# Lineare Algebra II Skript

Prof. Vogel

20. Mai 2020

# Inhaltsverzeichnis

## 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.** $h : V \times V \longrightarrow$ heißt eine **Sesquilinerform** auf $V$
$\overset{\text{Def}}{:\Leftrightarrow}$

(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.

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

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

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

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

$$\begin{gathered}(x_1 + x_2)^t y = x_1^t y + x_2^t y,\\ (\lambda x)^t y = \lambda(x^t y),\\ x^t(\overline{y_1 + y_2}) = x^t\overline{y_1} + x^t\overline{y_2},\\ x^t\overline{\lambda y} = \overline{\lambda} x^t y.\\ \text{für } x_1, x_2, y, y_1, y_2 \in \mathbb{C}^n.\end{gathered}$$

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

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

**Definition 0.3.** Sei $V$ ein $\mathbb{C}$-VR, $h$ Sesquilinearform auf $V$. $h$ heißt **hermitisch** $\overset{\text{Def:}}{\Leftrightarrow}$ $h(w, v) = \overline{h(v, w)}$ 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.** $h(x, y) = x^t\overline{y}$ aus Bsp. 0.2 ist hermitesch, denn es ist $h(y, x) = \underbrace{y^t\overline{x}}_{\in\mathbb{C}} = (y^t\overline{x})^t = \overline{x}^t(y^t)^t = \overline{x}^t y = x^t\overline{y} = \overline{h(x, y)}$.

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

**Definition 0.5.** Sei $h : V \times V \longrightarrow \mathbb{C}$ eine Sesquilinearform, $B = (v_1, ..., v_n)$ 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 $h(x, y) = x^t\overline{y}$ 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** $\overset{\text{Def:}}{\Leftrightarrow} M = M^*$

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

**Satz 0.8.** Sei $B = (v_1, ..., v_n)$ eine Basis von $V$.
Sesq(V) $:= \{h : V \times V \longrightarrow \mathbb{C} | h$ ist Sesquilinearform$\}$ ist ein $\mathbb{C}$-VR. (UVR von $\mathbb{C}$-VR Abb$(V \times V, \mathbb{C})$. Die Abbildung

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

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

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

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

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 $A = (a_{ij}) \in M_{n,n}(\mathbb{C}) \Rightarrow h_B(A)(v_i, v_j) = e_i^t A\overline{e_j} = a_{ij}$, d.h. Darstellungsmatrix von $h_B(A)$ bzgl. $B$ ist $A$.
- $h_B \circ M_B = id$, denn: Sei $h \in \mathrm{Sesq}(V) \Longrightarrow h_B(M_B(h))(v_i, v_j) = e_i^t M_B(h)\overline{e_j} = h(v_i, v_j) \Longrightarrow h_b(M_B(h)) = h$. Für $h \in \mathrm{Sesq}(V)$ ist

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

□

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

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

*Beweis.* analog zum reellen Fall □

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

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

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

**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

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

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 $(v_1, .., v_n)$ eine Basis von $V$. $(v_1, \ldots, v_n)$ heißt eine

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

**Orthonormalbasis** von V $\overset{\text{Def:}}{\Leftrightarrow} h(v_i, v_j) = \delta_{ij}$ 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 $\phi : V \longrightarrow \mathbb{C}, w \mapsto h(w, v_1)$ ist Linearform mit $\ker \phi = H$

$\Rightarrow \dim H = \dim \ker \phi = \dim V - \underbrace{\dim \operatorname{im} \phi}_{\in\{0,1\}} \in \{n, n-1\}$.

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 $(v_2, .., v_n)$

$\Rightarrow (v_1, v_2, ..., v_n)$ 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. $U^\perp = \{v \in V | h(v, u) = 0$ 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 $(u_1, ..., u_m)$ ONB von $U$.

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

Für $i = 1, ..., m$ 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, $\varphi : V \longrightarrow W$ 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 $\varphi \in \mathrm{End}(V)$ 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, $B = (v_1, ..., v_n)$ ONB von $(V,h)$. Dann ist die Abbildung

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

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

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

(i) $A$ ist unitär

(ii) Die Abbildung $(\mathbb{C}^n, \langle\cdot,\cdot\rangle) \longrightarrow (\mathbb{C}^n, \langle\cdot,\cdot\rangle), x \mapsto Ax$ ist unitär. Hierbei ist $\langle\cdot,\cdot\rangle$ das Standartskalarprodukt.

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

Somit ist die Abbildung aus (ii) unitär
$\Leftrightarrow x^tA^t\overline{A}\overline{y} = \langle x,y\rangle = x^t\overline{y}$ für alle $x, y \in \mathbb{C}^n$
$\Leftrightarrow h_{(e_1,...,e_n)}(A^t, \overline{A}) = h_{(e_1,...,e_n)}(E_n)$ (vgl. Satz 0.7 )
$\overset{0.7}{=} A^tA = E_n \Leftrightarrow \overline{A}^t(A^t)^t = E_n \Leftrightarrow \overline{A}^tA = A^*A = E_n \Leftrightarrow A$ ist unitär

□

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

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

$f^*$ 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, $f \in \mathrm{End}(V), A \in M_{n,n}(\mathbb{C})$.

- $f$ heißt **selbstadjungiert** $\overset{\text{Def:}}{\Leftrightarrow} f^* = f$
- $f$ heißt **normal** $\overset{\text{Def:}}{\Leftrightarrow} f^* \circ f = f \circ f^*$
- $A$ heißt **selbstadjungiert** $\overset{\text{Def:}}{\Leftrightarrow} A^* = A$
- $A$ heißt **normal** $\overset{\text{Def:}}{\Leftrightarrow} A^*A = AA^*$

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

**Bemerkung 0.25.** Sei $(V, h)$ ein unitärer Raum, $f \in \mathrm{End}(V)$. 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 $v, w \in V$

$$\underset{f \text{ Isomorphismus, da unitär}}{\Rightarrow} h(v, f^{-1}(w)) \underset{\text{f unitär}}{=} h(f(v), f(f^{-1}(w))) = h(f(v), w)$$
$$\underset{0.23}{\Rightarrow} f^* = f^{-1} \Rightarrow f^* \circ f = f^{-1} \circ f = id_V = f \circ f^{-1} = f \circ f^*$$

(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, $f \in \mathrm{End}(V)$. 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 $\overline{\lambda}$

(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 $g := \lambda id_V - f$

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

(a) Beh.: $g^* = \overline{\lambda} id_V - f^*$

denn: $h((\lambda id_V - f)(x), y) = \lambda h(, y) - h(f(x), y) = h(x, \overline{\lambda} y) - h(x, f^*(y))$
$h(x, \overline{\lambda} y - f^*(y)) = h(x, (\overline{\lambda} id_V - f^*(y)))$ für alle $x, y \in V$

(b) Beh.: $g^* \circ g = g \circ g^*$, d.h. $g$ ist normal denn: $g \circ g^* = (\lambda id_V - f) \circ (\overline{\lambda} id_V - f^) * f \circ f^* = f^* \circ f \underset{f \text{ normal}}{=} (\overline{\lambda} id_V - f^* \circ (\lambda id_V - f)) = g^* \circ g$

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

Dann: $v$ Eigenvektor zum Eigenwert $\lambda$ von $f$

$v$ Eigenvektoren zum Eigenwert $\overline{\lambda} v$

(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 $\overline{\lambda}$ von $f^* = f \Rightarrow \lambda = \overline{\lambda} \Rightarrow \lambda \in \mathbb{R}$

□

**Satz 0.27** (Spektralsatz für normale Operatoren)**.** Sei $(V, h)$ ein unitärer Raum, $f \in \mathrm{End}(V)$ normal. Dann exisitiert 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 $f^*(v) = \overline{\lambda}v$, also $f^*(L) \subset L \overset{0.26(a)}{\Rightarrow} \underbrace{(f^*)^*}_{=f} L^\perp \subset L^\perp \Rightarrow f$ induziert einen normalen Endimorphismus des unitären Raums $(L^\perp, h\mid_{L^\perp \times L^\perp})$ Nach Induktionsvorraussetzung existiert eine ONB $(v_2, ..., v_n)$ von $L^\perp$ aus Eigenvektoren zu $f\mid_{L^\perp} \Rightarrow (v, v_2, ..., v_n)$ 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 $f$ exisitiert, 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 $(\mathbb{C}^n, \langle\cdot,\cdot\rangle) \longrightarrow (\mathbb{C}^n, \langle\cdot,\cdot\rangle), x \mapsto Ax$ an. (Basiswechselmatrix unitär, da ONB von Eigenvektoren). Erhalte $U \in$ 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

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

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 $R \overset{\text{Def.}}{\Leftrightarrow}$ 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 in $R$.

(b) Für $n \in \mathbb{Z}$ ist $nZ := \{na | a \in \mathbb{Z}\}$ 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

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

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

*Beweis.* Setze $R := \{a - \widetilde{q}b | \widetilde{q} \in \mathbb{Z}\} \cap \mathbb{N}_0 \implies R$ ist nichtleere Teilmenge von $N_0$, insbesondere besitzt $R$ kleinstes Element, etwa $r$. Sei $q \in \mathbb{Z}$ mit $a - qb = r \implies a = qb + r$ *Annahme*: $r \geq |b| \implies 0 \leq r - |b| = a - qb - \operatorname{sgn}(b)b = \underbrace{a - (q + \operatorname{sgn}(b))}_{\in R} b < r$ Das ist ein Widerspruch zur Minimalität von $r$. □

**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 $J \cap \mathbb{N} \neq \varnothing \implies J \cap \mathbb{N}$ 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 $x = \underbrace{nq}_{\in J} \overset{\text{J Ideal}}{\implies} x \in J$

  (ii) "$\subseteq$": Sei $x \in J \overset{\text{Division mit Rest}}{\implies}$ Es existieren $q, r \in \mathbb{Z}$ 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 $r = 0 \implies x = qn \in \mathbb{Z}$

□

**Definition 1.7.** Sei $\varphi : R \longrightarrow S$ eine Abbildung. $\varphi$ heißt ein **Ringhomomorphismus** $\overset{\text{Def:}}{\implies}$ Die folgenen 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) $J \subseteq S$ Ideal $\implies (\varphi)^{-1}(J) \subseteq R$ Ideal

(b) $\ker \varphi := \{a \in R | \varphi(a) = 0\} \subseteq R$ Ideal

(c) $\varphi$ injektiv $\Leftrightarrow \ker \varphi = \{0\}$

(d) $J \subseteq R$ Ideal und $\varphi$ surjektiv $\implies \varphi(S) \subseteq S$ Ideal

(e) $\operatorname{im} \varphi := \varphi(R)$ 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) $a, b \in \varphi^{-1}(J) \implies \varphi(a), \varphi(b) \in J \overset{\text{J Ideal}}{\implies} \underbrace{\varphi(a) + \varphi(b)}_{=\varphi(a+b)} \in J \implies a + b \in \varphi^{-1}(J)$

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

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

(c) nachrechnen

(d) nachrechnen

(e) nachrechnen

□

**Anmerkung.** (d) wird falsch, wenn man die Vorraussetzung $\varphi$ surjektiv weglässt. Die kanonische Inklusion $i.\mathbb{Z} \longrightarrow \mathbb{Q}, x \longmapsto x$ 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 $r_1 \sim r_2 \overset{\text{Def:}}{\Leftrightarrow} r_1 - r_2 \in J$ 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

$$\overline{r} := r + J := \{r + a | a \in J\}$$

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

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

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

(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

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

und der Multipikation

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

zu einem Ring, dem **Faktorring (Restklassenring)** $R/J$. Die Abbildung $\pi : R \longrightarrow R/J, r \mapsto \overline{r}$ 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: $\pi(a + b) = \overline{a + b} = \overline{a} + \overline{b} = \pi(a) + \pi(b)$, analog für $\cdot$, $\pi(1) = \overline{1}$
- $\pi$ ist surjektiv nach Konstruktion
- $\ker \pi = \{r \in R | \overline{r} = \overline{0}\} = \{r \in R | r \sim 0\} = \{r \in R | r - 0 \in J\} = J$

□

**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: $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, ..., \overline{n-1}\}$ mit den Verknüpfungen $\overline{a} + \overline{b} := \overline{a + b}, \overline{a} \cdot \overline{b} = \overline{a \cdot b}$.

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

$$\phi : R/\ker\varphi \longrightarrow \operatorname{im}\varphi, \overline{r} = r + \ker\varphi \mapsto \varphi(r).$$

*Beweis.*

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

□

**Beispiel 1.13.** Seien $K$ ein Körper, $R = K[t]$, $\varphi : K[t] \longrightarrow K, f \mapsto f(0)$. $\varphi$ ist ein Ringhomomorphismus, $\operatorname{im}\varphi = K, \ker\varphi = \{f \in K[t] | f(0) = 0\} = \{tg | g \in K[t]\} = tK[t]$. 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 , $\pi : R \longrightarrow R/J$ die kanonische Projektion. Dann sind die Abbildungen

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

zueienander inverse, inklusionserhaltende Abbildungen.

*Beweis. Übung* □

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

**Anmerkung.**

- vgl. LA1 Lemma 1.11
- $R$ ist Körper $\Leftrightarrow R^\times = R \setminus \{0\}$
- 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 $\varphi : R \longrightarrow S$ in einen Ringhomomorphismus $S \neq 0$ ist injektiv

*Beweis.*

- (i) $\implies$ (ii) Sei $R$ ein Körper. Sei $J \subseteq R$ ein Ieal, $J \neq \{0\}$. Es exisitiert ein $a \in J, a \neq 0 \implies 1 = \underbrace{a}_{\in J} a^{-1} \in J \implies$ ist $b \in R$, dann ist $b = b \cdot \underbrace{1}_{\in J} \in J$, d.h. $J = R$
- (ii) $\implies$ (iii) Sei $\varphi : R \longrightarrow S$ 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. $S = 0$ *Widerspuch*) $\implies \ker \varphi = \{0\}$, d.h. $\varphi$ ist injektiv.
- (iii) $\implies$ (i) Sei $a \in R \backslash R^\times$, insbesondere existiert kein $b \in R$ mit $ab = 1_R \implies aR := \{ar | r \in R\} \subsetneq R$, und $aR$ ist ein Ideal in $R$. $\implies R/aR$ ist nicht der Nullring (denn: Wenn $R/aR = 0$, dann $1_R + aR = 0_R + aR$, also $1 \in aR$ *Widerspruch*) $\overset{\text{(iii)}}{\implies}$ Die kankonische Projektion $\pi : R \longrightarrow S = R/aR$ ist injektiv, d.h. $\ker \pi = \{0\}$, anderer seits ist $\ker \pi = aR$ nach 1.10, also: $\underbrace{a \cdot 1_R}_{\in aR} = \{0\} \implies a = 0$, d.h. $R$ ist Körper.

□

**Definition 1.18.** $x \in R$ heißt **Nullteiler** $\overset{\text{Def:}}{\Leftrightarrow}$ 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.**

- $R \neq 0 \implies 0_R$ ist ein Nullteiler in $R$ (wegen $0_R \cdot 1_R = 0_R, 0_R \neq 1_R$)(Achtung: Unterschiedliche Notatio in Literatur)
- Im Nullring ist 0 kein Nullteiler (aber: Nullring ist nicht nullteilerfrei)

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

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

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

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

$$(a_1, ..., a_n) := \{\sum_{i=1}^{n} a_i r_i | r_1, ..., r_n \in R\} \subseteq R \text{ heißt das } \textbf{von } a_1, ..., a_n \textbf{ erzeugte Ideal}$$

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

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

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

**Beispiel 1.21.** (a) $K$ Körper $\Longrightarrow$ $K$ ist HIR (denn: $K$ Körper $\overset{1.17}{\Longrightarrow}$ $\{0\}, R$ sind dei 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 $z = hf \Longrightarrow \deg h = \deg f = 0$, d.h. $f$ ist konstant (?), etwa $f = a$ für ein $a \in \mathbb{Z}$. Außerdem existiert ein $\widetilde{h} \in \mathbb{Z}[t]$ mit $t = \widetilde{h}f = \widetilde{h}a \overset{\text{t normiert}}{\Longrightarrow} a = 1 \Longrightarrow f = 1$, aber: $1 \notin (2, t)$, denn anderenfalls existieren $u, v \in \mathbb{Z}[t]$ mit $1 = 2 \cdot u + t \cdot v \overset{t=0}{\Longrightarrow} 1 = 2 \cdot u(0) + 0 \cdot v(0) = 2 \cdot 1(0)$ *Widersrpuch* □

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

$$\textbf{Primideal} \overset{\text{Def:}}{\Leftrightarrow} J \neq R \text{ und für alle } x, y \in R \text{ gilt: } xy \in J \Longrightarrow x \in J \text{ oder } y \in J.$$

$$\textbf{maximales Ideal} \overset{\text{Def:}}{\Leftrightarrow} J \neq R \text{ und es existiert kein Ideal } I \subseteq R \text{ mit } J \subsetneq I \subsetneq R$$

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

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

(a) $J$ ist Primideal $\Leftrightarrow$ $R/J$ nullteilerfrei

(b) $J$ maximales Ideal $\Leftrightarrow$ $R/J$ Körper

*Beweis.* (a) Die Bedingung $xy \in J \Longrightarrow x \in J$ oder $y \in J$ ist äquivalent zu $\overline{x} \cdot \overline{y} = \overline{0} \Longrightarrow \overline{x} = \overline{0}$ oder $\overline{y} = \overline{0}$ 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.

□

**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) □

**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) $\implies$ (ii): Körper sind nullteilerfrei. LA 1; Lemma 1.15
- (ii) $\implies$ (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 $1 < a, b < n \implies \overline{0} = \overline{n} = \overline{a} \cdot \overline{b} \implies \mathbb{Z}/n\mathbb{Z}$ 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 bwnötigen wir ein Axiom aus der Mengenlehre, das **Auswahlaxiom**. Ist $I$ eine Menge und $(A_i)_{i \in J}$ ein Familie von nichtleeren Mengen, dann gibt es eine Abbildung

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

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 $M$.

- $$\begin{aligned} \sim \text{ heißt } \textbf{antisymmetrisch} &\overset{\text{Def:}}{\Leftrightarrow} \text{Für alle } a, b \in M \text{ gilt } : a \sim b \text{ und } b \sim a \implies a = b \\ \textbf{total} &\overset{\text{Def:}}{\Leftrightarrow} \text{Für alle } a, b \in M \text{ gilt } : a \sim b \text{ oder } b \sim a \end{aligned}$$
- $$\begin{aligned} \sim \text{ heißt } \textbf{Halbordnung} \text{ auf } M &\overset{\text{Def:}}{\Leftrightarrow} \sim \text{ reflexiv, antisymmetrisch und transitiv} \\ \textbf{Totalordnung} \text{ auf } M &\overset{\text{Def:}}{\Leftrightarrow} \sim \text{ ist eine Halbordnung und } \sim \text{ ist total} \end{aligned}$$

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 $M \overset{\text{Def:}}{\Leftrightarrow}$ Für alle $x \in M$ gilt $a \leq x \implies x = a$

**Anmerkung.** Für ein maximales Element $a \in M$ gilt nicht notwendig $x \leq a$ für $x \in M$. Im allgemeinen extisieren 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 $\{I \subsetneq R | I \text{ ist Ideal}\}$ bezüglich $\subseteq$.

**Definition 1.29.** Sei $(M, \leq)$ eine halbgeordnete Menge. $(M, \leq)$ heißt **induktiv geordnet** $\overset{\text{Def:}}{\Leftrightarrow}$ 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 := $\{I \subsetneq R | I \text{ Ideal}\}$

- X ist bzgl. $\subseteq$ halbgeordnet
- X $\neq \emptyset$ wegen $\{0\} \in$ X
- Sei $\{I_\lambda | \lambda \in 1\}$ totalgeordnete Teilmenge von X (d.h. für $\lambda, \mu \in 1 : I_\lambda \subseteq I_\mu$ oder $I_\mu \subseteq I_\lambda$) Behauptung: $\{I_\lambda | \lambda \in 1\}$ besitzt eine obere Schranke in X, d.h, es existiert ein $J \in$ X mit $I_\lambda \subseteq I$ 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) $a, b \in J \implies$ Es existiert $\lambda, \mu$ mit $a \in J_\lambda, b \in I_\mu$, 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) $a \in J, r \in R \implies$ Es existiert $\lambda \in 1$ mit $a \in I_\lambda \implies ra \in I_\lambda \subseteq I$
  2. $I \subsetneq R$, 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 $I \subsetneq R$ ist einem Ideal von $R$ enthalten.

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

*Beweis.* (a) $J \subsetneq R$ Ideal $\implies R/I \neq 0$, also besitzt $R/I$ ein maximales Ideal $\overset{1.14}{\implies}$ $R$ besitzt ein maximales Ideal, das $I$ enthält.

(b) Sei $x \in R \setminus R^\times \implies (x) \subsetneq R$, 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

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

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

und $I \cap J$ Ideale in $R$. Analog für endliche Familien von Idealen, insbsondere $I^n := \underbrace{I \cdot ... \cdot I}_{n\text{-mal}}$ für $n \in \mathbb{N}$. Konvention: $I^0 := R$. I,J heißen **relatix prim** $\overset{\text{Def:}}{\Leftrightarrow}$ $i + J = R = (1)$

**Anmerkung.**
- Das dies tatsächlich Ideale sind, rechnet man nach
- Offenbar ist Multiplikation bzw. Addition von Idealen assoziaztiv, Klammerung ist nicht notwendig
- $(a_1, ..., a_n) = (a_1) + ... + (a_n)$

**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 $(m) + (n) = (\text{m}, \text{n}), (m) \cap (n) = (\text{kgV}(m, n)), (m)(n) = (mn)$

**Bemerkung 1.34.** $I, J, subseteqR$ 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 $I_1, ..., I_n \subseteq R$ paarweise relative Primideale. Dann gilt:

$$I_1 \cdot ... \cdot I_n = I_1 \cap ... \cap I_n$$

*Beweis.* Beweis durch Induktion nach n:

- $n = 2$: aus 1.37 (c)
- $n \geq 3$: Behauptung sei wahr für alle $k < n$. Setze $J := I - I_1 \cdot ... \cdot I_{n-1} \overset{IV}{=} I_1 \cap ... \cap I_{n-1}$ Behauptung: $J + I_n = (1)$. Denn: Nach Vorraussetzung ist $I_j + I_n = (1)$ für $j = 1, ..., n - 1$

$$\begin{aligned} &\implies \text{ Für alle } j \in \{1, ..., n-1\} \text{ existieren } x_j \in I_j, y_j \in I_n \text{ mit } x_j + y_j = 1 \\ &\implies x_1 \cdot ... \cdot x_n - 1 = (1 - y_1) \cdot ... \cdot (1 - y_{n-1}) \\ &\implies x_1 \cdot ... \cdot x_{n-1} = 1 + y \text{ für ein } y \in I_n \\ &\implies 1 = \underbrace{x_1 \cdot ... \cdot x_{n-1}}_{\in I_1 \cdot ... \cdot I_{n-1} = J} + \underbrace{(-1)y}_{I_n} \in J + I_n, \text{ d.h. } J + In = (1) \end{aligned}$$

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

□

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

(a) $\varphi$ ist surjektiv $\Leftrightarrow$ Die Ideale $I_1, ..., I_n$ 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 Vorraussetzung, dass $I_1, ..., I_n$ paarweise relativ prim sind, einen Ringidomorphismus

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

*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 $\overline{0}, \overline{1}$.

(a) "$\Rightarrow$SSei $\varphi$ surjektiv, seien $i, j \in \{1, ..., n\}, i \neq j$.
Behauptung: $I_i + I_j = (1)$. Wegen $\varphi$ surjektiv existiert ein $x \in R$ mit

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

Außerdem:

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

(b) "$\Leftarrow$SSeien $I_1, ..., I_n$ paarweise relativ prim.

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

$$\begin{aligned}&\text{Für } j \neq i \text{ ist } I_i + I_j = (1) \\ &\implies \text{ Es existieren } u_j \in I_i, v_j \in V_j \text{ mit } u_j + v_j = 1 \\ &\text{Setze } x := v_1 \cdot ... \cdot v_{i-1} \cdot v_{i+1} \cdot ... \cdot v_n \\ &\implies x \in I_j \text{ für } j \neq i \text{ und } x \\ &= (1-u_1) \cdot ... \cdot (1-u_{i-1})(1-u_{i+1} \cdot ... \cdot (1-u_n) \\ &= 1 + z \text{ für ein } z \in I_i \\ &\implies \varphi(x) = (\overline{0}, ..., \overline{0}, \underbrace{\overline{1}}_{i-\text{te Stelle}}, \overline{0}, ..., \overline{0})\end{aligned}$$

(b)

$$\begin{aligned}&\text{Sei } y = (r_1 + I_1, ..., r_n + I_n) \\ &\implies \varphi(r_1 + I_1, ..., r_n + I_n) = \varphi(r_1)\varphi(e_1) + ... + \varphi(r_n)\varphi(e_n) \\ &\qquad = (r_1 + I_1, \overline{0}, ..., \overline{0}) + ... + (\overline{0}, ..., \overline{0}, r_n + I_n) \\ &\qquad = (r_1 + I_1, ..., r_n + I_n) = y\end{aligned}$$

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

(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 Bedrifflichkeit (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: $b|a$) $\overset{\text{Def:}}{\Leftrightarrow}$ Es existiert ein $c \in R$ mit $a = bc$.
- $a, b$ heißen **assoziiert** (Notation: $a \widehat{=} b$) $\overset{\text{Def:}}{\Leftrightarrow}$ $a|b$ und $b|a$

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

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

(i) $a \widehat{=} b$

(ii) Es existiert ein $e \in R^\times$ mit $a = be$

(iii) $(a) = (b)$

*Beweis.*
- (i) $\implies$ (ii): Sei $a \widehat{=} b \implies a|b$ und $b|a \implies$ Es existieren $c, d \in R$ mit $b = ac$ und $a = bd \implies b = ac = bdc \implies b(1 - dc) = 0$
  1. Erster Fall: $b = 0 \implies a = 0$. Setze $e := 1$. Fertig.
  2. Zweiter Fall: $b \neq 0 \underset{R \text{ nullteilerfrei}}{\implies} 1 - dc = 0 \implies cd = 1 \implies c, d \in R^\times$. Setze $e := d$, dann $a = be$ mit $e \in R^\times$
- (ii) $\implies$ (iii): Sei $a = be$ mirt $e \in R^\times \implies a \in (b) \implies (a) \subseteq (b)$. Wegen $e \in R^\times$ ist $b = e^{-1}a \implies b \in (a) \implies (b) \subseteq (a)$
- (iii) $\implies$ (i): Sei $(a) = (b) \implies a \in (b) \implies$ Es existiert $c \in R$ mit $a = bc \implies b|a$. Analog: $a|b$. Also: $a \widehat{=} b$.

□

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

(GGT1) $d|a_1, ..., d|a_n$

(GGT2) $c|a_1, ..., c|a_n \implies c|d$

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

**Anmerkung.**
- Sind $d_1, d_2 \in \mathrm{GGT}(a_1, ..., a_n)$, dann folgt$d_1|d_2$ und $d_2|d_1$, also $d_1 \widehat{=} d_2$
- Ist $d \in \mathrm{GGT}(a_1, ..., a_n)$ und $d' \widehat{=} d$, dann ist $d' \in \mathrm{GGT}(a_1, .l.., a_n)$
- Ohne zusätzliche Vorraussetzung an $R$ kann man im Allgemeinen nicht erwarten, dass $\mathrm{GGT}(a_1, ..., a_n) \neq \emptyset$ (z.B. in $R = \mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-3} | a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ isr $\mathrm{GGT}(4, 2(1 + \sqrt{-3})) = \emptyset$)

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

(a) $\mathrm{GGT}(a_1, ..., a_n) \neq \emptyset$

(b) $d \in \mathrm{GGT}(a_1, ..., a_n) \Leftrightarrow (d) = (a_1, ..., a_n)$

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

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

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

(b) "$\Rightarrow$": Sei $d \in$ GGT$/a_1, ..., a_n) \overset{\text{Anm. 2.4}}{\implies} d \widehat{=} \tilde{d} \overset{2.3}{\implies} (d) = (\tilde{d}) = (a_1, ..., a_n)$

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

□

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

$$d =: \text{ggt}(a_1, ..., a_n)$$

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

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

den größten gemeinsamen Teiler von $f_1, ..., f_n$.(Und man setzt ggT$/0, ..., 0) := 0$.)

**Folgerung.** Sei $R$ ein HIR, $a, b \in R, d \in$ 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 $p \in R \backslash (R^\times \cup \{0\})$

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

p heißt **Primelement** $\overset{\text{Def:}}{\Leftrightarrow}$ Aus $p|ab$ mit $a, b \in R$ folgt stets $p|a$ oder $p|b$

$\Leftrightarrow (p)$ ist ein Primideal

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

**Beispiel 2.7.**

$$\begin{aligned} \text{irreduzible Elemente in } \mathbb{Z} &= \text{ Primzahlen aus } \mathbb{N} \text{ sowie deren Negative} \\ &= \text{ Primelemente in } \mathbb{Z} \end{aligned}$$

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

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

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

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

**Bemerkung 2.9.** Sei $R$ ein HIR, $p \in R \backslash (R^\times \cup \{0\})$. 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 $(p) \not\subseteq I$. Wegen $R$ HIR existiert $a \in R$ mit $I = (a) \underset{p \in I}{\implies}$ 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 $p \in R\backslash(R^\times \cup \{0\}) : p$ 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** $\overset{\text{Def.}}{\implies}$ Jedes $a \in R\backslash(R^\times \cup \{0\})$ lässt sich eindeutig bis auf Reihenfolge und Assoziierbarkeit als Produkt von irreduziblen Elementen aus $R$ schreiben, d.h es existieren irreduzible Elemente $p_1, ..., p_r \in R$ mit

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

und sind $q_1, ..., q_s$ irreduzible Elemente mit $a = q_1 \cdot ... \cdot q_s$, so ist $r = s$ und nach Umnummerieren ist $p_i \widehat{=} q_i$ für $i = 1, ..., r$

**Ziel.** Jeder HIR ist faktoriell.

**Definition 2.11.** R heißt **noethersch** $\overset{\text{Def.}}{\Leftrightarrow}$ Für jede aufsteigende Kette $I_1 \subseteq I_2 \subseteq ...$ 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 $I_1 \subseteq I_2 \subseteq ...$ eine aufsteigende Kette von Idealen aus $R$. Setze $I := \bigcup\limits_{k \geq 1} I_k$

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 $a \in I_n \implies (a) \subset I_n \subset I = (a) \implies I_n = I \implies I_k = I_n$ 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 $M := \{(a) | a \in R\backslash(R^\times \cup \{0\})$ besitzt keine Faktorisierung in irreduziele 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 $I \not\subseteq I'$, 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 $a_1, a_2 \in R\backslash(R^\times \cup \{0\})$ 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 $a = a_1 b = a_1 a_2 \implies a_1(a_2 - b) = 0 \overset{R \text{ nullteilerfrei}}{\implies} a_2 = b \in R^\times$ *Widerspruch.* Also: $(a) \not\subseteq (a_1)$, analog $(a) \not\subseteq (a_2) \implies (a_1), (a_2) \notin M \implies a_1, a_2$ haben Faktorisierung in irreduzible Elemente, also auch $a = a_1 a_2$ *Widerspruch.* Also: $M \neq \emptyset \implies$ Existenz.

2. Eindeutigkeit der Zerlegung: Sei $a = p_1 \cdot ... \cdot p_r = q_1 \cdot ... \cdot p_r = q_1 \cdot ... \cdot q_s$ mit $p_1, ..., p_r, p_1, ..., p_s$ irreduzibel. Beweis per Induktion nach $r$:
   - Induktionsanfang: $r = 0 \implies a = 1 \implies s = 0(\text{sonst} q_1, ..., q_s \in R^\times \textit{ Widerspruch})$
   - Induktionsannahme: Die Behauptung sei für $0, ..., r-1$ bewiesen.
   - Induktionsschritt: $p_1 | p_1 \cdot ... \cdot p_r = q_1 \cdot ... \cdot q_s \overset{p_1 \text{Primelememt}}{\implies}$ Es existiert ein $j \in \{1, ..., s\}$ mit $p_1 | q_j$. Nach Umnummerieren 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 $p_1 \widehat{=} q_1 \implies p_1 \cdot ... \cdot p_r = cp_1 q_2 \cdot ... \cdot q_s \implies p_1(p_2 \cdot ... \cdot p_r - cq_2 \cdot ... \cdot q_s) = 0 \underset{R \text{ nullteilerfrei}}{\implies} p_2 \cdot ... \cdot p_r 0(cq_2) q_3 \cdot ... \cdot q_s$. Wegen $c \in R^\times$ ist $cq_2$ irreduzibel $\overset{IV}{\implies} r - 1 = s - 1( \implies r = s)$ und nach Umnummerieren ist $p_2 \widehat{=} cq_2 \widehat{=} q_2, p_3 \widehat{=} q_3, ..., p_r \widehat{=} q_r$

□

# 3 Euklidische Ringe

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

**Definition 3.1.** $R$ heißt **euklidischer Ring** $\overset{\text{Def:}}{\Leftrightarrow}$ $R$ ist nullteilerfrei und es existiert eine Abbildung $\delta : R \backslash \{0\} \longrightarrow \mathbb{N}_0$ , so dass gilt: Für alle $f, g \in R, g \neq 0$ existieren $q, r \in R$ mit $f = qg + r$ und $(\delta(r) < \delta(g)$ 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 $\delta : K \backslash \longrightarrow \mathbb{N}_0, x \mapsto 1$ 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 $\emptyset \neq \{\delta(a) | a \in I \backslash \{0\}\} \subseteq N_0$. Wähle $a \in I \backslash \{0\}$, 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 $(\delta(r) < \delta(a)$ oder $r = 0) \implies r = \underset{\in I}{f} - \underset{\in I}{qa} \in I$. 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 $\overset{3.3}{\implies}$ $R$ Hauptidealring $\overset{2.14}{\implies}$ $R$ faktoriell. □

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

$$f = c\overset{e_1}{p_1} \cdot ... \cdot \overset{e_r}{p_r}$$

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

*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 $\delta, a, b \in R\backslash\{0\}$. Wir betrachten eine Folge $a_0, a_1, ...$ von Elementen aus $R$, dei induktiv wie folgt gegeben ist:

$$\begin{aligned} a_0 &:= a \\ a_1 &:= b \\ a_0 &:= q_0a_1 + a_2 \text{ mit } \delta(a_2) < \delta(a_1) \text{ oder } a_2 = 0 \\ \text{Falls } a_2 \neq 0: a_1 &= q_1a_2 + a_3 \text{ mit } \delta(a_3) < \delta(a_2) \text{ oder } a_3 = 0 \\ &\vdots \\ \text{Falls } a_i \neq 0: a_{i-1} &= q_{i-1}a_i + a_{i+1} \text{ mit } \delta(a_{i+1}) < \delta(a_i) \text{ oder } a_{i+1} = 0 \\ &\vdots \end{aligned}$$

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

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

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

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

(ërweiterter 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 $\delta(a_1) > \delta(a_2) > ...$ 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:

$$\begin{aligned} (G_0)\ a_0 &= q_0a_1 + a_2 \\ &\vdots \\ (G_{n-2})\ a_{n-2} &= q_{n-2}a_{n-1} + a_n \\ (G_{n-1})\ a_{n-1} &= q_{n-1}a_n \end{aligned}$$

Dann gilt: $a_n | a_{n-1} \overset{(a_{n-2})}{\implies} a_n | (q_{n-2}a_{n-1} + a_n) = a_{m-2} \implies ... \implies a_n | a_1$ und $a_n | a_0$. Sei $c \in R$ mit $c | a_0$ und $c | a_1 \overset{(a_0)}{\implies} c | (a_0 - q_0a_1) = a_2 \implies ... \implies c | a_n$. Also: $a_n \in \text{GGT}(a_0, a_1) = \text{GGT}(a, b)$. Es ist

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

(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

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

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

*Beweis.* Falls $A = 0$, dann fertig. Im Folgenden sei $\underset{=(a_{ij})}{A} \neq 0$. Dei $\delta$ 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 $\delta$

   - <u>1. Fall:</u> In der ersten Spalte/Zeile stehen keine Elemente $\neq 0$ außer $a_{11}$; dann fertig
   - <u>2. Fall:</u> 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 obuge 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 $d_{11} \neq 0, \delta(d_{11}) \leq d(d_{ij})$ falls $d_{ij} \neq 0, \delta(d_{11}) \leq \delta(a_{11})$

3. Erreiche $d_{11}|d_{ij}$ für alle $i, j$.
   - <u>1. Fall:</u> Es gilt bereits $d_{11}|d_{ij}$ für alle $i, j$ dann fertig
   - <u>2. Fall:</u> Es existeiren $i, j$ 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

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

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

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

mit $d'_{ij} = d_{ij} - qd_{11}, \delta(d'_{ij}) < \delta(d_{11}) \leq \delta(a_{11})$. Widerhole 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 $c_1|c_2|c_3|...|c_r$ bringen.

□

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

$$A = \begin{pmatrix} 4 & 3 \\ 6 & 5 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 3 & 4 \\ 5 & 6 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 3 & 1 \\ 5 & 1 \end{pmatrix}$$
$$\rightsquigarrow \begin{pmatrix} 1 & 3 \\ 1 & 5 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix} \begin{matrix} \\ |\,\mathrm{II} - \mathrm{I} \end{matrix} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

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

$$A = \begin{pmatrix} t-1 & 0 \\ -1 & t-1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -1 & t-1 \\ t-1 & 0 \end{pmatrix} \begin{matrix} \\ |\,\mathrm{II} + (t-1)\mathrm{I} \end{matrix} \rightsquigarrow \begin{pmatrix} -1 & t-1 \\ 0 & (t-1)^2 \end{pmatrix} \rightsquigarrow\rightsquigarrow \begin{pmatrix} -1 & 0 \\ 0 & (t-1)^2 \end{pmatrix}$$

**Erinnerung an LA1**

- Zeilen-/bzw. Spaltenoperationene wie in 3.8 lassen sich durch Multiplikation mit Elementarmatrizen
$$E_{ij} = \begin{pmatrix} 1 & & \\ & \ddots & \\ \lambda & & 1 \end{pmatrix}$$
,
$$P_{ij} = \begin{pmatrix} 1 &&&&&&&&&& \\ & \ddots &&&&&&&&& \\ && 1 &&&&&&&& \\ &&& 0 &&&& 1 &&& \\ &&&& 1 &&&&&& \\ &&&&& \ddots &&&&& \\ &&&&&& 1 &&&& \\ &&& 1 &&&& 0 &&& \\ &&&&&&&& 1 && \\ &&&&&&&&& \ddots & \\ &&&&&&&&&& 1 \end{pmatrix}$$
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.**
$$\mathrm{GL}(R) = \{A \in M_{n,n}(R) | A \text{ ist invertierbar } \} \qquad = \{A \in M_{n,n}(R) | \det(A) \in R^\times\}$$
ist eine Gruppe bzgl. Multiplikation, die **allgemeine lineare Gruppe** über $R$ von Rang $n$.

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

**Anmerkung.**
- $\sim, \approx$ sind Äquivalenzrelationen auf $M_{m,n}(K)$, nzw. $M_{n,m}(K)$
- $K$ Körper, $A, B \in M_{n,n}(K)$, $\mathrm{C}$ Basis von $K^n$, $\mathrm{D}$ Basis von $K^m$, $f : K^n \longrightarrow K^m$ lineate Abbildung mit $M_{\mathrm{D}}^{\mathrm{C}}(f) = A$. Dann: $A \sim B \Leftrightarrow$ Es existieren Basen $\mathrm{C}', \mathrm{D}'$ von $K^n$ bzw. $K^m$ mit $M_{\mathrm{D}'}^{\mathrm{C}'}(f) = B$ (d.h. $A, B$ beschreiben bzgl. geeignter Basen dieselber lineare Abbildun)

**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 $c_1, ..., c_r \in R\backslash\{0\}$ mit $c_1|c_2|...|c_r$ 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) □

**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:

- Rang $A = r \implies$
$$A \sim \left(\begin{array}{c|c} E_r & 0 \\ \hline 0 & 0 \end{array}\right)$$
- $S \in \mathrm{GL}_n(K), T \in \mathrm{GL}_n(K) \implies$ Rang$(SAT^{-1})$=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** $\overset{\text{Def:}}{\Leftrightarrow}$ $B$ 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 $A$.
- $\mathrm{Fit}_l(A) = (\det(B) | B$ ist $l \times l -$ 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.**

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

- $\mathrm{Fit}_1(A) = (\det(1), \det(2), \det(3), \det(4)) = (1,2,3,4) = (1) = \mathbb{Z}$
-
$$\mathrm{Fit}_2(A) = \left(\det \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \right) = (-2) = 2\mathbb{Z}$$

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

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

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

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

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

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

von $SA$

$$\implies \det(B) = \det \begin{pmatrix} \sum_{r_1=1}^{m} s_{i_1,r_1} a_{r_1,j_1} & \dots & \sum_{r_1=1}^{m} s_{i_1,r_1} a_{r_1,j_l} \\ b_{i_2,j_1} & \dots & b_{i_2,j_l} \\ \vdots & & \vdots \\ b_{i_l,j_1} & \dots & b_{i_l,j_l} \end{pmatrix}$$

$$= \sum_{r_1=1}^{m} s_{i_1,r_1} \cdot \det \begin{pmatrix} a_{r_1,j_1} & \dots & a_{r_1,j_l} \\ b_{i_2,j_1} & \dots & b_{i_2,i_l} \\ \vdots & & \vdots \\ b_{i_l,j_1} & \dots & b_{i_l,j_l} \end{pmatrix}$$

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

$\implies \mathrm{Fit}_l(SA) \subseteq \mathrm{Fit}_l(A)$.

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

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

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

□

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

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

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

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

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

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

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

*Beweis.*

- Für $l > r$ erhält jede $l \times l$-Untermmatrix von $A$ stets eine Nullzeile, d.h. $\mathrm{Fit}_l(A) = (0)$
- $l \leq r$: 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 $1 \leq i_1 < i_2 < ... < i_l \leq r$

$$\Longrightarrow \text{Fit}_l(A) = (c_{i_1} \cdot ... \cdot c_{i_l})|1 \leq i_1 < i_2 ... < i_l \leq r)$$
$$\Longrightarrow (c_1 \cdot ... \cdot c_l) \subseteq \text{Fit}_l(A)$$

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

$$\Longrightarrow c_1|c_{i_1}, ..., c_l|c_{i_l} \Longrightarrow c_1 \cdot ... \cdot c_l|c_{i_1} \cdot ... \cdot c_{i_l} \Longrightarrow (c_{i_1} \cdot ... \cdot c_{i_l}) \subseteq (c_1 \cdot ... \cdot c_l)$$
$$\Longrightarrow \text{Fit}_l(A) \subseteq (c_1 \cdot ... \cdot c_l)$$

□

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

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

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

*Beweis.* 1. Existenz aus 3.12

2. Eindeutigkeit von $r$: 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

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

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

$$\overset{3.16}{\underset{3.17}{\Longrightarrow}} \text{Fit}_l(A) = \begin{cases} (c1 \cdot ... \cdot c_l) & l \leq r \\ (0) & \text{sonst} \end{cases} = \begin{cases} (d_1 \cdot ... \cdot d_l) & \\ (0) & \text{sonst} \end{cases}$$

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

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

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

- IA: $\text{Fit}_1(A) = (c_1) = (d_1) \overset{2.3}{\Longrightarrow} c_1 \widehat{=} d_1$

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

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

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

□

**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 Assoziietheit überein

(iii) $\mathrm{Fit}_l(A) = \mathrm{Fit}_l(B)$ für alle $1 \leq l \leq \min\{m, n\}$

*Beweis.*

- (i) $\implies$ (iii): aus 3.16
- (iii) $\implies$ (ii): Seien $c_1, ..., c_r, d_1, ..., d_s$ 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 $c_1 \widehat{=} d_1, ..., c_r \widehat{=} d_r$, etwa $d_1 = \lambda_1 c_1, ..., d_r 0 \lambda_r c_r$ mit $\lambda_1, ..., \lambda_r \in R^\times$

$$\Longrightarrow \left(\begin{array}{cccc|c} d_1 & & & & 0 \\ & d_2 & & & \vdots \\ & & \ddots & & \\ & & & d_r & 0 \\ \hline 0 & \dots & & 0 & 0 \end{array}\right) = \left(\begin{array}{cccc|c} \lambda_1 c_1 & & & & 0 \\ & \lambda_2 c_2 & & & \vdots \\ & & \ddots & & \\ & & & \lambda_r c_r & 0 \\ \hline 0 & \dots & & 0 & 0 \end{array}\right)$$

$$= \underbrace{\begin{pmatrix} \lambda_1 & & & & & \\ & \ddots & & & & \\ & & \lambda_r & & & \\ & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix}}_{\in \mathrm{GL}(m,R)} \left(\begin{array}{cccc|c} c_1 & & & & 0 \\ & c_2 & & & \vdots \\ & & \ddots & & \\ & & & c_r & 0 \\ \hline 0 & \dots & & 0 & 0 \end{array}\right)$$

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

□

**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 Assoziietheit: $\underbrace{1, ..., 1}_{r \text{ Stück}} 0, ..., 0$ (mit $r = \text{Rang } A$). D.h.

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

**Beispiel 3.16.**

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

$$\begin{aligned} \mathrm{Fit}_1(A) &= (6, -2, -2, 2) = (2), \\ \mathrm{Fit}_2(A) &= (\det A) = (8) \\ \mathrm{Fit}_1(B) &= (4, 8, 4, 6) = (2) \\ \mathrm{Fit}_2(B) &= (\det B) = (-8) = (8) \end{aligned}$$

$\Longrightarrow \; A \sim B$ Es ist $(c_1) = \mathrm{Fit}_1(A), (c_1, c_2) = \mathrm{Fit}_2(A) = (8) = (2)$ 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 $\varphi \in \mathrm{End}(V)$. Wie einfach kann man $M_B(\varphi)$ bekommen durch geeignete Wahl einer Basis $B$? In Termen von MAtrizen: Suche möglichst einfache Vertreter der Äquivalenzklasen bezüglich "$\approx$".

# 4 Invarianten-und Determinantenteiler

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

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

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

$P_A := tE_n - A \in \mathrm{M}_{n,n}(K[t])$ 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 $A, b \in \mathrm{M}_{n,n}(K)$. Dann sind äquivalent:

(i) $A \approx B$ (in $\mathrm{M}_{n,n}(K)$)

(ii) $P_A \sim P_B$ (in $M_n, n(K[t])$)

*Beweis.* (i) $\implies$ (ii): Sei $A \approx B \implies$ Es existiert ein $S \in \mathrm{GL}_n(K)$ 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 komnstruieren $R \in \mathrm{M}_{n,n}(K)$ mit $AR = RB$. Nach Vorraussetzung existieren $S, T \in \mathrm{GL}_n(K[t])$ mit $P_A = SP_BT^{-1}$, d.h. $SP_B = P_AT$

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

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

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

$$
\begin{aligned}
\Longrightarrow S(tE_n - B) &= \sum_{i=0}^{m} t^i S_i(zE_n - B) \\
&= \sum_{i=0}^{m} (t^{i+1} S_i - t^i S_i B) \\
&= \sum_{i=1}^{m+1} t^i S_{i-1} - \sum_{i=0}^{m} t^i S_i B \\
&= \sum_{i=0}^{m+1} (S_{i-1} - S_i B) t^i \text{ mit } S_{i-1}, S_{m+1} := 0. \\
(tE_n - B) &= (tE_n - A) \sum_{i=0}^{m} t^i T_i \\
&= \sum i = 0^m (t^{i+1} T_i - t^i A T_i) \\
&= \sum_{i=0}^{m+1} (T_{i-1} - AT_i) t^i \\
\overset{(*)}{\Longrightarrow} \sum_{i=0}^{m+1} (S_{i-1} - S_i B) t^i &= \sum_{i=0}^{m+1} (T_{i-1} - AT_i) z^i \\
\Longrightarrow S_{i-1} - S_i B &= T_{i-1} A T_i \text{ für } 0 \le i \le m+1 \\
\Longrightarrow A_i S_{i-1} - A^i S_i B &= A^i T_{i-1} - A^{i+1} T_i \text{ für } 0 \le i \le m+1 \\
\Longrightarrow \sum_{i=0}^{m+1} (A^i S_{i-1} - A^i S_i B) &= \sum_{i=0}^{m+1} (A^i T_{i-1} - A^{i+1} T - i) \\
&= (AT_{i-1} - AT_0) + (AT_o - A^2 T_1) \\
&+ ... + (A^{m+1} T_m - A^{m+2} T_{m+1}) \\
&= AT_{i-1} - A^{m+2} T_{m+1} = 0. \\
\Longrightarrow \sum_{i=0}^{m+1} A^i S_{i-1} &= \sum_{i=0}^{m+1} A^i S_i B \\
\underset{S_{-1}=0}{\overset{S_{m+1}=0}{\Longrightarrow}} \sum_{i=0}^{m+1} A^i S_{i-1} &= \sum_{i=0}^{m} A^i S_i B \\
\Longrightarrow A \left( \sum_{i=0}^{m} A^i S_i \right) &= \left( \sum_{i=0}^{m} A^i S_i \right) B
\end{aligned}
$$

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

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

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

ohne Einschränkung $m$ wie vorhin.

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

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

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

Wegen $SM = E_n$ folgt $\left(\sum\limits_{i=0}^{m} t^i S_i\right)\left(\sum\limits_{j=0}^{m} t^j M_j\right) = E_n$.
$S_0M_0 + \sum\limits_{k=0} \left(\sum_{i+j=k} S_iM_j\right) t^k = E_n$
$\overset{\text{Koeffizentenvergleich}}{\Longrightarrow} S_0M_0 = E_n, \sum\limits_{i+j=k} S_iM_j = 0$ für $K \geq 1$.
$\Longrightarrow RN = \sum\limits_{i,j=0}^{m} A^{i+j}S_iM_j = S_0M_0 + \sum\limits_{k=1}^{2m} A^k \underbrace{\sum_{i+j=k} S_iM_j}_{=0} = E_n \Longrightarrow$
Behauptung.

□

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

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

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

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

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

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

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

*Beweis.* (a) $K[t]$ ist ein Euklidischer Ring (Bsp. 3.2).
$\overset{\text{Satz 3.18}}{\Longrightarrow}$ Es existieren $\tilde{c_1}, ..., \tilde{c_r} \in K[t] \setminus \{0\}$ mit

$$P_A \sim \begin{pmatrix} \tilde{c_1} & & & & & \\ & \ddots & & & & \\ & & \tilde{c_r} & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}$$

mit $\tilde{c_1}|...|\tilde{c_r}$. Es ist $\mathrm{Fit}_n(P_A) = (\det P_A) = (\chi_A^{\mathrm{char}}) \neq (0) \Longrightarrow r = n$ und Fit : $n(P_A =) \overset{3.16}{=}$ $(\tilde{c_1} \cdot ... \cdot \tilde{c_n})$. Wegen $\tilde{c_i} \neq 0$ für $i = 1, ..., n$ existieren normierte Polynome $c_i(A), i = 1, ..., n$ mit $c_i(A) \widehat{=} \tilde{c_i}$.

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

Eindeutigkeit: $c_1'(A), ..., c_n'(A) \in K[t]$ normiert mit $c_1'(A)|c_2'(A)|...|c_n'(A)$ und

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

$\Longrightarrow c_i'(A) \subseteq c_i(A)$ für $i = 1, ..., n \underset{c_i(A), c_i'(A) \text{ normiert}}{\Longrightarrow} c_i'(A) = c_i(A)$ für $i = 1, ..., n$

(b) $K[t]$ HIR nach Satz 3.3 $\Longrightarrow$ $\mathrm{Fit}_l(P_A), l = 1, ..., n$ sind Hauptideale und nach 3.16, 3.17 ist $\mathrm{Fit}_l(P_A) = (c_1(A) \cdot ... \cdot c_l(A))$ für $l = 1, ..., n$, insbesondere ist $\mathrm{Fit}_l(P_A) \neq 0$. Erzeuger der Hauptidealringe $\mathrm{Fit}_l(P_A)$ sind eindeutig bis auf Assoziiertheit (2.3) $\implies$ Es existieren eindeutig bestimmte Polynome $d_1(A), ..., d_n(A) \in K[t]$ mit $\mathrm{Fit}_l(P_A) = (d_l(A))$ für $l = 1, ..., n$. Es ist

$$\begin{aligned}\mathrm{Fit}_l(P_A) =&(\det(B)|B \text{ ist } l \times l\text{-Untermatrix von } P_A)\\ \overset{2.5}{=}&(\mathrm{ggT}(\det(B)|B \text{ ist } l \times l\text{-Untermatrix von } P_A)\\ =&(D_l(A)\end{aligned}$$

$$\underset{\text{ggT normiert}}{\overset{d_l \text{ normiert}}{\Longrightarrow}} d_l(A) = \mathrm{ggT}(...).$$

□

**Anmerkung.** Also:

$$\begin{aligned}\text{Invariantenteiler von } A =& \text{ normierte Elementarteiler von } P_A\\ \text{Determinantenteiler von } A =& \text{ normierten Erzeuger der Fittingideale von} P_A\end{aligned}$$

**Folgerung.** Sei $A \in \mathrm{M}_{n,n}(K)$.

Dann gilt:

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

Insbesondere gilt

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

sowie

$$\begin{gathered}d_1(A)|...|d_n(A),\\ \mathrm{Fit}_n(P_A) \subseteq \mathrm{Fit}_{n-1}(P_A) \subseteq ... \subseteq \mathrm{Fit}_1(P_A)\end{gathered}$$

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

(a) $A \approx B$

(b) Die Invariantenteiler von $A$ stimmen mit den Invarianten von $B$ überein:

$$c_1(A) = c_1(B), ..., c_n(A) = c_(B)$$

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

$$d_1(A) = d_1(B), ..., d_n(A) = d_n(B)$$

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

**Beispiel 4.5.** Sei

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

Es ist

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

Bestimmen der Determinantenteiler von $A$:

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

Sei

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

Bestimmen der Invariantenteiler von $B$:

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

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

Also $A \not\approx B$.

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

(i) $A \approx B$ in $\mathrm{M}_{n,n}(K)$

(ii) $A \approx B$ in $\mathrm{M}_{n,n}(L)$

*Beweis.* Übung. □

test2