \text{M}_{n,n}(K)$  gilt  $RN = E_n$ , d.h.  $N \in \text{GL}_n(K)$

denn: Es ist  $RN = \sum_{j=0}^m RB^j M_j$ . Wegen  $RB \stackrel{1}{=} AR$  folgt  $RB^j = RBB^{j-1} = ARB^{j-1} = \dots = A^j R$

$$\implies RN = \sum_{j=0}^m A_j R M_j = \sum_{j=0}^m A^j \left( \sum_{i=0}^m A^i S_i \right) M_j = \sum_{i,j=0}^m A^{i+j} S_i M_j$$

$$\begin{aligned}
 & \text{Wegen } SM = E_n \text{ folgt } \left( \sum_{i=0}^m t^i S_i \right) \left( \sum_{j=0}^m t^j M_j \right) = E_n. \\
 & S_0 M_0 + \sum_{k=0}^m \left( \sum_{i+j=k} S_i M_j \right) t^k = E_n \\
 & \xRightarrow{\text{Koeffizientenvergleich}} S_0 M_0 = E_n, \sum_{i+j=k} S_i M_j = 0 \text{ für } k \geq 1. \\
 & \Rightarrow RN = \sum_{i,j=0}^m A^{i+j} S_i M_j = S_0 M_0 + \sum_{k=1}^{2m} A^k \underbrace{\sum_{i+j=k} S_i M_j}_{=0} = E_n \\
 & \Rightarrow \text{Behauptung.}
 \end{aligned}$$

□

**Bemerkung 4.3.** Sei  $A \in M_{n,n}(K)$ . Dann gilt:

(a) Es gibt bestimmte normierte Polynome  $c_1(A), \dots, c_n(A) \in K[t]$  mit

$$P_A \sim \begin{pmatrix} c_1(A) & & 0 \\ & \ddots & \\ 0 & & c_n(A) \end{pmatrix}$$

mit  $c_1(A)|c_2(A)|\dots|c_n(A)$ .  $c_1(A), \dots, c_n(A)$  heißen die **Invariantenteiler** von  $A$ .

(b) Es gibt eindeutig bestimmte normierte Polynome  $d_1(A), \dots, d_n(A) \in K[t]$  mit

$$\text{Fit}_l(P_A) = (d_l(A)) \text{ für } l = 1, \dots, n$$

Es ist  $d_l(A) = \text{ggT}(\det(B) \mid B \text{ ist } l \times l\text{-Untermatrix von } P_A)$ . Insbesondere ist  $D_n(A) = \chi_A^{\text{char}}$ .  $d_1(A), \dots, d_n(A)$  heißen die **Determinantenteiler** von  $A$ .

*Beweis.* (a)  $K[t]$  ist ein Euklidischer Ring (Bsp. 3.2).

$\xRightarrow{\text{Satz 3.18}}$  Es existieren  $\tilde{c}_1, \dots, \tilde{c}_r \in K[t] \setminus \{0\}$  mit

$$P_A \sim \begin{pmatrix} \tilde{c}_1 & & & \\ & \ddots & & \\ & & \tilde{c}_r & \\ & & & 0 \\ & & & & \ddots \\ & & & & & 0 \end{pmatrix}$$

mit  $\tilde{c}_1|\dots|\tilde{c}_r$ . Es ist  $\text{Fit}_n(P_A) = (\det P_A) = (\chi_A^{\text{char}}) \neq (0) \Rightarrow r = n$  und  $\text{Fit} : n(P_A) \stackrel{3.16}{=} (\tilde{c}_1 \cdot \dots \cdot \tilde{c}_n)$ . Wegen  $\tilde{c}_i \neq 0$  für  $i = 1, \dots, n$  existieren normierte Polynome  $c_i(A), i = 1, \dots, n$  mit  $c_i(A) \hat{=} \tilde{c}_i$ .

$$\Rightarrow P_A \sim \begin{pmatrix} c_1(A) & & 0 \\ & \ddots & \\ 0 & & c_n(A) \end{pmatrix}.$$

Eindeutigkeit:  $c'_1(A), \dots, c'_n(A) \in K[t]$  normiert mit  $c'_1(A)|c'_2(A)|\dots|c'_n(A)$  und

$$P_A \sim \begin{pmatrix} c'_1(A) & & \\ & \ddots & \\ & & c'_n(A) \end{pmatrix}$$

$$\Rightarrow c'_i(A) \subseteq c_i(A) \text{ für } i = 1, \dots, n \xRightarrow{c_i(A), c'_i(A) \text{ normiert}} c'_i(A) = c_i(A) \text{ für } i = 1, \dots, n$$

(b)  $K[t]$  HIR nach Satz 3.3  $\Rightarrow \text{Fit}_l(P_A), l = 1, \dots, n$  sind Hauptideale und nach 3.16, 3.17 ist  $\text{Fit}_l(P_A) = (c_1(A) \cdot \dots \cdot c_l(A))$  für  $l = 1, \dots, n$ , insbesondere ist  $\text{Fit}_l(P_A) \neq 0$ . Erzeuger

der Hauptidealringe  $\text{Fit}_l(P_A)$  sind eindeutig bis auf Assoziiertheit (2.3)  $\implies$  Es existieren eindeutig bestimmte Polynome  $d_1(A), \dots, d_n(A) \in K[t]$  mit  $\text{Fit}_l(P_A) = (d_l(A))$  für  $l = 1, \dots, n$ . Es ist

$$\begin{aligned} \text{Fit}_l(P_A) &= (\det(B) | B \text{ ist } l \times l\text{-Untermatrix von } P_A) \\ &\stackrel{2.5}{=} (\text{ggT}(\det(B) | B \text{ ist } l \times l\text{-Untermatrix von } P_A)) \\ &= d_l(A) \\ &\stackrel{d_l \text{ normiert}}{\text{ggT normiert}} d_l(A) = \text{ggT}(\dots). \end{aligned}$$

□

**Anmerkung.** Also:

Invariantenteiler von  $A$  = normierte Elementarteiler von  $P_A$   
 Determinantenteiler von  $A$  = normierten Erzeuger der Fittingideale von  $P_A$

**Folgerung.** Sei  $A \in M_{n,n}(K)$ .

Dann gilt:

$$d_l(A) = c_1(A) \cdot \dots \cdot c_l(A) \text{ für } l = 1, \dots, n$$

Insbesondere gilt

$$\chi_A^{\text{char}} = d_n(A) \cdot \dots \cdot c_n(A)$$

sowie

$$d_1(A) | \dots | d_n(A), \\ \text{Fit}_n(P_A) \subseteq \text{Fit}_{n-1}(P_A) \subseteq \dots \subseteq \text{Fit}_1(P_A)$$

**Satz 4.4** (Invariantenteilersatz). Seien  $A, B \in M_{n,n}(K)$ . Dann sind äquivalent:

- (a)  $A \approx B$
- (b) Die Invariantenteiler von  $A$  stimmen mit den Invarianten von  $B$  überein:

$$c_1(A) = c_1(B), \dots, c_n(A) = c_n(B)$$

- (c) Die Determinantenteiler von  $A$  stimmen mit den Determinantenteilen von  $B$  überein:

$$d_1(A) = d_1(B), \dots, d_n(A) = d_n(B)$$

*Beweis.* Folgt aus Satz von Frobenius und Satz 4.3

□

**Beispiel 4.5.** Sei

$$A = \begin{pmatrix} 0 & 1 & 3 \\ 3 & 1 & -4 \\ -2 & 1 & 5 \end{pmatrix} \in M_{3,3}(\mathbb{Q})$$

Es ist

$$P_A = \begin{pmatrix} t & -1 & -3 \\ -3 & t-1 & 4 \\ 2 & -1 & t-5 \end{pmatrix} \in M_{3,3}(\mathbb{Q}[t])$$

Bestimmen der Determinantenteiler von  $A$ :

$$\begin{aligned}
 d_1(A) &= \text{ggT}(-1, \dots) = 1 \\
 d_2(A) &= \text{ggT}((-1) \cdot 4 - (-3)(t-1), (-3)(-1) - 2(t-1), \dots) \\
 &= \text{ggT}(\underbrace{3t-7, -2t+5, \dots}_{\text{teilerfremd}}) = 1 \\
 d_3(A) &= \chi_A^{\text{char}} = \dots = (t-2)^3 \\
 \implies c_1(A) &= 1, c_2(A) = 1, c_3(A) = (t-2)^3
 \end{aligned}$$

Sei

$$B = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 1 & -2 \\ -1 & 1 & 4 \end{pmatrix} \in M_{3,3}(\mathbb{Q}) \implies P_B = \begin{pmatrix} t-1 & -1 & -2 \\ -1 & t-1 & 2 \\ 1 & -1 & t-4 \end{pmatrix}$$

Bestimmen der Invariantenteiler von  $B$ :

$$\begin{aligned}
 P_B &= \begin{pmatrix} t-1 & -1 & -2 \\ -1 & t-1 & 2 \\ 1 & -1 & t-4 \end{pmatrix} \begin{matrix} \swarrow \\ \swarrow \end{matrix} \sim \begin{pmatrix} -1 & t-1 & 2 \\ t-1 & -1 & -2 \\ 1 & -1 & t-4 \end{pmatrix} \begin{matrix} | \text{II} + (t-1)\text{I} \\ | \text{III} + \text{I} \end{matrix} \\
 &\sim \begin{pmatrix} -1 & t-1 & 2 \\ 0 & (t-1)^2 - 1 & 2(t-1) - 2 \\ 0 & t-2 & t-2 \end{pmatrix} \sim \begin{pmatrix} -1 & 0 & 0 \\ 0 & t^2 - 2t & 2t - 4 \\ 0 & t-2 & t-2 \end{pmatrix} \begin{matrix} \swarrow \\ \swarrow \end{matrix} \\
 &\sim \begin{pmatrix} -1 & 0 & 0 \\ 0 & t^2 & t-2 \\ 0 & t^2 - 2t & 2t - 4 \end{pmatrix} \stackrel{3. \text{ SP-2.SP}}{\sim} \begin{pmatrix} -1 & 0 & 0 \\ 0 & t^2 & 0 \\ 0 & t^2 - 2t & -t^2 + 4t - 4 \end{pmatrix} \\
 &\sim \begin{pmatrix} -1 & 0 & 0 \\ 0 & t^2 & 0 \\ 0 & 0 & -(t-2)^2 \end{pmatrix} \sim \begin{pmatrix} -1 & 0 & 0 \\ 0 & t^2 & 0 \\ 0 & 0 & (t-2)^2 \end{pmatrix}
 \end{aligned}$$

$$\begin{aligned}
 \implies c_1(B) &= 1, c_2(B) = t-2, c_3(B) = (t-2)^2 \\
 d_1(B) &= 1, d_2(B) = c_1(B)c_2(B) = t-2, \\
 d_3(B) &= c_1(B)c_2(B)c_3(B) = (t-2)^3 - \chi_{\text{char}}^B
 \end{aligned}$$

Also  $A \not\approx B$ .

**Bemerkung 4.6.** Seien  $A, B \in M_{n,n}(K)$ ,  $K$  Teilkörper eines Körpers  $L$ . Dann sind äquivalent:

- (i)  $A \approx B$  in  $M_{n,n}(K)$
- (ii)  $A \approx B$  in  $M_{n,n}(L)$

*Beweis.* Übung. □