

Lineare Algebra II (Vogel)

Robin Heinemann

12. November 2017

Inhaltsverzeichnis

18 Eigenwerte	1
19 Dualraum	14
20 Bilinearformen	18
21 Quadratische Räume	22
22 Euklidische Räume	28
23 Die orthogonale Gruppe	34
24 Der Spektralsatz	39
25 Unitäre Räume	45
26 Ringe, Ideale und Teilbarkeit	50
27 Euklidische Ringe	57
28 Normalformen von Endomorphismen	65
29 Moduln	78
30 Moduln über Hauptidealringen	85

18 Eigenwerte

In diesem Abschnitt sei $n \in \mathbb{N}$, V ein K -VR und $\varphi \in \text{End}_K(V)$.

Frage: V endlichdim. Existiert eine Basis $\mathcal{B} = (v_1, \dots, v_n)$ von V , sodass $M_{\mathcal{B}}(\varphi)$ eine Diagonalmatrix ist, das heißt

$$M_{\mathcal{B}}(\varphi) = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

mit $\lambda_1, \dots, \lambda_n \in K$?

Für $i = 1, \dots, n$ wäre dann $\varphi(v_i) = \lambda_i v_i$

Definition 18.1 $\lambda \in K, v \in V$

- λ heißt Eigenwert von $\varphi \stackrel{\text{Def}}{\iff} \exists v \in V, v \neq 0 : \varphi(v) = \lambda v$
- v heißt Eigenvektor zum Eigenwert $\lambda \stackrel{\text{Def}}{\iff} v \neq 0 \wedge \varphi(v) = \lambda v$
- φ heißt diagonalisierbar $\stackrel{\text{Def}}{\iff} V$ besitzt eine Basis aus EV von φ

(Falls V endlichdimensional, ist die äquivalent zu: Es gibt eine Basis \mathcal{B} von V und $\lambda_1, \dots, \lambda_n \in K$ mit

$$M_{\mathcal{B}}(\varphi) = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

)

Eigenwerte, Eigenvektoren, Diagonalisierbarkeit einer Matrix $A \in M(n \times n, K)$ sind über den Endomorphismus $\tilde{A} : K^n \rightarrow K^n$ definiert.

Bemerkung 18.2 $A \in M(n \times n, K)$. Dann sind äquivalent:

1. A ist diagonalisierbar.
2. Es gibt eine Basis von K^n aus Eigenvektoren von A

$$3. \text{ Es gibt ein } S \in \text{GL}(n, K), \lambda_1, \dots, \lambda_n \in K \text{ mit } SAS^{-1} = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

4. A ist ähnlich zu einer Diagonalmatrix

In diesem Fall steht in den Spalten von S^{-1} eine Basis des K^n aus EV von A , und für jede Matrix $A \in M(n \times n, K)$ mit der Eigenschaft, dass die Spalten von S^{-1} eine Basis des K^n aus EV von A bilden, dann ist SAS^{-1} eine Diagonalmatrix (mit den EW auf der Diagonalen.)

Beweis Äquivalenz:

1. \iff 2. Definition, 2. \iff 3. aus Basiswechselsatz (16.6), 3. \iff 4. aus Definition Ähnlichkeit (16.12)

$$\text{Zusatz: Sei } S \in \text{GL}(n, K) \text{ mit } SAS^{-1} = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \implies A(S^{-1}e_j) = S^{-1} \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} e_j.$$

Wegen $S^{-1} \in \text{GL}(n, K)$ ist $S^{-1}e_j \neq 0$, das heißt S^{-1} ist EV von A zum EW λ_j

Wegen $S^{-1} \in \text{GL}(n, K)$ ist $(S^{-1}e_1, \dots, S^{-1}e_n)$ eine Basis des K^n aus EV von A .

Sei $S \in \text{GL}(n, K)$, das heißt die Spalten von S^{-1} eine Basis des K^n aus EV von A bilden, das heißt für alle $j \in \{1, \dots, n\}$ ist $AS^{-1}e_j = \lambda_j S^{-1}e_j$ für ein $\lambda_j \in K$.

$$\implies AS^{-1}e_j = S^{-1}\lambda_j e_j = S^{-1} \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} e_j \implies SAS^{-1}e_j = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} e_j, j = 1, \dots, n$$

$$\implies SAS^{-1} = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

□

Beispiel 18.3 $K = \mathbb{R}, V = \mathbb{R}^2$

1. $\varphi : \mathbb{R}^2 \rightarrow \mathbb{R}^2, \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} x_2 \\ x_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ Es ist $\varphi\left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} 1 \\ 1 \end{pmatrix} = 1 \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, das heißt $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ ist EV von φ zum EW 1.
 $\varphi\left(\begin{pmatrix} 1 \\ -1 \end{pmatrix}\right) = \begin{pmatrix} -1 \\ 1 \end{pmatrix} = (-1) \begin{pmatrix} 1 \\ -1 \end{pmatrix}$, also ist $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$ EV von φ zum EW -1 . Somit: $\left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix}\right)$ ist eine Basis des \mathbb{R}^2 aus EV von φ , das heißt φ ist diagonalisierbar.
 In Termen von Matrizen: $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in M(2 \times 2, \mathbb{R})$ ist diagonalisierbar, und mit $S = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ ist dann ist $SAS^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ Achtung: Das φ diagonalisierbar ist, heißt nicht, dass jeder Vektor aus $V = \mathbb{R}^2$ ein EV von φ ist, zum Beispiel ist $\varphi\left(\begin{pmatrix} 1 \\ 2 \end{pmatrix}\right) = \begin{pmatrix} 2 \\ 1 \end{pmatrix} \neq \lambda \begin{pmatrix} 1 \\ 2 \end{pmatrix} \forall \lambda \in \mathbb{R}$.
2. $\varphi : \mathbb{R}^2 \rightarrow \mathbb{R}^2, \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} -x_2 \\ x_1 \end{pmatrix}$ (= Drehung um $\frac{\pi}{2}$). hat keinen EW. Beweis dafür: später.

Ziel: Suche Kriterien für Diagonalisierbarkeit.

Bemerkung 18.4 v_1, \dots, v_m EV von φ zu paarweise verschiedenen EW $\lambda_1, \dots, \lambda_m \in K$. Dann ist (v_1, \dots, v_m) linear unabhängig, insbesondere ist $m \leq \dim V$. Insbesondere gilt: ist V endlichdimensional, dann hat φ höchstens $\dim(V)$ Eigenwerte.

Beweis per Induktion nach m :IA: $m = 1 : v_1 \neq 0$, da v_1 EV $\implies (v_1)$ linear unabhängig.IS: sei $m \geq 2$, und die Aussage für $m - 1$ bewiesen.Seien $\alpha_1, \dots, \alpha_m \in K$ mit $\alpha_1 \lambda_1 v_1 + \dots + \alpha_m \lambda_m v_m = 0$. Außerdem: $\alpha_1 \lambda_1 v_1 + \dots + \alpha_m \lambda_1 v_m = 0$

$$\implies \alpha_2(\lambda_2 - \lambda_1)v_2 + \dots + \alpha_m(\lambda_m - \lambda_1)v_m = 0$$

$$\alpha_2 \lambda_2 - \lambda_1 = \dots = \alpha_m(\lambda_m - \lambda_1) = 0$$

$$\implies \alpha_2 = \dots = \alpha_m = 0$$

$$\implies \alpha_1 v_1 = 0 \implies \alpha_1 = 0 \implies (v_1, \dots, v_m) \text{ linear unabhängig} \quad \square$$

Folgerung 18.5 V endlichdimensional, φ habe n paarweise verschiedene EW, wobei $n = \dim V$ Dann ist φ diagonalisierbar.

Beweis Für $i = 1, \dots, n$ sei v_i ein EV von φ zum EW $\lambda_i \implies (v_1, \dots, v_n)$ linear unabhängig, wegen $n = \dim V$ ist (v_1, \dots, v_n) eine Basis von V aus EV von φ \square

Definition 18.6 $\lambda \in K$ $\text{Eig}(\varphi, \lambda) := \{v \in V \mid \varphi(v) = \lambda v\}$ heißt der Eigenraum von φ bezüglich λ . $\mu_{\text{geo}}(\varphi, \lambda) := \dim \text{Eig}(\varphi, \lambda)$ heißt die geometrische Vielfachheit von λ .Für $A \in M(n \times n, K)$ setzen wir $\text{Eig}(A, \lambda) := \text{Eig}(\tilde{A}, \lambda), \mu_{\text{geo}}(A, \lambda) := \mu_{\text{geo}}(\tilde{A}, \lambda)$.**Bemerkung 18.7** $\lambda \in K$. Dann gilt:

1. $\text{Eig}(\varphi, \lambda)$ ist ein UVR von V .
2. λ ist EW von $\varphi \iff \text{Eig}(\varphi, \lambda) \neq \{0\}$.

3. $\text{Eig}(\varphi, \lambda) \setminus \{0\}$ ist die Menge der zu λ gehörenden EV von φ .
4. $\text{Eig}(\varphi, \lambda) = \ker(\lambda \text{id}_V - \varphi)$, insbesondere ist $\text{Eig}(A, \lambda) = \ker(\lambda E_m - \varphi) = \text{Lös}(\lambda E_n - A, 0)$ für $A \in M(n \times n, K)$
5. Sind $\lambda_1, \lambda_2 \in K$ mit $\lambda_1 \neq \lambda_2$, dann $\text{Eig}(\varphi, \lambda_1) \cap \text{Eig}(\varphi, \lambda_2) = \{0\}$

Beweis 4. Es ist $v \in \text{Eig}(\varphi, \lambda) \iff \varphi(v) = \lambda v \iff \lambda v - \varphi(v) = 0 \iff (\lambda \text{id}_V - \varphi)(v) = 0 \iff v \in \ker(\lambda \text{id}_V - \varphi)$ Es ist $\text{Eig}(A, \lambda) = \ker(\lambda \text{id}_{K^n} - \tilde{A}) = \ker(\widetilde{\lambda E_n - A}) = \ker(\lambda E_n - A) = \text{Lös}(\lambda E_n - A, 0)$

1. aus 4.
2. λ EW von $\varphi \iff \exists v \in V, v \neq 0$ mit $\varphi(v) = \lambda v \iff \text{Eig}(\varphi, \lambda) \neq \{0\}$.
3. klar.
5. Sei $\lambda_1 \neq \lambda_2, v \in \text{Eig}(\varphi, \lambda_1) \cap \text{Eig}(\varphi, \lambda_2) \implies \lambda_1 v = \varphi(v) = \lambda_2 v \implies \underbrace{(\lambda_1 - \lambda_2)}_{\neq 0} v = 0 \implies v = 0$ □

Bemerkung 18.8 V endlichdimensional, $\lambda \in K$. Dann sind äquivalent:

1. λ ist EW von φ
2. $\det(\lambda \text{id}_V - \varphi) = 0$

Beweis 1. $\iff \text{Eig}(\varphi, \lambda) \neq \{0\} \implies \ker(\lambda \text{id}_V - \varphi) \neq \{0\} \implies \lambda \text{id}_V - \varphi$ nicht injektiv $\implies \lambda \text{id}_V - \varphi$ kein Isomorphismus $\implies \det(\lambda \text{id}_V - \varphi) = 0$. □

Definition 18.9 K Körper, $A = (a_{ij}) \in M(n \times n, K)$

$$\chi_A^{\text{char}} := \det(tE_n - A) = \det \begin{pmatrix} t - a_{11} & -a_{12} & & -a_{1n} \\ -a_{21} & t - a_{22} & & \\ & & \ddots & \\ -a_{n1} & \dots & & t - a_{nn} \end{pmatrix} \in K[t]$$

heißt das **charakteristische Polynom** von A .

Anmerkung Hierfür nötig: Determinanten von Matrizen mit Einträgen in einem kommutativen Ring. In manchen Büchern $\chi_A^{\text{char}} = \det(A - tE_n)$ (schlecht)

Beispiel 18.10

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in M(2 \times 2, \mathbb{R})$$

$$\implies A\chi_a^{\text{char}} = \det \begin{pmatrix} t - 1 & -1 \\ -3 & t - 4 \end{pmatrix} = (t - 1)(t - 4) - 6 = t^2 - 5t - 2$$

Bemerkung 18.11 $A, B \in M(n \times n, K), A \approx B$. Dann ist $\chi_A^{\text{char}} = \chi_B^{\text{char}}$.

Beweis $A \approx B \implies \exists S \in \text{GL}(n, K) : B = SAS^{-1}$

$$\begin{aligned} \implies tE_n - B &= tE_n - SAS^{-1} = SS^{-1}tE_n - SAS^{-1} = StE_nS^{-1} - SAS^{-1} = S(tE_n - A)S^{-1} \\ \implies \chi_B^{char} &= \det(tE_n - B) = \det(S(tE_n - A)S^{-1}) = \det(S) \det(tE_n - A) \det(S^{-1}) = \\ &= \underbrace{\det(S) \det(S)^{-1}}_{=1} \det(tE_n - A) = \chi_A^{char} \quad \square \end{aligned}$$

Definition 18.12 V endlichdim, $n = \dim V$, \mathcal{B} Basis von V , $\varphi \in \text{End}(V)$, $A = M_{\mathcal{B}}(\varphi)$

$$\chi_{\varphi}^{char} := \chi_A^{char} = \det(tE_n - A) \in K[t]$$

heißt das **charakteristische Polynom** von φ .

Anmerkung χ_{φ}^{char} ist wohldefiniert, dann: Ist \mathcal{B}' eine weitere Basis von V , $A' = M_{\mathcal{B}'}(\varphi)$, dann ist $A \approx A'$ und deshalb nach 18.11: $\chi_A^{char} = \chi_{A'}^{char}$.

Satz 18.13 V endlichdimensional, $n = \dim V$. Dann gilt:

1. χ_{φ}^{char} ist ein normiertes Polynom von Grad n :

$$\chi_{\varphi}^{char} = t^n + c_{n-1}t^{n-1} + \dots + c_0$$

mit $c_0 = (-1)^n \det \varphi$, $c_{n-1} = -(\varphi)$ (vgl. Übung zur Spur)

2. Die Nullstellen von χ_{φ}^{char} sind genau die EW von φ :

$$\lambda \in K \text{ ist EW von } \varphi \iff \chi_{\varphi}^{char} \lambda = 0$$

Beweis Sei \mathcal{B} eine Basis von V , $A := M_{\mathcal{B}}(\varphi) \in M(n \times n, K)$

- 1.

$$\begin{aligned} \chi_{\varphi}^{char} &= \chi_A^{char} = \det \underbrace{(tE_n - A)}_{=: B = (B_{ij})} = \sum_{\sigma \in S_n} \text{sgn}(\sigma) B_{1,\sigma(1)} \cdot \dots \cdot B_{n,\sigma(n)} \\ &= (t - a_{11} \cdot \dots \cdot (t - a_{nn})) + \underbrace{\sum_{\sigma \in S_n \setminus \{\text{id}\}} \text{sgn}(\sigma) B_{1,\sigma(1)} \cdot \dots \cdot B_{n,\sigma(n)}}_{:=g} \end{aligned}$$

Für $\sigma \in S_n \setminus \{\text{id}\}$ treten in $B_{1,\sigma(1)}, \dots, B_{n,\sigma(n)}$ höchstens $n - 2$ Diagonalelemente auf, also $\deg(g) \leq n - 2$.

$$\implies \chi_{\varphi}^{char} = t^n - (a_{11} + \dots + a_{nn})t^{n-1} + \text{Terme kleineren Grades}$$

insbesondere:

$$c_{n-1} = -(a_{11} + \dots + a_{nn}) = -\text{tr} A = -\varphi$$

Es ist

$$c_0 = \chi_{\varphi}^{char}(0) = (\det(tE_n - A))(0) = \det(0E_n - A) = \det(-A) = (-1)^n \det A$$

2. Aus $A = M_{\mathcal{B}}(\varphi)$ folgt $\lambda E_n - A = M_{\mathcal{B}}(\lambda \text{id}_V - \varphi)$. Also:

$$\begin{aligned} \chi_{\varphi}^{char}(\lambda) = 0 &\iff (\det(tE_n - A))(\lambda) = 0 \implies \det(\lambda E_n - A) = 0 \iff \det(M_{\mathcal{B}}(\lambda \text{id}_V - \varphi)) = 0 \\ &\implies \det(\lambda \text{id}_V - \varphi) = 0 \iff \lambda \text{ ist EW von } \varphi \quad \square \end{aligned}$$

Definition 18.14 $\lambda \in K$

$$\mu_{alg}(\varphi, \lambda) := \mu(\chi_{\varphi}^{char}, \lambda)$$

heißt die **algebraische Vielfachheit**

Beispiel 18.15

1. $\varphi : \mathbb{R}^2 \rightarrow \mathbb{R}^2, \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{=:A} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$. Es ist $\chi_{\varphi}^{char} = \chi_A^{char} = \det \begin{pmatrix} t & -1 \\ -1 & t \end{pmatrix} = t^2 - 1 = (t-1)(t+1) \in \mathbb{R}[t] \implies \text{EW von } \varphi : 1, -1$.
Es ist $\mu_{alg}(\varphi, 1) = 1, \mu_{alg}(\varphi, -1) = 1$

$$\text{Eig}(\varphi, 1) = \text{Eig}(A, 1) = \text{Lös}(E_2 - A, 0) = \text{Lös}\left(\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}, 0\right) = \text{Lin}\left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right)$$

$$\text{also } \mu_{geo}(\varphi, 1) = \dim \text{Eig}(\varphi, 1) = 1$$

$$\text{Eig}(\varphi, -1) = \text{Eig}(A, -1) = \text{Lös}((-1) \cdot E_2 - A, 0) = \text{Lös}\left(\begin{pmatrix} -1 & -1 \\ -1 & -1 \end{pmatrix}, 0\right) = \text{Lin}\left(\begin{pmatrix} 1 \\ -1 \end{pmatrix}\right)$$

$$\text{also } \mu_{geo}(\varphi, -1) = 1.$$

2. $\varphi : \mathbb{R}^2 \rightarrow \mathbb{R}^2, \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{=:A} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$. Es ist $\chi_{\varphi}^{char} = \chi_A^{char} = \det \begin{pmatrix} t & 1 \\ -1 & t \end{pmatrix} = t^2 + 1, \chi_{\varphi}^{char}$ hat keine NS in $\mathbb{R} \implies \varphi$ hat keine EW.

3. $\varphi : \mathbb{R}^2 \rightarrow \mathbb{R}^2, \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \underbrace{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}}_{=:A} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$. Es ist $\chi_{\varphi}^{char} = \chi_A^{char} = \det \begin{pmatrix} t-1 & -1 \\ 0 & t-1 \end{pmatrix} = (t-1)^2 \implies 1$ ist einziger EW von φ , es ist $\mu_{alg}(\varphi, 1) = 2$

$$\text{Eig}(\varphi, 1) = \text{Eig}(A, 1) = \text{Lös}(1E_2 - A, 0) = \text{Lös}\left(\begin{pmatrix} 0 & -1 \\ 0 & 1 \end{pmatrix}, 0\right) = \text{Lin}\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right)$$

$$\implies \mu_{geo}(\varphi, 1) = 1. \implies \varphi \text{ ist nicht diagonalisierbar.}$$

Satz 18.16 V endlichdimensional, $n = \dim V$

1. Ist φ diagonalisierbar, dann ist $\chi_{\varphi}^{char} = (t - \lambda_1) \cdot \dots \cdot (t - \lambda_n)$ mit $\lambda_1, \dots, \lambda_n \in K$, nicht notwendig verschieden, das heißt χ_{φ}^{char} zerfällt in Linearfaktoren.
2. Ist $\chi_{\varphi}^{char} = (t - \lambda_1) \cdot \dots \cdot (t - \lambda_n)$ mit paarweise verschiedene $\lambda_1, \dots, \lambda_n \in K$, dann ist φ diagonalisierbar.

Beweis 1. Sei φ diagonalisierbar $\rightarrow V$ besitzt Basis $\mathcal{B} = (v_1, \dots, v_n)$ aus EV zu EW $\lambda_i \in K$.

$$\implies M_{\mathcal{B}}(\varphi) = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \implies \chi_{\varphi}^{char} = \det \begin{pmatrix} t - \lambda_1 & & 0 \\ & \ddots & \\ 0 & & t - \lambda_n \end{pmatrix} = (t - \lambda_1) \cdot \dots \cdot (t - \lambda_n)$$

2. Aus $\chi_{\varphi}^{char} = (t - \lambda_1) \cdot \dots \cdot (t - \lambda_n)$ mit $\lambda_1, \dots, \lambda_n$ paarweise verschieden $\implies \lambda_1, \dots, \lambda_n$ sind paarweise verschiedene EW von $\varphi \implies \varphi$ diagonalisierbar. \square

Bemerkung 18.17 V endlichdimensional, $n = \dim V$, λ EW von φ . Dann gilt:

$$1 \leq \mu_{geo}(\varphi, \lambda) \leq \mu_{alg}(\varphi, \lambda)$$

Beweis Sei (v_1, \dots, v_s) eine Basis von $\text{Eig}(\varphi, \lambda) \implies s = \mu_{geo}(\varphi, \lambda) \geq 1$, da λ EW von φ . Nach Basiserweiterungssatz $\exists v_{s+1}, \dots, v_n \in V$, sodass $\mathcal{B} := (v_1, \dots, v_s, v_{s+1}, \dots, v_n)$ eine Basis von V ist.

$$\begin{aligned} \implies A := A_{\mathcal{B}}(\varphi) &= \left(\begin{array}{ccc|ccc} \lambda & & 0 & & & \\ & \ddots & & & & \\ 0 & & \lambda & & & \\ \hline & & 0 & & & \end{array} \right), A' \in M((n-s) \times (n-s), K) \\ \implies \chi_{\varphi}^{char} &= \chi_A^{char} = \det \left(\begin{array}{ccc|ccc} t-\lambda & & 0 & & & \\ & \ddots & & & & \\ 0 & & t-\lambda & & & \\ \hline & & 0 & & & \end{array} \right) = (t-\lambda)^s \det(tE_{n-s} - A') = (t-\lambda)^s \chi_{A'}^{char} \\ \implies \mu_{geo}(\varphi, \lambda) &= s \leq \mu(\chi_{\varphi}^{char}, \lambda) = \mu_{alg}(\varphi, \lambda) \quad \square \end{aligned}$$

Bemerkung 18.18 $\lambda_1, \dots, \lambda_r$ paarweise verschiedene EW von φ . Dann gilt:

$$\text{Eig}(\varphi, \lambda_i) \cap \sum_{\substack{j=1 \\ j \neq i}}^r \text{Eig}(\varphi, \lambda_j) = \{0\} \forall i \in \{1, \dots, r\}$$

Beweis Sei $i \in \{1, \dots, r\}$. Annahme: $\exists v_i \in \text{Eig}(\varphi, \lambda_i) \cap \sum_{\substack{j=1 \\ j \neq i}}^r \text{Eig}(\varphi, \lambda_j) : v_i \neq 0$.

$$\implies \exists v_j \in \text{Eig}(\varphi, \lambda_j), j = 1, \dots, r, j \neq i : v_i = v_1 + \dots + v_{i-1} + v_{i+1} + \dots + v_r$$

Setze $J := \{j \in \{1, \dots, r\}, j \neq i \mid v_j \neq 0\} = \{j_1, \dots, j_s\}$

$$\implies v_i = v_{j_1} + \dots + v_{j_s} \implies v_{j_1} + \dots + v_{j_s} + (-1)v_i = 0 \implies (v_{j_1}, \dots, v_{j_s}, v_i) \text{ linear abhängig} \nmid$$

□

Satz 18.19 V endlichdimensional. Dann sind äquivalent:

1. φ diagonalisierbar
2. χ_{φ}^{char} zerfällt in Linearfaktoren und $\mu_{alg}(\varphi, \lambda) = \mu_{geo}(\varphi, \lambda) \forall$ EW von φ .
3. Sind $\lambda_1, \dots, \lambda_k$ die paarweise verschiedenen EW von φ , dann ist

$$V = \text{Eig}(\varphi, \lambda_1) \oplus \dots \oplus \text{Eig}(\varphi, \lambda_k)$$

In diesem Fall erhält man eine Basis von V aus EV von φ , indem man Basen von $\text{Eig}(\varphi, \lambda_i), i = 1, \dots, k$ zusammenfügt.

Beweis 1. \implies 2. Sei φ diagonalisierbar. $\implies \exists$ Basis \mathcal{B} von V aus EV von φ . Wir ordnen die EV in \mathcal{B} den verschiedenen EW von φ zu und gelangen so zu Familien $\mathcal{B}_i := (v_1^{(i)}, \dots, v_{s_i}^{(i)})$ von linear unabhängigen im $\text{Eig}(\varphi, \lambda_i), i = 1, \dots, k$

- a) Behauptung: \mathcal{B}_i ist eine Basis von $\text{Eig}(\varphi, \lambda_i)$, denn gezeigt: \mathcal{B}_i ist ein ES von $\text{Eig}(\varphi, \lambda_i)$. Sei $v \in \text{Eig}(\varphi, \lambda_i) \leq V$

$$\begin{aligned} \implies \exists \lambda^{(j)} \in K : v &= \sum_{j=1}^k \left(\lambda_1^{(j)} v_1^{(j)} + \dots + \lambda_{s_j}^{(j)} v_{s_j}^{(j)} \right) \\ \implies \underbrace{v - \left(\lambda_1^{(i)} v_1^{(i)} + \dots + \lambda_{s_i}^{(i)} v_{s_i}^{(i)} \right)}_{\in \text{Eig}(\varphi, \lambda_i)} &= \sum_{\substack{j=1 \\ j \neq i}}^k \left(\lambda_1^{(j)} v_1^{(j)} + \dots + \lambda_{s_j}^{(j)} v_{s_j}^{(j)} \right) \in \sum_{\substack{j=1 \\ j \neq i}}^k \text{Eig}(\varphi, \lambda_j) \\ \implies v &= \lambda_1^{(i)} v_1^{(i)} + \dots + \lambda_{s_i}^{(i)} v_{s_i}^{(i)} \end{aligned}$$

- a) Nach 1. ist

$$\mu_{\text{geo}}(\varphi, \lambda_1) + \dots + \mu_{\text{geo}}(\varphi, \lambda_k) = s_1 + \dots + s_k = \dim V$$

$\chi_\varphi^{\text{char}}$ zerfällt nach 18.16 in Linearfaktoren, somit

$$\mu_{\text{alg}}(\varphi, \lambda_1) + \dots + \mu_{\text{alg}}(\varphi, \lambda_k) = \deg(\chi_\varphi^{\text{char}}) = \dim V$$

Wegen $\mu_{\text{geo}}(\varphi, \lambda_i) \leq \mu_{\text{alg}}(\varphi, \lambda_i)$ für $i = 1, \dots, k$ folgt: $\mu_{\text{geo}}(\varphi, \lambda_i) = \mu_{\text{alg}}(\varphi, \lambda_i)$ für $i = 1, \dots, k$.

2. \implies 3. Es gelte 2. Es seien $\lambda_1, \dots, \lambda_k$ die verschiedenen EW von φ . Wir setzen $W := \text{Eig}(\varphi, \lambda_1) + \dots + \text{Eig}(\varphi, \lambda_k)$. Wegen 18.18 ist

$$W = \text{Eig}(\varphi, \lambda_1) \oplus \dots \oplus \text{Eig}(\varphi, \lambda_k)$$

$$\begin{aligned} \implies \dim W &= \dim \text{Eig}(\varphi, \lambda_1) + \dots + \dim \text{Eig}(\varphi, \lambda_k) \\ &= \mu_{\text{geo}}(\varphi, \lambda_1) + \dots + \mu_{\text{geo}}(\varphi, \lambda_k) \\ &= \mu_{\text{alg}}(\varphi, \lambda_1) + \dots + \mu_{\text{alg}}(\varphi, \lambda_k) = \deg(\chi_\varphi^{\text{char}}) \\ &= \dim V \end{aligned}$$

$$\implies W = V$$

3. \implies 1. Es gelte 3. Sei $\mathcal{B} = (v_1^{(i)}, \dots, v_{s_i}^{(i)})$ eine Basis von $\text{Eig} \varphi, \lambda_i \implies \mathcal{B} := (v_1^{(1)}, \dots, v_{s_1}^{(1)}, \dots, v_1^{(k)}, v_{s_r}^{(k)})$ ist eine Basis von V aus EV von $\varphi \implies \varphi$ diagonalisierbar. \square

Anmerkung In der Praxis ist es in der Regel schwierig festzustellen, ob $\chi_\varphi^{\text{char}}$ in Linearfaktoren zerfällt oder die NS von $\chi_\varphi^{\text{char}}$ zu bestimmen. Für Polynome von Grad ≥ 5 existiert keine Lösungsformel zur Bestimmung der NS. (Algebra 1 Vorlesung), die NS müssen numerisch bestimmt werden.

Beispiel 18.20

1. In 18.15.3 ist $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in M(2 \times 2, \mathbb{R})$ ist $\chi_A^{\text{char}} = (t-1)^2, \mu_{\text{geo}}(A, 1) = 1 < \mu_{\text{alg}}(A, 1) = 2 \implies A$ nicht diagonalisierbar.

2. $A = \begin{pmatrix} 2 & -1 & -1 \\ -6 & 1 & 2 \\ 3 & -1 & -2 \end{pmatrix} \in M(3 \times 3, \mathbb{R})$

$$\chi_A^{\text{char}} = \det \begin{pmatrix} t-2 & 1 & 1 \\ 6 & t-1 & -1 \\ -3 & 1 & t+2 \end{pmatrix} = t^3 - t^2 - 5t - 3 = (t+1)^2(t-3)$$

EW von A : $-1, 3, \mu_{alg} = (A, -1) = 2, \mu_{alg}(A, 3) = 1$

$$\text{Eig}(A, -1) = \text{Lös}(-E_n - A, 0) = \text{Lös}\left(\begin{pmatrix} -3 & 1 & 1 \\ 6 & -1 & -2 \\ -3 & 1 & 1 \end{pmatrix}, 0\right) = \text{Lin}\left(\begin{pmatrix} -1 \\ 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \\ 3 \end{pmatrix}\right)$$

$$\mu_{geo}(A, -1) = 2 = \mu_{alg}(A, -1).$$

$$\text{Eig}(A, 3) = \text{Lös}(3E_n - A, 0) = \text{Lös}\left(\begin{pmatrix} 1 & 1 & 1 \\ 6 & 2 & -2 \\ -3 & 1 & 5 \end{pmatrix}, 0\right) = \text{Lin}\left(\begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}\right)$$

$\mu_{geo}(A, 3) = 1 = \mu_{alg}(A, 3)$. Also ist A diagonalisierbar, $\mathcal{B} := \left(\begin{pmatrix} -1 \\ 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}\right)$ ist eine Basis des \mathbb{R}^3 aus EV von A ,

$$M_{\mathcal{B}}(\tilde{A}) = \begin{pmatrix} 1 & & 0 \\ & -1 & \\ 0 & & 3 \end{pmatrix}$$

Mit

$$S := \begin{pmatrix} -1 & 0 & 1 \\ 3 & -1 & -1 \\ 0 & 3 & 1 \end{pmatrix}^{-1}, SAS^{-1} = \begin{pmatrix} -1 & & 0 \\ & -1 & \\ 0 & & 3 \end{pmatrix}$$

Anmerkung Ist $f = a_m t^m + \dots + a_1 t + a_0 \in K[t]$, dann können wir in f :

- Endomorphismen $\varphi \in \text{End}_K(V)$ einsetzen durch die Regel

$$f(\varphi) := a_m \varphi^m + \dots + a_1 \varphi + a_0 \text{id}_V \in \text{End}_K(V)$$

wobei $\varphi^k := \underbrace{\varphi \circ \dots \circ \varphi}_{k\text{-mal}}$

- Matrizen $A \in M(n \times n, K)$ einsetzen durch die Regel

$$f(A) := a_m A^m + \dots + a_1 A + a_0 E_n \in M(n \times n, K)$$

Für $f, g \in K[t]$, $\varphi \in \text{End}_K(V)$ ist $f(\varphi) \circ g(\varphi) = (fg)(\varphi) = (gf)(\varphi) = g(\varphi) \circ f(\varphi)$, analog für Matrizen.

Satz 18.21 (Satz von Cayley-Hamilton) V endlichdimensional. Dann gilt: $\chi_{\varphi}^{char}(\varphi) = 0$. Insbesondere gilt für alle $A \in M(n \times n, K)$: $\chi_A^{char}(A) = 0$.

Beweis 1. Es genügt zu zeigen, dass $\chi_A^{char} = 0$ für alle $A \in M(n \times n, K)$, denn:

Ist $\varphi \in \text{End}_K(V)$, \mathcal{B} Basis von V , $A = A_{\mathcal{B}}$, $\chi_{\varphi}^{char} = t^n + a_{n-1}t^{n-1} + \dots + a_0 = \chi_A^{char} \in K[t]$

$$\begin{aligned} \implies 0 &= \chi_A^{char}(A) = A^n + a_{n-1}A^{n-1} + \dots + a_0 E_n = M_{\mathcal{B}}(\varphi^n + a_{n-1}\varphi^{n-1} + \dots + a_0 \text{id}_V) \\ &= M_{\mathcal{B}}(\chi_{\varphi}^{char}(\varphi)) \end{aligned}$$

$$\implies \chi_{\varphi}^{char}(\varphi) = 0$$

2. Sei $A \in M(n \times n, K)$. Wir setzen $D := (tE_n - A)^\# \in M(n \times n, K[t])$

$$\implies D(tE_n - A) = \det(tE_n - A)E_n = \chi_A^{char} E_n$$

Sei $D = \sum_{i=0}^{n-1} D_i t^i$ mit $D_i \in M(n \times n, K)$, $\chi_A^{char} = \sum_{i=0}^n a_i t^i$ mit $a_i \in K$

$$\begin{aligned} \implies \sum_{i=0}^n a_i E_n t^i &= \left(\sum_{i=0}^n a_i t^i \right) E_n = \chi_A^{char} E_n = D(tE_n - A) \\ &= \left(\sum_{i=0}^{n-1} D_i t^i \right) (tE_n - A) = \sum_{i=0}^{n-1} D_i t^{i+1} - \sum_{i=0}^{n-1} D_i A t^i \\ &= \sum_{i=0}^n (D_{i-1} - D_i A) t^i \quad (\text{mit } D_{-1} := 0, D_n := 0) \end{aligned}$$

Koeffizientenvergleich liefert: $a_i A_n = D_{i-1} - D_i A$ für $i = 0, \dots, n$

$$\begin{aligned} \chi_A^{char} &= \sum_{i=0}^n a_i A_i = \sum_{i=0}^n (a_i E_n) A^i = \sum_{i=0}^n (D_{i-1} - D_i A) A^i \\ &= (D_{-1} - D_0 A) + (D_0 - D_1 A) A + \dots + (D_{n-1} - D_n A) A^n \\ &= D_{-1} - D_n A^{n+1} = 0 \end{aligned} \quad \square$$

Anmerkung Der „Beweis“

$$\chi_A(A) = (\det(tE_n - A))(A) = \det(AE_n - A) = \det(A - A) = \det(0) = 0$$

funktioniert nicht, denn:

$$\underbrace{\underbrace{(\det(tE_n - A))(A)}_{\in K[t]}}_{\in M(n \times n, K)} \quad \underbrace{\underbrace{\det(AE_n - A)}_{\in M(n \times n, K)}}_{\in K}$$

Satz+Definition 18.22 V endlichdimensional, $I := \{f \in K[t] \mid f(\varphi) = 0\}$. Dann gilt:

1. Es gibt ein eindeutig bestimmtes, normiertes Polynom $\chi_\varphi^{min} \in K[t]$, sodass

$$I = \chi_\varphi^{min} K[t] := \{\chi_\varphi^{min} q \mid q \in K[t]\}$$

χ_φ^{min} heißt das **Minimalpolynom** von φ . χ_φ^{min} ist das eindeutig bestimmte normierte Polynom kleinsten Grades mit $f(\varphi) = 0$.

2. $\chi_\varphi^{mit} \mid \chi_\varphi^{char}$, das heißt $\exists q \in K[t] : \chi_\varphi^{char} = q \cdot \chi_\varphi^{min}$

Analog konstruiert man für $A \in M(n \times n, K)$, das Minimalpolynom χ_A^{min} . Es ist $\chi_A^{min} = \chi_A^{min}$.

Beweis 1. Existenz: Wegen Satz von Cayley-Hamilton ist $\chi_\varphi^{char}(\varphi) = 0$. Somit ist $\chi_\varphi^{char} \in I$, insbesondere $I \neq \emptyset$.

$\deg(f) \mid f \in I, f \neq 0$ ist eine nichtleere Teilmenge von \mathbb{N}_0 , hat somit ein minimales Element. $\implies \exists g \in I, g \neq 0 : \deg(g)$ minimal in $I \setminus \{0\}$ ist. Wir setzen

$$\chi_\varphi^{min} := \frac{1}{l(g)} g \implies \chi_\varphi^{min} \text{ normiert}$$

und es ist

$$\chi_{\varphi}^{\min}(\varphi) = \frac{1}{l(g)} g g(\varphi) = 0$$

das heißt $\chi_{\varphi}^{\min} \in I$.

Behauptung: $I = \chi_{\varphi}^{\min} K[t]$, denn:

„ \supseteq “ Für $q \in K[t]$ ist $(\chi_{\varphi}^{\min} q)(\varphi) = \underbrace{\chi_{\varphi}^{\min}(\varphi)}_{=0} \cdot g(\varphi) = 0$, das heißt $\chi_{\varphi}^{\min} q \in I$.

„ \subseteq “ Sei $f \in I \implies \exists q, r \in K[t] : f = q \chi_{\varphi}^{\min} + r, \deg(r) < \deg(\chi_{\varphi}^{\min})$

$$\implies 0 = f(\varphi) = (q \chi_{\varphi}^{\min} \varphi + r)(\varphi) = q(\varphi) \cdot \chi_{\varphi}^{\min}(\varphi) + r(\varphi) = r(\varphi) \implies r \in I$$

Wegen $\deg(r) < \deg(\chi_{\varphi}^{\min})$ und der Minimalität des Grades von χ_{φ}^{\min} in $I \setminus \{0\}$ folgt $r = 0 \implies f = q \chi_{\varphi}^{\min}$

Eindeutigkeit: Sei $\chi \in K[t]$ ein weiteres Polynom mit $I = \chi K[t] = \chi_{\varphi}^{\min} K[t]$

$$\implies \chi = \chi \cdot 1 \in I = \chi_{\varphi}^{\min} K[t] \implies \exists q \in K[t] : \chi = \chi_{\varphi}^{\min} q$$

Analog $\exists p \in K[t] : \chi_{\varphi}^{\min} = \chi p$

$$\implies \chi_{\varphi}^{\min} = \chi p = \chi_{\varphi}^{\min} q p \implies p q = 1 \implies p, q \in K^*$$

Wegen $\chi, \chi_{\varphi}^{\min}$ normiert folgt $p = q = 1$, also $\chi = \chi_{\varphi}^{\min}$

2. Wegen $\chi_{\varphi}^{\text{char}}(\varphi) = 0$ nach Satz von Cayley-Hamilton folgt $\chi_{\varphi}^{\text{char}} \in I$.

$$\implies \exists q \in K[t] : \chi_{\varphi}^{\text{char}} = q \chi_{\varphi}^{\min}$$

das heißt $\chi_{\varphi}^{\min} \mid \chi_{\varphi}^{\text{char}}$

□

Bemerkung 18.23 V endlichdimensional, $\lambda \in K$. Dann gilt:

$$\chi_{\varphi}^{\text{char}}(\lambda) = 0 \iff \chi_{\varphi}^{\min}(\lambda) = 0$$

Insbesondere haben $\chi_{\varphi}^{\text{char}}$ und χ_{φ}^{\min} dieselben NS.

Beweis „ \Leftarrow “ Sei $\chi_{\varphi}^{\min}(\lambda) = 0$. Nach 18.22 $\exists q \in K[t]$ mit $\chi_{\varphi}^{\text{char}} = q \chi_{\varphi}^{\min}$

$$\implies \chi_{\varphi}^{\text{char}}(\lambda) = q(\lambda) \underbrace{\chi_{\varphi}^{\min}(\lambda)}_{=0} = 0$$

„ \Rightarrow “ Sei $\chi_{\varphi}^{\text{char}}(\lambda) = 0 \implies \lambda$ ist EW von φ , sei $v \in V$ EV zum EW λ . Sei $\chi_{\varphi}^{\min} = t^r + a_{r-1}t^{r-1} + \dots + a_1t + a_0$

$$\begin{aligned} \implies 0 &= (\chi_{\varphi}^{\min}(\varphi))(v) = (\varphi^r + a_{r-1}\varphi^{r-1} + \dots + a_1\varphi + a_0 \text{id}_V)(v) \\ &= \lambda^r v + a_{r-1}\lambda^{r-1}v + \dots + a_1\lambda v + a_0v \\ &= \underbrace{(\lambda^r + a_{r-1}\lambda^{r-1} + \dots + a_1\lambda + a_0)}_{=\chi_{\varphi}^{\min}(\lambda)} v \end{aligned}$$

$$\implies \chi_{\varphi}^{\min}(\lambda) = 0.$$

□

Beispiel 18.24

1. $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M(2 \times 2, \mathbb{Q})$, $\chi_A^{char} = (t-1)^2$ Wegen 18.22, 18.23 gilt: χ_A^{min} normiert, $\chi_A^{min} \mid \chi_A^{char}$, $\chi_A^{char}(1) = 0 \implies \chi_A^{min} \in \{t-1, (t-1)^2\}$ Wegen $A - E_2 = 0$ ist $\chi_A^{min} = t-1$

2. $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in M(2 \times 2, \mathbb{Q}) \implies \chi_A^{char} = (t-1)(t+1) \implies \chi_A^{min} = (t-1)(t+1)$

3. $A = \begin{pmatrix} 1 & -1 & 0 \\ -8 & 1 & 4 \\ 2 & -1 & -1 \end{pmatrix} \in M(3 \times 3, \mathbb{R})$

$$\implies \chi_A^{char} = (t+1)^2(t-3) \implies \chi_A^{min} = \{(t+1)(t-3), (t+1)^2(t-3)\}$$

Es ist $(A + E_n)(A - 3E_n) \neq 0$, also ist $\chi_A^{min} = (t+1)^2(t-3)$

4. $A = \begin{pmatrix} 2 & -1 & -1 \\ -6 & 1 & 2 \\ 3 & -1 & -2 \end{pmatrix} \in M(3 \times 3, \mathbb{R}) \implies \chi_A^{char} = (t+1)^2(t-3)$

$$\chi_A^{min} \in \{(t+1)(t-3), (t+1)^2(t-3)\}$$

Es ist $(A + E_n)(A - 3E_n) = 0 \implies \chi_A^{min} = (t+1)(t-3)$

Satz 18.25 V endlichdimensional. Dann sind äquivalent:

1. φ diagonalisierbar
2. Das Minimalpolynom χ_φ^{min} zerfällt in Linearfaktoren und besitzt nur einfache NS, das heißt $\chi_\varphi^{min} = (t - \lambda_1) \cdot \dots \cdot (t - \lambda_r)$ mit paarweise verschiedenen $\lambda_1, \dots, \lambda_r \in K$

Beweis 1. \implies 2. Sei φ diagonalisierbar, seinen $\lambda_1, \dots, \lambda_r$ die verschiedenen EW von φ . Sei $v \in V$. Da φ diagonalisierbar, ist $V = \bigoplus_{i=1}^r \text{Eig}(\varphi, \lambda_i)$ nach 18.19, das heißt es existieren $v_i \in \text{Eig}(\varphi, \lambda_i)$, $i = 1, \dots, r$ mit $v = v_1 + \dots + v_r$

$$\begin{aligned} \implies (\varphi - \lambda_r \text{id}_V)(V) &= \varphi(v_1) + \dots + \varphi(v_r) - \lambda_r v_1 - \dots - \lambda_r v_r \\ &= \lambda_1 v_1 + \dots + \lambda_r v_r - \lambda_r v_1 - \dots - \lambda_r v_r \\ &= (\lambda_1 - \lambda_r) v_1 + \dots + (\lambda_{r-1} - \lambda_r) v_{r-1} \\ &\in \text{Eig}(\varphi, \lambda_1) \oplus \dots \oplus \text{Eig}(\varphi, \lambda_{r-1}) \end{aligned}$$

analog:

$$(\varphi - \lambda_{r-1} \text{id}_V) \circ (\varphi - \lambda_r \text{id}_V)(v) \in \text{Eig}(\varphi, \lambda_1) \oplus \dots \oplus \text{Eig}(\varphi, \lambda_{r-2})$$

Induktiv erhalten wir:

$$\begin{aligned} 0 &= (\varphi - \lambda_1 \text{id}_V) \circ (\varphi - \lambda_2 \text{id}_V) \circ \dots \circ (\varphi - \lambda_r \text{id}_V)(V) \\ \implies 0 &= (\varphi - \lambda_1 \text{id}_V) \circ \dots \circ (\varphi - \lambda_r \text{id}_V) \\ \implies 0 &= ((t - \lambda_1) \cdot \dots \cdot (t - \lambda_r))(\varphi) \end{aligned}$$

\implies Es existiert $g \in K[t]$ mit $(t - \lambda_1) \cdot \dots \cdot (t - \lambda_r) = g \chi_\varphi^{min}$. Wegen $\chi_\varphi^{min}(\lambda_1) = \dots = \chi_\varphi^{min}(\lambda_r) = 0$ nach 18.23 existiert $h \in K[t]$ mit

$$\chi_\varphi^{min} = (t - \lambda_1) \cdot \dots \cdot (t - \lambda_r) h = g \chi_\varphi^{min} h = g h \chi_\varphi^{min} \implies g h = 1$$

$$\implies g, h \in K^*, \chi_\varphi^{min} \text{ normiert} \implies g = h = 1 \implies \chi_\varphi^{min} = (t - \lambda_1) \cdot \dots \cdot (t - \lambda_r)$$

2. \implies 1. Sei $\chi_\varphi^{\min} = (t - \lambda_1) \cdot \dots \cdot (t - \lambda_r)$, wobei $\lambda_1, \dots, \lambda_r \in K$ paarweise verschieden. Nach 18.23 sind $\lambda_1, \dots, \lambda_r$ die EW von φ . Beweis der Behauptung per Induktion nach $n := \dim V$

IA: $n = 1$ klar

IS: Sei $n > 1$, die Behauptung sei für $1, \dots, n-1$ gezeigt.

a) Behauptung: $V = \ker(\varphi - \lambda_1 \operatorname{id}_V) \oplus \operatorname{im}(\varphi - \lambda_1 \operatorname{id}_V)$, denn: Nach 7.6 $\exists v, s \in K[t]$ mit

$$(t - \lambda_2) \cdot \dots \cdot (t - \lambda_r) = q(t - \lambda_1) + s, \deg(s) < \deg(t - \lambda_1) = 1$$

das heißt s ist konstantes Polynom. Wegen

$$s(\lambda_1) = (\lambda_1 - \lambda_2) \cdot \dots \cdot (\lambda_1 - \lambda_r) - \underbrace{q(\lambda_1)(\lambda_1 - \lambda_1)}_{=0} \neq 0$$

das heißt $s \in K^*$. Einsetzen von φ liefert:

$$(\varphi - \lambda_2 \operatorname{id}_V) \circ \dots \circ (\varphi - \lambda_r \operatorname{id}_V) = q(\varphi) \circ (\varphi - \lambda_1 \operatorname{id}_V) + s \operatorname{id}_V$$

$\implies \forall v \in V$ ist

$$sv = (\varphi - \lambda_2 \operatorname{id}_V) \circ \dots \circ (\varphi - \lambda_r \operatorname{id}_V)(v) - q(\varphi) \circ (\varphi - \lambda_1 \operatorname{id}_V)(v)$$

$$\implies v = \frac{1}{s} \underbrace{(\varphi - \lambda_2 \operatorname{id}_V) \circ \dots \circ (\varphi - \lambda_r \operatorname{id}_V)(v)}_{=:u} - \underbrace{q(\varphi) \circ (\varphi - \lambda_1 \operatorname{id}_V)(v)}_{=:w}$$

$$(\varphi - \lambda_1 \operatorname{id}_V)(u) = \frac{1}{s} (\varphi - \lambda_1 \operatorname{id}_V) \circ \dots \circ (\varphi - \lambda_r \operatorname{id}_V)(v) = \frac{1}{s} \underbrace{\chi_\varphi^{\min}(\varphi)(v)}_{=0} = 0$$

$$\implies u \in \ker(\varphi - \lambda_1 \operatorname{id}_V)$$

$$w = \frac{1}{s} q(\varphi) \circ (\varphi - \lambda_1 \operatorname{id}_V)(v) = \frac{1}{s} ((\varphi - \lambda_1 \operatorname{id}_V) \circ q(\varphi))(v) \in \operatorname{im}(\varphi - \lambda_1 \operatorname{id}_V)$$

$$\implies V = \ker(\varphi - \lambda_1 \operatorname{id}_V) + \operatorname{im}(\varphi - \lambda_1 \operatorname{id}_V)$$

Nach der Dimensionsformel für lineare Abbildungen ist

$$\dim \ker(\varphi - \lambda_1 \operatorname{id}_V) + \dim \operatorname{im}(\varphi - \lambda_1 \operatorname{id}_V) = \dim V$$

\implies Summe ist direkt \implies Behauptung.

b) Wir setzen $W := \operatorname{im}(\varphi - \lambda_1 \operatorname{id}_V)$, dann ist

$$V = \ker(\varphi - \lambda_1 \operatorname{id}_V) \oplus W = \underbrace{\operatorname{Eig}(\varphi, \lambda_1)}_{\neq 0} \oplus W$$

$\implies \dim W < \dim V$. Es gilt:

$$\varphi \circ (\varphi - \lambda_1 \operatorname{id}_V) = \varphi \circ \varphi - \lambda_1 \varphi = (\varphi - \lambda_1 \operatorname{id}_V) \circ \varphi$$

$$\implies \varphi(W) = \varphi((\varphi - \lambda_1 \operatorname{id}_V)(V)) = (\varphi - \lambda_1 \operatorname{id}_V)(\varphi(V)) \leq (\varphi - \lambda_1 \operatorname{id}_V)(V) = W$$

Wir betrachten die Abbildung $\psi := \varphi|_W^W : W \rightarrow W$. Sei $\chi_\varphi^{\min} = t^n + a_{n-1}t^{n-1} + \dots + a_0$.

$\implies \forall w \in W$ ist

$$\begin{aligned} \chi_\varphi^{\min}(\psi)(w) &= (\psi^n + a_{n-1}\psi^{n-1} + \dots + a_0 \operatorname{id}_W)(w) \\ &= \psi^n(w) + a_{n-1}\psi^{n-1}(w) + \dots + a_0 w \\ &= \varphi^n(w) + a_{n-1}\varphi^{n-1}(w) + \dots + a_0 w \\ &= (\varphi^n + a_{n-1}\varphi^{n-1} + \dots + a_0 \operatorname{id}_V)(w) \\ &= \underbrace{(\chi_\varphi^{\min}(\varphi))}_{=0}(w) = 0 \end{aligned}$$

$$\implies \chi_\varphi^{\min} \psi = 0 \implies \chi_\psi^{\min} \mid \chi_\varphi^{\min} = (t - \lambda_1) \cdot \dots \cdot (t - \lambda_r)$$

$\implies \chi_\psi^{\min}$ zerfällt in Linearfaktoren und besitzt nur einfache Nullstellen. $\implies \psi$ diagonalisierbar, das heißt es existiert eine Basis von W aus EV zu $\psi = \varphi|_W$. Wegen $V = \text{Eig}(\varphi, \lambda_1) \oplus W$ existiert nach 11.8 eine Basis von V aus EV zu φ , das heißt φ ist diagonalisierbar. \square

Beispiel 18.26 1. $A = \begin{pmatrix} 1 & -1 & 0 \\ -8 & 1 & 4 \\ 2 & -1 & -1 \end{pmatrix} \in M(3 \times 3, \mathbb{R})$. Es ist $\chi_A^{\min} = (t+1)^2(t-3) \implies A$ ist nicht diagonalisierbar.

2. $A = \begin{pmatrix} 2 & -1 & -1 \\ -6 & 1 & 2 \\ 3 & -1 & -2 \end{pmatrix} \in M(3 \times 3, \mathbb{R})$. Es ist $\chi_A^{\min} = (t+1)(t-3) \implies A$ ist diagonalisierbar.

19 Dualraum

In diesem Abschnitt sei V ein K Vektorraum.

Definition 19.1 (Dualraum)

$$V^* := \text{Hom}_K(V, K) = \{\varphi : V \rightarrow K \mid \varphi \text{ linear}\}$$

heißt der **Dualraum** von V , die Elemente aus V^* heißen **Linearformen** auf V .

Beispiel 19.2

1. $K = \mathbb{R}, V = \mathbb{R}^n, \varphi : \mathbb{R}^n \rightarrow \mathbb{R}, \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto x_1$ ist eine Linearform auf \mathbb{R}^n .

2. $K = \mathbb{R}, V = C[0, 1] = \{f : [0, 1] \rightarrow \mathbb{R} \mid f \text{ stetig}\}$

$$\varphi : C[0, 1] \rightarrow \mathbb{R}, f \mapsto \int_0^1 f(t) dt$$

ist eine Linearform auf $C[0, 1]$

Bemerkung+Definition 19.3 V endlichdimensional $\mathcal{B} = (v_1, \dots, v_n)$ Basis von V . Wir definieren für $i = 1, \dots, n$ die linear Abbildung

$$v_i^* : V \rightarrow K, v_j \mapsto \delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

Dann ist $\mathcal{B}^* := (v_1^*, \dots, v_n^*)$ ist eine Basis von V^* , die **duale Basis** zu \mathcal{B} .

Beweis 1. \mathcal{B}^* ist linear unabhängig: Seien $\lambda_1, \dots, \lambda_n \in K, \lambda_1 v_1^* + \dots + \lambda_n v_n^* = 0$. $\implies \forall i \in \{1, \dots, n\}$ ist

$$0 = \underbrace{\lambda_1 v_1^*(v_i)}_{=0} + \dots + \underbrace{\lambda_{i-1} v_{i-1}^*(v_i)}_{=0} + \underbrace{\lambda_i v_i^*(v_i)}_{=1} + \underbrace{\lambda_{i+1} v_{i+1}^*(v_i)}_{=0} + \dots + \underbrace{\lambda_n v_n^*(v_i)}_{=0} = \lambda_i$$

2. \mathcal{B}^* ist ES von V^* : Sei $\varphi \in V^*$. Setze $\lambda_i := \varphi(v_i)$ für $i = 1, \dots, n$

$$\implies (\lambda_1 v_1^* + \dots + \lambda_n v_n^*)(v_i) = \lambda_i = \varphi(v_i), i = 1, \dots, n$$

$$\implies \varphi = \lambda_1 v_1^* + \dots + \lambda_n v_n^*$$

\square

Anmerkung Ist V unendlichdimensional mit Basis $(v_i)_{i \in I}$, dann ist $(v_i^*)_{i \in I}$ (analog definiert) linear unabhängig, aber kein ES von V .

Notation:

Elemente des K^n schreiben wir im Folgenden als Spaltenvektoren. Ist $\varphi \in (K^n)^* = \text{Hom}_K(K^n, K)$, dann existiert nach LA1 ein eindeutig bestimmtes $A = (a_1 \ \dots \ a_n) \in M(1 \times n, K)$ mit

$$\varphi = \tilde{A} : K^n \rightarrow K, x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto (a_1 \ \dots \ a_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

Es ist $A = M_{(e_1)}^{(e_1, \dots, e_n)}(\varphi)$. Dementsprechende schreiben wir Elemente von $(K^n)^*$ als Zeilenvektoren.

Beispiel 19.4

1. $V = K^n, \mathcal{B} = (e_1, \dots, e_n) \implies \mathcal{B}^* = (e_1^*, \dots, e_n^*)$ duale Basis zu \mathcal{B} mit

$$e_i^* = (0, \dots, 0, 1, 0, \dots, 0)$$

Für die Abbildung aus 19.2.1 gilt $\varphi = e_1^* = (1, \dots, 0)$.

2. $K = \mathbb{R}, V = \mathbb{R}^2, \mathcal{B} = (v_1, v_2), v_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, v_2 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Es ist $e_1 = v_1, e_2 = v_2 - v_1$

$$\implies v_1^*(e_1) = v_1^*(v_1) = 1, v_1^*(e_2) = v_1^*(v_2 - v_1) = \underbrace{v_1^*(v_2)}_{=0} - \underbrace{v_1^*(v_1)}_{=1} = -1$$

$$\implies v_1^* = (1, -1)$$

$$\implies v_2^*(e_1) = v_2^*(v_1) = 0, v_2^*(e_2) = v_2^*(v_2 - v_1) = \underbrace{v_2^*(v_2)}_{=1} - \underbrace{v_2^*(v_1)}_{=0} = 1$$

$$\implies v_2^* = (0, 1)$$

Folgerung 19.5 V endlichdimensional, $v \in V, v \neq 0$. Dann existiert $\varphi \in V^*$ mit $\varphi(v) \neq 0$

Beweis Ergänze die linear unabhängige Familie (v) zu einer Basis (v, v_2, \dots, v_n) von V . Dann ist $(v^*, v_2^*, \dots, v_n^*)$ eine Basis von V^* , und es ist $v^*v = 1 \neq 0$. \square

Anmerkung Die Aussage gilt auch ohne die Voraussetzung „ V endlichdimensional.“

Folgerung 19.6 V endlichdimensional, $\mathcal{B} = (v_1, \dots, v_n)$ Basis von $V, \mathcal{B}^* = (v_1^*, \dots, v_n^*)$ duale Basis zu \mathcal{B} . Dann gibt es einen Isomorphismus

$$\psi_{\mathcal{B}} : V \rightarrow V^*, v_i \mapsto v_i \mapsto v_i^* \quad (i = 1, \dots, n)$$

Insbesondere ist $\dim V = \dim V^*$

Beweis folgt direkt aus 19.3 \square

Bemerkung+Definition 19.7 $U \subseteq V$ UVR

$$U^0 := \{\varphi \in V^* \mid \varphi(u) = 0 \forall u \in U\} \subseteq V^*$$

heißt der Annulator von U . U^0 ist ein UVR von V^* .

Beweis leicht nachzurechnen. \square

Satz 19.8 V endlichdimensional, $U \subseteq V$ UVR, (u_1, \dots, u_k) von U , $\mathcal{B} = (u_1, \dots, u_k, v_1, \dots, v_r)$ Basis von V . Dann ist die Teilfamilie (v_1^*, \dots, v_r^*) von \mathcal{B}^* eine Basis von U^0 . Insbesondere ist $\dim U^0 = \dim V - \dim U$.

Beweis 1. (v_1^*, \dots, v_r^*) linear unabhängig, da Teilfamilie der Basis \mathcal{B}^* von V^*

2. $\text{Lin}((v_1^*, \dots, v_r^*)) = U^0$

„ \subseteq “ $\varphi \in \text{Lin}((v_1^*, \dots, v_r^*)) \implies$ Es existieren $\lambda_1, \dots, \lambda_r \in K$ mit $\varphi = \lambda_1 v_1^* + \dots + \lambda_r v_r^* \implies$ Für $i = 1, \dots, k$ ist $\varphi(u_i) = \lambda_1 v_1^*(u_i) + \dots + \lambda_r v_r^*(u_i) = 0 \implies \varphi(u) = 0 \forall u \in U$
 „ \supseteq “ Sei $\varphi \in U^0$. Es existieren $\mu_1, \dots, \mu_k, \lambda_1, \dots, \lambda_r \in K$ mit $\varphi = \mu_1 u_1^* + \dots + \mu_k u_k^* + \lambda_1 v_1^* + \dots + \lambda_r v_r^* \implies$ Für $i = 1, \dots, k$ ist $0 = \varphi(u_i) = \mu_i \implies \varphi \in \text{Lin}((v_1^*, \dots, v_r^*))$ \square

Bemerkung+Definition 19.9 V, W K-VR, $f : V \rightarrow W$ lineare Abbildung. Wir definieren $f^* : W^* \rightarrow V^*$, $\psi \mapsto f^*(\psi) := \psi \circ f$ f^* heißt die zu f duale **Abbildung**. Es gilt: f^* ist linear.

Beweis • f^* ist wohldefiniert, da $f^*(\psi) = \psi \circ f \in V^* \forall \psi \in W^*$.

• f^* ist linear, denn: Seien $\varphi, \psi \in W^*, \lambda \in K$

$$\implies f^*(\varphi + \psi) = (\varphi + \psi) \circ f = \varphi \circ f + \psi \circ f = f^*(\varphi) + f^*(\psi)$$

$$f^*(\lambda\varphi) = \lambda f^*(\varphi) \text{ analog.}$$

\square

Bemerkung 19.10 V, W endlichdimensionaler K-VR. Dann ist die Abbildung

$$* : \text{Hom}_K(V, W) \rightarrow \text{Hom}_K(W^*, V^*), f \mapsto f^*$$

ist ein Isomorphismus von K-VR.

Beweis 1. $*$ ist linear: Seien $f, g \in \text{Hom}_K(V, W), \psi \in W^*$

$$\implies (f + g)^*(\psi) = \psi \circ (f + g) = \psi \circ f + \psi \circ g = f^*(\psi) + g^*(\psi) \implies (f + g)^* = f^* + g^*$$

Rest analog.

2. $*$ ist injektiv: Sei $f \in \text{Hom}_K(V, W)$ mit $f^* = 0 \implies \psi \circ f = 0 \forall \psi \in W^*$. Annahme: $f \neq 0 \implies \exists v \in V : f(v) \neq 0 \implies \exists \varphi \in W^* : \varphi(f(v)) \neq 0 \implies \varphi \circ f \neq 0$

3. $*$ ist surjektiv: Es ist $\dim \text{Hom}_K(V, W) = \dim(V) \dim(W) = \dim(V^*) \dim(W^*) = \dim \text{Hom}_K(W^*, V^*) \implies *$ surjektiv. \square

Satz 19.11 (19.11) V, W endlichdimensionale K-VR, \mathcal{A}, \mathcal{B} Basen von V beziehungsweise W , $f : V \rightarrow W$ lineare Abbildung. Dann gilt:

$$M_{\mathcal{A}^*}^{\mathcal{B}^*}(f^*) = (M_{\mathcal{B}}^{\mathcal{A}}(f))^T$$

Beweis Sei $\mathcal{A} = (v_1, \dots, v_n), \mathcal{B} = (w_1, \dots, w_m), M_{\mathcal{B}}^{\mathcal{A}}(f) = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ insbesondere

$$f(v_j) = \sum_{i=1}^m a_{ij} w_i$$

$$\implies a_{ij} = w_i^*(f(v_j)) = (w_i^* \circ f)(v_j) = f^*(w_i^*)(v_j)$$

Sei $M_{\mathcal{A}^*}^{\mathcal{B}^*}(f^*) = (b_{ij})_{\substack{1 \leq j \leq n \\ 1 \leq i \leq m}}$, dann ist

$$\begin{aligned} f^*(w_i^*) &= \sum_{j=1}^n b_{ji} v_j^* \\ \implies b_{ji} &= (f^*(w_i^*))(v_j) = a_{ij} \end{aligned} \quad \square$$

Satz 19.12 V, W endlichdimensionale K -VR, $f : V \rightarrow W$ lineare Abbildung. Dann gilt:

1. $\text{im}(f^*) = \text{ker}(f)^0$
2. $\text{ker}(f^*) = \text{im}(f)^0$

Beweis 1. „ \subseteq “ Sei $\varphi \in \text{im}(f^*) \subseteq V^* \implies \exists \psi \in W^* : f^*(\psi) = \varphi$, das heißt $\psi \circ f = \varphi$. $\implies \varphi|_{\text{ker } f} = 0 \implies \varphi \in (\text{ker } f)^0$ „ \supseteq “ Sei $\varphi \in (\text{ker } f)^0 \subseteq V^*$, das heißt $\varphi|_{\text{ker } f} = 0$. Zu zeigen: Es existiert ein $\psi \in W^*$ mit $\varphi = f^*(\psi) = \psi \circ f$. Sei (v_1, \dots, v_k) eine Basis von $\text{ker } f$, (w_1, \dots, w_r) eine Basis von $\text{im } f$, $u_i \in f^{-1}(\{w_i\})$, $i = 1, \dots, r \implies (v_1, \dots, v_k, u_1, \dots, u_r)$ Basis von V . Wir ergänzen (w_1, \dots, w_r) zu einer Basis $w_1, \dots, w_r, v_{r+1}, \dots, w_m$ von W . \implies Es existiert genau eine lineare Abbildung $\psi : W \rightarrow K$ mit

$$\psi(w_i) = \begin{cases} \varphi(u_i) & i = 1, \dots, r \\ 0 & i = r+1, \dots, m \end{cases}$$

Für $i = 1, \dots, r$ ist $\varphi(u_i) = \psi(w_i) = \psi(f(u_i)) = (\psi \circ f)(u_i)$, und für $i = 1, \dots, k$ ist $\varphi(v_i) = 0 = \psi(f(v_i))$. Also: $\varphi = \psi \circ f = f^*(\psi)$, das heißt $\varphi \in \text{im } f^*$

$$\begin{aligned} 2. \varphi \in \text{ker}(f^*) &\iff f^*(\varphi) = 0 \iff \varphi \circ f = 0 \iff \varphi(f(v)) = 0 \forall v \in V \iff \varphi|_{\text{im } f} = 0 \iff \\ &\varphi \in (\text{im } f)^0 \end{aligned} \quad \square$$

Folgerung 19.13 V, W endlichdimensionale K -VR, $f : V \rightarrow W$ lineare Abbildung. Dann gilt:

$$\text{Rang}(f^*) = \text{Rang}(f)$$

Beweis $\text{Rang } f^* = \dim \text{im } f^* = \dim(\text{ker } f)^0 = \dim V - \dim \text{ker } f = \dim \text{im } f = \text{Rang}(f) \quad \square$

Folgerung 19.14 $A \in M(m \times n, K)$. Dann gilt:

$$\text{Zeilenrang}(A) = \text{Spaltenrang}(A)$$

Beweis Es ist $A = M_{(e_1, \dots, e_m)}^{(e_1^*, \dots, e_n^*)}(\tilde{A})$, $A^T = M_{(e_1^*, \dots, e_n^*)}^{(e_1, \dots, e_m)}(\tilde{A}^*)$

$$\text{Spaltenrang}(A) = \dim \text{im } \tilde{A} = \text{Rang } \tilde{A} = \text{Rang}(\tilde{A}^*) = \text{Spaltenrang}(A^T) = \text{Zeilenrang}(A) \quad \square$$

Definition 19.15 $V^{**} := (V^*)^* = \text{Hom}_K(V^*, K)$ heißt der Bidualraum von V .

Satz 19.16 V endlichdimensional. Dann gibt es einen kanonischen (das heißt basisunabhängigen) Isomorphismus

$$i : V \rightarrow V^{**}, v \mapsto i_v, i_v : V^* \rightarrow K, \varphi \mapsto \varphi(v)$$

Beweis 1. i wohldefinier und linear: leicht nachzurechnen.

2. i injektiv: Sei $v \in \ker i \implies i_v = 0 \implies \forall \varphi \in V^* = \text{Hom}_K(V, K) : \varphi(v) = 0 \implies v = 0$

3. $\dim V^{**} = \dim V^* = \dim V$. Somit nach 12.15: i Isomorphismus \square

Anmerkung • Im Gegensatz zu $\psi_B : V \rightarrow V^*$ ist der Isomorphismus $i : V \rightarrow V^{**}$ unabhängig von der Wahl einer Basis, das heißt V und V^* sind unkanonisch isomorph, V und V^{**} sind kanonisch isomorph (für V endlichdimensional).

• Ist V unendlichdimensional, dann liefert i zumindest noch eine kanonische Inklusion von V nach V^{**} . Diese ist jedoch nicht surjektiv.

20 Bilinearformen

In diesem Abschnitt sei V stets ein K -VR.

Definition 20.1 $\gamma : V \times V \rightarrow K$ heißt eine Bilinearform auf V , genau dann wenn die folgenden Bedingungen erfüllt sind:

- (B1) $\gamma(v_1 + v_2, w) = \gamma(v_1, w) + \gamma(v_2, w), \gamma(\lambda v, w) = \lambda \gamma(v, w)$
- (B2) $\gamma(v, w_1 + w_2) = \gamma(v, w_1) + \gamma(v, w_2), \gamma(v, \lambda w) = \lambda \gamma(v, w)$

$\forall v, w, v_1, v_2, w_1, w_2 \in V, \lambda \in K$.

Beispiel 20.2

1. $K = \mathbb{R}, V = \mathbb{R}^n, \gamma : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}, \gamma\left(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}\right) = x_1 y_1 + \cdots + x_n y_n$ ist eine Bilinearform auf \mathbb{R}^n .
2. $K = \mathbb{R}, V = l[0, 1], \gamma : l[0, 1] \times l[0, 1] \rightarrow \mathbb{R}, \gamma(f, g) := \int_0^1 f(t)g(t)dt$ ist eine Bilinearform auf $l[0, 1]$.
3. $K = \mathbb{R}, V = \mathbb{R}^2, \gamma : \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}, \gamma\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}\right) = x_1 y_1 + 2x_1 y_2 - x_2 y_2$ ist eine Bilinearform auf \mathbb{R}^2 .

Definition 20.3 V endlichdimensional, $\mathcal{B} = (v_1, \dots, v_n)$ Basis von V , γ Bilinearform auf V

$$M_{\mathcal{B}}(\gamma) = (\gamma(v_i, v_j))_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} \in M(n \times n, K)$$

heißt die **Darstellungsmatrix (Fundamentalmatrix)** von γ bezüglich \mathcal{B} .

Beispiel 20.4

1. In 20.2a ist für $\mathcal{B} = (e_1, \dots, e_n) : M_{\mathcal{B}}(\gamma) = E_n$
2. In 20.2p ist für $\mathcal{B} = (e_1, e_2) : M_{\mathcal{B}}(\gamma) = \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}$

Bemerkung 20.5 V endlichdimensional, $\mathcal{B} = (v_1, \dots, v_n)$ Basis von V , γ Bilinearform auf V , $A = M_{\mathcal{B}}(\gamma)$, $\Phi_{\mathcal{B}} : K^n \rightarrow V$ Koordinatensystem zu \mathcal{B} , $v, w \in V$, $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \Phi_{\mathcal{B}}^{-1}(v)$, das heißt $v = x_1 v_1 + \dots + x_n v_n$,

$$y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \Phi_{\mathcal{B}}^{-1}(w)$$

das heißt $w = y_1 v_1 + \dots + y_n v_n$. Dann gilt:

$$\gamma(v, w) = \Phi_{\mathcal{B}^{-1}}^T A \Phi_{\mathcal{B}}^{-1}(w) = x^T A y = \begin{pmatrix} x_1 & \dots & x_n \end{pmatrix} A \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

Beweis Es ist

$$\begin{aligned} \gamma(v, w) &= \gamma(x_1 v_1 + \dots + x_n v_n, y_1 v_1 + \dots + y_n v_n) = \sum_{i=1}^n \sum_{j=1}^n x_i y_j \gamma(v_i, v_j) \\ &= \sum_{i=1}^n x_i \sum_{j=1}^n \gamma(v_i, v_j) y_j = x^T A y \end{aligned} \quad \square$$

Bemerkung 20.6 V endlichdimensional, $\mathcal{B} = (v_1, \dots, v_n)$ Basis von V , $A \in M(n \times n, K)$. Dann gilt: Durch

$$\Delta_{\mathcal{B}}^A : V \times V \rightarrow K, (v, w) \mapsto \Phi_{\mathcal{B}}^{-1}(v)^T A \Phi_{\mathcal{B}}^{-1}(w)$$

ist eine Bilinearform auf V gegeben.

Beweis Nachrechnen. □

Beispiel 20.7 (wichtiger Spezialfall von 20.6)

$V = K^n$, $\mathcal{B} = (e_1, \dots, e_n)$, $A \in M(n \times n, K) \implies \Phi_{\mathcal{B}} = \text{id}_{K^n}$. Durch

$$\Delta_A^{(e_1, \dots, e_n)} : K^n \times K^n \rightarrow K, (v, w) \mapsto v^t A w$$

ist eine Bilinearform auf K^n gegeben. Wir setzen kurz $\Delta(A) := \Delta_A := \Delta_A^{(e_1, \dots, e_n)}$

Bemerkung+Definition 20.8 $\text{Bil}(V) := \{\gamma : V \times V \rightarrow K \mid \gamma \text{ ist Bilinearform}\}$ ist ein K -VR, ist ein UVR vom K -VR $\text{Abb}(V \times V, K)$

Bemerkung 20.9 V endlichdimensional, $\mathcal{B} = (v_1, \dots, v_n)$ Basis von V . Dann gilt: Die Abbildung

$$M_{\mathcal{B}} : \text{Bil}(V) \rightarrow M(n \times n, K)$$

ist ein Isomorphismus von K -VR mit Umkehrabbildung

$$\Delta^{\mathcal{B}} : M(n \times n, K) \rightarrow \text{Bil}(V), A \mapsto \Delta_A^{\mathcal{B}}$$

Beweis 1. $M_{\mathcal{B}}$ linear: nachrechnen.

2. $\Delta^{\mathcal{B}} \circ M_{\mathcal{B}} = \text{id}_{\text{Bil}(V)}$, denn: Sei $\gamma \in \text{Bil}(V)$

$$\begin{aligned} \implies (\Delta^{\mathcal{B}} \circ M_{\mathcal{B}})(\gamma)(v_i, v_j) &= \Delta_{M_{\mathcal{B}}(\gamma)}^{\mathcal{B}}(v_i, v_j) = \Phi_{\mathcal{B}}^{-v}(v_1)^t M_{\mathcal{B}}(\gamma) \Phi_{\mathcal{B}}^{-1}(v_j) \\ &= e_i^T M_{\mathcal{B}}(\gamma) e_j = \gamma(v_i, v_j) \end{aligned}$$

3. $M_{\mathcal{B}} \circ \Delta^{\mathcal{B}} = \text{id}_{M(n \times n, K)}$, denn: Sei $A = (a_{ij}) \in M(n \times n, K)$, $B = (b_{ij}) = (M_{\mathcal{B}} \circ \Delta^{\mathcal{B}})(A) = M_{\mathcal{B}} \circ \Delta_A^{\mathcal{B}}$

$$b_{ij} = \Delta_A^{\mathcal{B}}(v_i, v_j) = \Phi_{\mathcal{B}}^{-1}(v_i)^T A \Phi_{\mathcal{B}}(v_j) = e_i^T A e_j = a_{ij}$$

$$\implies B = A$$

□

Satz 20.10 V endlichdimensional, \mathcal{A}, \mathcal{B} Basen von V , γ Bilinearform auf V . Dann gilt:

$$M_{\mathcal{B}}(\gamma) = (T_{\mathcal{A}}^{\mathcal{B}})^T M_{\mathcal{A}}(\gamma) T_{\mathcal{A}}^{\mathcal{B}}$$

Beweis Für $v, w \in V$ ist

$$\Phi_{\mathcal{B}}^{-1}(v)^T M_{\mathcal{B}}(w) = \gamma(v, w) = \Phi_{\mathcal{A}}^{-1}(v)^T M_{\mathcal{A}}(\gamma) \Phi_{\mathcal{A}}^{-1}(w)$$

$$16.2.2: \tilde{T}_{\mathcal{A}}^{\mathcal{B}} = \Phi_{\mathcal{A}}^{-1} \circ \Phi_{\mathcal{B}}$$

$$= (T_{\mathcal{A}}^{\mathcal{B}} \Phi_{\mathcal{B}}^{-1}(v))^T M_{\mathcal{A}}(\gamma) T_{\mathcal{A}}^{\mathcal{B}} \Phi_{\mathcal{B}}^{-1}(w)$$

$$= (\Phi_{\mathcal{B}}^{-1})^T (T_{\mathcal{A}}^{\mathcal{B}})^T M_{\mathcal{A}}(\gamma) T_{\mathcal{A}}^{\mathcal{B}} \Phi_{\mathcal{B}}^{-1}(w)$$

$$\implies \Delta^{\mathcal{B}}(M_{\mathcal{B}}(\gamma))(v, w) = \Delta^{\mathcal{B}}\left((T_{\mathcal{A}}^{\mathcal{B}})^T M_{\mathcal{A}}(\gamma) T_{\mathcal{A}}^{\mathcal{B}}\right)(v, w)$$

$$\implies \Delta^{\mathcal{B}}(M_{\mathcal{B}}(\gamma)) = \Delta^{\mathcal{B}}\left((T_{\mathcal{A}}^{\mathcal{B}})^T M_{\mathcal{A}}(\gamma) T_{\mathcal{A}}^{\mathcal{B}}\right)$$

$\Delta^{\mathcal{B}}$ Isomorphismus

$$\implies M_{\mathcal{B}}(\gamma) = (T_{\mathcal{A}}^{\mathcal{B}})^T M_{\mathcal{A}}(\gamma) T_{\mathcal{A}}^{\mathcal{B}}$$

□

Definition 20.11 V endlichdimensional, γ Bilinearform auf V . Wir setzen $\text{Rang}(\gamma) := \text{Rang } M_{\mathcal{B}}(\gamma)$, wobei \mathcal{B} eine Basis von V ist.

Anmerkung Dies ist wohldefiniert. (folgt aus 20.10, da die Matrizen $T_{\mathcal{A}}^{\mathcal{B}}$ invertierbar sind)

Bemerkung+Definition 20.12 Es gilt:

1. Ist $\gamma : V \times V \rightarrow K$ eine Bilinearform, dann induziert γ die linearen Abbildungen

$$\Gamma_l : V \rightarrow V^*, w \mapsto \gamma(\cdot, w) \quad \gamma(\cdot, w) : V \rightarrow K, v \mapsto \gamma(v, w)$$

$$\Gamma_r : V \rightarrow V^*, v \mapsto \gamma(v, \cdot) \quad \gamma(v, \cdot) : V \rightarrow K, v \mapsto \gamma(v, w)$$

2. Jede lineare Abbildung $\Gamma : V \rightarrow V^*$ induziert Bilinearformen

$$\gamma_l : V \times V \rightarrow K, \gamma_l(v, w) := \Gamma(w)(v)$$

$$\gamma_r : V \times V \rightarrow K, \gamma_r(v, w) := \Gamma(v)(w)$$

Die Zuordnungen aus 1., 2. induzieren den Isomorphismus $\text{Bil}(V) \cong \text{Hom}_K(V, V^*)$

Beweis Nachrechnen. □

Definition 20.13 γ Bilinearform auf V . γ heißt **nicht-ausgeartet** $\iff \Gamma_l$ und Γ_r sind injektiv.

$$\iff \gamma(v, w) = 0 \forall v \in V \implies w = 0$$

(Injektivität von Γ_l), und

$$\iff \gamma(v, w) = 0 \forall w \in V \implies v = 0$$

(Injektivität von Γ_r).

γ heißt **perfekt** $\iff \Gamma_l$ und Γ_r sind Isomorphismen.

Bemerkung 20.14 V endlichdimensional, γ Bilinearform auf V , $\mathcal{B} = (v_1, \dots, v_n)$ Basis von V , \mathcal{B}^* duale Basis zu \mathcal{B} . Dann gilt:

$$M_{\mathcal{B}^*}^{\mathcal{B}}(\Gamma_l) = M_{\mathcal{B}}(\gamma) = (M_{\mathcal{B}^*}^{\mathcal{B}}(\Gamma_r))^T$$

Beweis Behauptung: Es ist $\Gamma_l(v_i) = \gamma(v_1, v_i)v_1^* + \dots + \gamma(v_n, v_i)v_n^*$, denn $\Gamma_l(v_i)(v_j) = \gamma(v_j, v_i)$ nach Definition

$$(\gamma(v_1, v_i)v_1^* + \dots + \gamma(v_n, v_i)v_n^*)(v_j) = \gamma(v_j, v_i)$$

Somit: $M_{\mathcal{B}^*}^{\mathcal{B}}(\Gamma_l) = M_{\mathcal{B}}(\gamma)$.

Analog: $\Gamma_r(v_i) = \gamma(v_i, v_1)v_1^* + \dots + \gamma(v_i, v_n)v_n^* \implies M_{\mathcal{B}^*}^{\mathcal{B}}(\Gamma_r) = (M_{\mathcal{B}}(\gamma))^T$ □

Folgerung 20.15 V endlichdimensional, γ Bilinearform auf V , \mathcal{B} Basis von V . Dann sind äquivalent:

1. γ ist nicht-ausgeartet
2. γ ist perfekt
3. $M_{\mathcal{B}}(\gamma)$ invertierbar
4. Γ_l injektiv
5. Γ_r injektiv

Beweis 1. \iff 2. wegen $\dim V = \dim V^*$ und 12.12

γ perfekt $\iff \Gamma_l, \Gamma_r$ Isomorphismen $\iff M_{\mathcal{B}^*}^{\mathcal{B}}(\Gamma_l), M_{\mathcal{B}^*}^{\mathcal{B}}(\Gamma_r)$ invertierbar $\iff M_{\mathcal{B}}(\gamma)$ invertierbar.
 $M_{\mathcal{B}^*}^{\mathcal{B}}(\Gamma_l), M_{\mathcal{B}^*}^{\mathcal{B}}(\Gamma_r) \iff \Gamma_l$ Isomorphismus $\iff M_{\mathcal{B}^*}^{\mathcal{B}}$ invertierbar. □

Definition 20.16 γ Bilinearform auf V .

γ heißt **symmetrisch** $\iff \gamma(v, w) = \gamma(w, v) \forall v, w \in V$

γ heißt **antisymmetrisch** $\iff \gamma(v, w) = -\gamma(w, v) \forall v, w \in V$

γ heißt **alternierend** $\iff \gamma(v, v) = 0 \forall v \in V$.

Anmerkung • γ symmetrisch $\implies \Gamma_l = \Gamma_r$

• Für $\text{char}(K) \neq 2$ gilt: γ alternierend $\iff \gamma$ antisymmetrisch

• Für $\text{char}(K) = 2$ gilt immer noch γ alternierend $\implies \gamma$ (anti)symmetrisch Die Umkehrung ist falsch:
 $\gamma: \mathbb{F}_2^3 \times \mathbb{F}_2^3 \rightarrow \mathbb{F}, \gamma(x, y) = x_1y_1 + x_2y_2 + x_3y_3$ ist (anti)symmetrisch, aber nicht alternierend:

$$\gamma\left(\begin{pmatrix} \bar{1} \\ \bar{0} \\ \bar{0} \end{pmatrix}, \begin{pmatrix} \bar{1} \\ \bar{0} \\ \bar{0} \end{pmatrix}\right) = \bar{1} \neq \bar{0}$$

Bemerkung 20.17 V endlichdimensional, \mathcal{B} Basis von V , γ Bilinearform auf V . Dann gilt:

1. γ symmetrisch $\iff M_{\mathcal{B}}(\gamma)$ ist symmetrisch, das heißt $M_{\mathcal{B}}(\gamma)^T = M_{\mathcal{B}}(\gamma)$
2. γ antisymmetrisch $\iff M_{\mathcal{B}}(\gamma)$ ist antisymmetrisch, das heißt $M_{\mathcal{B}}(\gamma)^T = -M_{\mathcal{B}}(\gamma)$

Beweis 1. „ \implies “ klar

„ \impliedby “ Sei $M_{\mathcal{B}}(\gamma) = M_{\mathcal{B}}(\gamma)^T \implies$ Für v, w ist

$$\begin{aligned}\gamma(v, w) &= \Phi_{\mathcal{B}}^{-1}(v)^T M_{\mathcal{B}}(\gamma) \Phi_{\mathcal{B}}^{-1}(w) = \Phi_{\mathcal{B}}^{-1}(v)^T M_{\mathcal{B}}(\gamma)^T \Phi_{\mathcal{B}}^{-1}(w)^T \\ &= \underbrace{\left(\Phi_{\mathcal{B}}^{-1}(w)^T M_{\mathcal{B}}(\gamma) \Phi_{\mathcal{B}}^{-1} \right)^T}_{\in K} = \Phi_{\mathcal{B}}^{-1}(w)^T M_{\mathcal{B}}(\gamma) \Phi_{\mathcal{B}}^{-1}(v) = \gamma(w, v).\end{aligned}$$

2. analog. □

21 Quadratische Räume

Definition 21.1 (Quadratische Form) V K -VR. Eine Abbildung $q : V \rightarrow K$ heißt eine **quadratische Form** auf V , genau dann wenn folgende Bedingungen erfüllt sind:

- (Q1) $q(\lambda v) = \lambda^2 q(v) \forall \lambda \in K, v \in V$
- (Q2) Die Abbildung $\varepsilon_q : V \times V \rightarrow K, (v, w) \mapsto q(v+w) - q(v) - q(w)$ ist eine (automatisch symmetrische) Bilinearform

Beispiel 21.2

$K = \mathbb{R}, V = \mathbb{R}^2, q\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) = x_1^2 + x_1 x_2 + x_2^2$ ist eine quadratische Form auf \mathbb{R}^2 (Q1) ist erfüllt, (Q2) ist ebenfalls erfüllt, denn

$$\begin{aligned}\varepsilon_q\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}\right) &= q\left(\begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \end{pmatrix}\right) - q\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) - q\left(\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}\right) \\ &= (x_1 + y_1)^2 + (x_1 + y_1)(x_2 + y_2) + (x_2 + y_2)^2 - x_1^2 - x_1 x_2 - x_2^2 - y_1^2 - y_1 y_2 - y_2^2 \\ &= 2x_1 y_1 + x_1 y_2 + x_2 y_1 + 2x_2 y_2\end{aligned}$$

das heißt ε_q ist symmetrische Bilinearform.

Bemerkung 21.3 $\text{char } K \neq 2, V$ K -VR, $\text{SymBil}(V) := \{\gamma : V \times V \rightarrow K \mid \gamma \text{ ist symmetrische Bilinearform}\}, \text{Quad}(V) := \{q : V \rightarrow K \mid q \text{ ist eine quadratische Form}\}$. Dann sind die Abbildungen

$$\Phi : \text{SymBil}(V) \rightarrow \text{Quad}(V), \gamma \mapsto q_\gamma \quad q_\gamma : V \rightarrow K, v \mapsto \gamma(v, v)$$

$$\Psi : \text{Quad}(V) \rightarrow \text{SymBil}(V), q \mapsto \gamma_q \frac{1}{2} \varepsilon_q$$

zueinander inverse Bijektionen.

Beweis 1. Φ ist wohldefiniert, das heißt $q_\gamma \in \text{Quad}(V) \forall \gamma \in \text{SymBil}(V)$.

Q1: Sei $\lambda \in K, v \in V \implies q_\gamma(\lambda v) = \gamma(\lambda v, \lambda v) = \lambda^2 \gamma(v, v) = \lambda^2 q_\gamma(v)$

Q2:

$$\begin{aligned}\varepsilon_{q_\gamma} &= q_\gamma(v+w) - q_\gamma(v) - q_\gamma(w) = \gamma(v+w, v+w) - \gamma(v, v) - \gamma(w, w) \\ &= \gamma(v, w) + \gamma(w, v) = 2\gamma(v, w)\end{aligned}$$

$\implies \varepsilon_{q_\gamma}$ symmetrische Bilinearform.

2. Ψ ist wohldefiniert, denn für jedes $q \in \text{Quad}(V)$ ist $\gamma_q = (1/2)\varepsilon_q \in \text{SymBil}(V)$, da $\varepsilon_q \in \text{SymBil}(V)$
3. $\Phi \circ \Psi = \text{id}_{\text{Quad}(V)}$: Für $q \in \text{Quad}(V), v \in V$ ist

$$(\Phi \circ \Psi)(q)(v) = \Phi(\gamma_q)(v) = \gamma_q(v, v) = \frac{1}{2}(q(v+v) - q(v) - q(v)) = q(v)$$

4. $\Psi \circ \Phi = \text{id}_{\text{SymBil}(V)}$: Für $\gamma \in \text{SymBil}(V), v, w \in V$ ist

$$(\Psi \circ \Phi)(\gamma)(v, w) = \Psi(q_\gamma)(v, w) = \frac{1}{2}\varepsilon_{q_\gamma}(v, w) = \gamma(v, w)$$

□

Anmerkung Philosophie dahinter: symmetrische Bilinearformen, quadratische Formen auf K sind für $\text{char } K \neq 2$ fast dasselbe. Für $\text{char } k = 2$ kann man die Abbildung Φ immer noch definieren, Φ ist im allgemeinen aber weder injektiv, noch surjektiv. Exemplarisch: Für $K = \mathbb{F}_2, V = \mathbb{F}_2^2$ liegt die quadratische Form $q : \mathbb{F}_2^2 \rightarrow \mathbb{F}_2, \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto x_1^2 + x_1x_2 + x_2^2$ liegt nicht im Bild vom Φ .

Für den Rest dieses Abschnittes sei K stets ein Körper mit $\text{char } K \neq 2$

Definition 21.4 (Quadratischer Raum) Ein **quadratischer Raum** ist ein Paar (V, γ) , bestehend aus endlichdimensionalem K -VR V und einer symmetrischen Bilinearform γ auf V . $v, w \in V$ heißen **orthogonal** bezüglich $\gamma \iff \gamma(v, w) = 0$. $(v_i)_{i \in I}$ Familie von Vektoren aus V heißt orthogonal bezüglich $\gamma \iff \gamma(v_i, v_j) = 0 \forall i, j \in I, i \neq j$. Eine Familie (v_1, \dots, v_n) von Vektoren aus V heißt eine **Orthogonalbasis** (OB) von $(V, \gamma) \iff (v_1, \dots, v_n)$ ist eine Basis von V und ist orthogonal bezüglich γ .

Anmerkung • Ist γ aus dem Kontext klar, wird es auch häufig weggelassen.

- Ist \mathcal{B} eine Basis von V , dann gilt \mathcal{B} OB von $(V, \gamma) \iff M_{\mathcal{B}}(\gamma)$ ist eine Diagonalmatrix.

Definition 21.5 $(V, \gamma_v), (W, \gamma_w)$ quadratische Räume, $f : V \rightarrow W$ lineare Abbildung. f heißt **Homomorphismus quadratischer Räume** \iff

$$\gamma_w(f(v_1), f(v_2)) = \gamma_v(v_1, v_2) \forall v_1, v_2 \in V$$

f heißt **Isomorphismus quadratischer Räume** $\iff f$ ist ein Isomorphismus von K -VR und ein Homomorphismus quadratischer Räume. Notation: Wir schreiben häufig $f : (V, \gamma_v) \rightarrow (W, \gamma_w)$ für Abbildungen / Homomorphismen quadratischer Räume.

Anmerkung Ist $f : (V, \gamma_v) \rightarrow (W, \gamma_w)$ ein Isomorphismus quadratischer Räume, dann ist $f^{-1} : (W, \gamma_w) \rightarrow (V, \gamma_v)$ ebenfalls ein Isomorphismus quadratischer Räume, und es ist $\text{Rang}(\gamma_v) = \text{Rang}(\gamma_w)$ (nachrechnen...)

Ziel: Klassifiziere quadratische Räume bis auf Isomorphie quadratischer Räume.

Satz 21.6 (V, γ) quadratischer Raum. Dann besitzt (V, γ) eine OB.

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

IA: $n = 0$: leere Familie ist OB.

IS: Sei $n \geq 1$

1. Fall: $\gamma(v, v) = 0 \forall v \in V$

$$\implies \forall v, w \in V : 0 = \gamma(v+w, v+w) = \gamma(v, v) + \gamma(w, w) + 2\gamma(v, w) = 2\gamma(v, w)$$

$$\implies \gamma(v, w) = 0 \forall v, w \in V \implies \text{Jede Basis von } V \text{ ist OB von } (V, \gamma)$$

2. $\exists v_1 \in V : \gamma(v_1, v_1) \neq 0$. Sei $\Gamma : V \rightarrow V^*, v \mapsto \gamma(v, \cdot)$ die zu γ gemäß 20.10 gehörige lineare Abbildung. Setze $H = \ker(\Gamma(v_1)) = \{w \in V \mid \gamma(v_1, w) = 0\}$

$$\implies \dim H = \dim V - \underbrace{\dim \text{im}(\Gamma(v_1))}_{\leq K \text{ beachte: } \Gamma(v_1) \in V^*} \in \{n, n-1\}$$

Es ist $v_1 \notin H$ wegen $\gamma(v_1, v_1) \neq 0 \implies \dim H = n-1 \implies V = \text{Lin}((v_1)) \oplus H$.
 $(H, \gamma|_{H \times H})$ ist ein quadratischer Raum der Dimension $n-1$. Wegen IV existiert eine OB (v_2, \dots, v_n) von $(H, \gamma|_{H \times H}) \implies (v_1, v_2, \dots, v_n)$ ist OB von (V, γ) \square

Folgerung 21.7 $A \in M(n \times n, K)$ symmetrisch. Dann existiert $T \in \text{GL}(n, K)$, sodass $T^T A T$ eine Diagonalmatrix.

Beweis A definiert eine symmetrische Bilinearform $\Delta(A) = \Delta_A^{(e_1, \dots, e_n)}$ auf K^n (vergleiche 20.7, $\Delta(A)(v, w) = v^T A w$). Nach 21.6 existiert eine OB \mathcal{B} von $(K^n, \Delta(A)) \implies M_{\mathcal{B}}(\Delta(A))$ ist Diagonalmatrix, und es ist

$$M_{\mathcal{B}}(\Delta(A)) = \underbrace{\left(T_{(e_1, \dots, e_n)}^{\mathcal{B}}\right)^T}_{=: T^T} \underbrace{M_{(e_1, \dots, e_n)}(\Delta(A))}_A \underbrace{T_{(e_1, \dots, e_n)}^{\mathcal{B}}}_{=: T} \quad \square$$

Folgerung 21.8 (V, γ) quadratischer Raum, $n = \dim V, r = \text{Rang}(\gamma)$. Dann existieren $\lambda_1, \dots, \lambda_r \in K \setminus \{0\}$ und ein Isomorphismus von quadratischen Räumen

$$\Phi : \left(K^n, \Delta \left(\begin{pmatrix} \lambda_1 & & & 0 \\ & \ddots & & \\ & & \lambda_r & \\ & & & 0 \\ & & & & \ddots \\ 0 & & & & & 0 \end{pmatrix} \right) \right) \rightarrow (V, \gamma)$$

Beweis Wegen 21.6 existiert eine OB $\mathcal{B} = (v_1, \dots, v_n)$ von (V, γ) . Nach Umordnung von v_1, \dots, v_n sei $\gamma(v_i, v_i) \neq 0$ für $i = 1, \dots, s$ und $\gamma(v_i, v_i) = 0$ für $i = s+1, \dots, n$

$$\implies M_{\mathcal{B}}(\gamma) = \begin{pmatrix} \lambda_1 & & & 0 \\ & \ddots & & \\ & & \lambda_s & \\ & & & 0 \\ & & & & \ddots \\ 0 & & & & & 0 \end{pmatrix} \quad \lambda_1, \dots, \lambda_s \in K \setminus \{0\}, r = \text{Rang}(\gamma) = \text{Rang } M_{\mathcal{B}}(\gamma) = s$$

Setze $\Phi := \Phi_{\mathcal{B}} : K^n \rightarrow V, e_i \mapsto v_i$ (Koordinatensystem zu \mathcal{B} , vergleiche 15.2). Φ ist Isomorphismus

$$\begin{aligned} \gamma(\Phi_{\mathcal{B}}(v), \Phi_{\mathcal{B}}(w)) &= \Phi_{\mathcal{B}}^{-1}(\Phi_{\mathcal{B}}(v))^T M_{\mathcal{B}}(\gamma) \Phi_{\mathcal{B}}^{-1}(\Phi_{\mathcal{B}}(w)) = v^T M_{\mathcal{B}}(\gamma) w \\ &= v^T \begin{pmatrix} \lambda_1 & & & 0 \\ & \ddots & & \\ & & \lambda_r & \\ & & & 0 \\ & & & & \ddots \\ 0 & & & & & 0 \end{pmatrix} w = \Delta \left(\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_r \end{pmatrix} \right) (v, w) \quad \square \end{aligned}$$

Anmerkung $\lambda_1, \dots, \lambda_r$ sind im allgemeinen nicht eindeutig bestimmt.

Frage: Kann man über speziellen Körpern mehr sagen? Wir werden $K = \mathbb{C}, \mathbb{R}$ untersuchen.

Satz 21.9 (V, γ) quadratischer Raum über \mathbb{C} , $n = \dim V$, $r = \text{Rang } \gamma$. Dann existiert eine Orthogonalbasis \mathcal{B} von (V, γ) mit

$$M_{\mathcal{B}}(\gamma) = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$$

Insbesondere existiert ein Isomorphismus quadratischer Räume $\Phi\left(\mathbb{C}^n, \Delta\left(\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}\right)\right) \rightarrow (V, \gamma)$

Beweis Sei $(\tilde{v}_1, \dots, \tilde{v}_n)$ eine Orthogonalbasis von (V, γ) . Setze

$$v_i := \begin{cases} \tilde{v}_i & \gamma(\tilde{v}_i, \tilde{v}_i) = 0 \\ \frac{1}{\sqrt{\gamma(\tilde{v}_i, \tilde{v}_i)}} \tilde{v}_i & \gamma(\tilde{v}_i, \tilde{v}_i) \neq 0 \end{cases}$$

Hierbei ist $\sqrt{\gamma(\tilde{v}_i, \tilde{v}_i)}$ eine komplexe Zahl α mit $\alpha^2 = \gamma(\tilde{v}_i, \tilde{v}_i)$. Falls $\gamma(\tilde{v}_i, \tilde{v}_i) \neq 0$, dann ist

$$\gamma(v_i, v_i) = \gamma\left(\frac{1}{\sqrt{\gamma(\tilde{v}_i, \tilde{v}_i)}}, \frac{1}{\sqrt{\gamma(\tilde{v}_i, \tilde{v}_i)}}\right) = \frac{1}{\gamma(\tilde{v}_i, \tilde{v}_i)} \gamma(\tilde{v}_i, \tilde{v}_i) = 1$$

Außerdem: $\gamma(v_i, v_j) = 0 \forall i \neq j$, da $\gamma(\tilde{v}_i, \tilde{v}_j) = 0 \forall i \neq j$. Setze $\mathcal{B} := (v_1, \dots, v_n)$. Nach eventueller Umnummerierung von v_1, \dots, v_n ist

$$M_{\mathcal{B}}(\gamma) = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$$

wobei $r = \text{Rang } M_{\mathcal{B}}(\gamma) = \text{Rang } \gamma$. □

Folgerung 21.10 $A \in M(n \times n, \mathbb{C})$ symmetrisch, $r = \text{Rang } A$. Dann existiert ein $T \in \text{GL}(n, \mathbb{C})$, sodass

$$T^T A T = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$$

Folgerung 21.11 (21.11) $(V, \gamma_V), (W, \gamma_W)$ quadratische Räume über \mathbb{C} . Dann sind äquivalent:

1. Es gibt einen Isomorphismus quadratischer Räume $(V, \gamma_V) \rightarrow (W, \gamma_W)$
2. $\dim V = \dim W$ und $\text{Rang } \gamma_V = \text{Rang } \gamma_W$

Beweis 1. \implies 2. vergleiche Anmerkung nach 21.5

2. \implies 1. Sei $n = \dim V = \dim W$, $r = \text{Rang } \gamma_V = \text{Rang } \gamma_W$. $\implies (V, \gamma_V), (W, \gamma_W)$ sind als quadratische Räume isomorph zu $\left(\mathbb{C}^n, \Delta\left(\begin{pmatrix} E_r \\ \end{pmatrix}\right)\right)$, also auch $(V, \gamma_V) \cong (W, \gamma_W)$ □

Definition 21.12 (V, γ) quadratischer Raum, $U_1, \dots, U_m \subseteq V$ UVR mit $V = U_1 \oplus \dots \oplus U_m$. Die direkte Summe heißt **orthogonale direkte Summe**

$$(V = U_1 \oplus \dots \oplus U_m) \stackrel{\text{Def}}{\iff} \gamma(u_i, u_j) = 0 \forall u_i \in U_i, u_j \in U_j, i \neq j$$

alternativ \oplus

Satz 21.13 (V, γ) quadratischer Raum über \mathbb{R} , $n = \dim V$. Dann existiert eine Orthogonalbasis \mathcal{B} von (V, γ) , sowie $r_+, r_- \in \{0, \dots, \dim V\}$ mit

$$M_{\mathcal{B}}(\gamma) = \begin{pmatrix} E_{r_+} & & 0 \\ & -E_{r_-} & \\ 0 & & 0 \end{pmatrix}$$

Insbesondere existiert ein Isomorphismus quadratischer Räume

$$\left(\mathbb{R}^n, \Delta \left(\begin{pmatrix} E_{r_+} & & 0 \\ & -E_{r_-} & \\ 0 & & 0 \end{pmatrix} \right) \right) \rightarrow (V, \gamma)$$

Die Zahlen r_+, r_- sind unabhängig von der Wahl einer solchen Basis. Wir nennen $\text{Signatur}(\gamma) := (r_+, r_-)$ heißt die **Signatur** von γ .

Beweis 1. Sei $(\tilde{v}_1, \dots, \tilde{v}_n)$ eine Orthogonalbasis von (V, γ) . Wir setzen

$$v_i := \begin{cases} \tilde{v}_i & \gamma(\tilde{v}_i, \tilde{v}_i) = 0 \\ \frac{1}{\sqrt{|\gamma(\tilde{v}_i, \tilde{v}_i)|}} \tilde{v}_i & \gamma(\tilde{v}_i, \tilde{v}_i) \neq 0 \end{cases}$$

Falls $\gamma(\tilde{v}_i, \tilde{v}_i) \neq 0$, dass ist

$$\begin{aligned} \gamma(v_i, v_i) &= \gamma\left(\frac{1}{\sqrt{|\gamma(\tilde{v}_i, \tilde{v}_i)|}} \tilde{v}_i, \frac{1}{\sqrt{|\gamma(\tilde{v}_i, \tilde{v}_i)|}} \tilde{v}_i\right) \\ &= \frac{1}{|\gamma(\tilde{v}_i, \tilde{v}_i)|} \gamma(\tilde{v}_i, \tilde{v}_i) \in \{\pm 1\} \end{aligned}$$

$\gamma(v_i, v_j) = 0$ für $i \neq j$. Setze $\mathcal{B} := (v_1, \dots, v_n)$. Nach eventueller Umnummerierung von v_1, \dots, v_n ist

$$M_{\mathcal{B}}(\gamma) = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & -1 & & & \\ & & & & \ddots & & \\ 1 & & & & & -1 & \\ & & & & & & 0 \\ & & & & & & \ddots \\ & & & & & & & 0 \end{pmatrix} = \begin{pmatrix} E_{r_+} & & 0 \\ & -E_{r_-} & \\ 0 & & 0 \end{pmatrix}$$

mit geeigneten $r_+, r_- \in \{0, \dots, n\}$

2. r_+, r_- sind basisunabhängig: Es ist $r_+ + r_- = \text{Rang } \gamma$, dies ist basisunabhängig. Es gilt zu zeigen: r_+ ist basisunabhängig. Setze $V_+ := \text{Lin}((v_1, \dots, v_{r_+}))$, $V_- = \text{Lin}((v_{r_++1}, \dots, v_{r_++r_-}))$, $V_0 := \text{Lin}((v_{r_++r_-+1}, \dots, v_n)) \implies V = V_+ \hat{\oplus} V_- \hat{\oplus} V_0$. Setze

$$s := \max\{\dim W \mid W \subseteq V \text{ UVR mit } \gamma(w, w) > 0 \forall w \in W, w \neq 0\}$$

dies ist wohldefiniert. V_+ ist ein UVR von V mit $\gamma(w, w) > 0 \forall w \in V_+, w \neq 0$, denn für $w = \lambda_1 v_1 + \dots + \lambda_{r_+} v_{r_+}$ ist

$$\gamma(w, w) = \lambda_1^2 \underbrace{\gamma(v_1, v_1)}_{=1} + \dots + \lambda_{r_+}^2 \underbrace{\gamma(v_{r_+}, v_{r_+})}_{=1} = \lambda_1^2 + \dots + \lambda_{r_+}^2 > 0 \text{ falls } w \neq 0$$

$\Rightarrow s \geq \dim V_+ = r_+$ Annahme: Es existiert ein UVR $W \subseteq V$ mit $\gamma(w, w) > 0 \forall w \in W, w \neq 0$ und $\dim W > r_+$

$$\Rightarrow \underbrace{\dim W}_{>r_+} + \underbrace{\dim V_-}_{=r_-} + \underbrace{\dim V_0}_{n-(r_++r_-)} > n$$

$$\begin{aligned} \Rightarrow \dim(W \cap (V_- \hat{\oplus} V_0)) &= \dim W + \dim(V_- \hat{\oplus} V_0) - \dim(W + (V_- \hat{\oplus} V_0)) \\ &= \underbrace{\dim W + \dim V_- + \dim V_0}_{>n} - \underbrace{\dim(W + (V_- \hat{\oplus} V_0))}_{\leq n, \text{ da } W + (V_- \hat{\oplus} V_0) \text{ UVR von } V} \\ &=> 0 \end{aligned}$$

\Rightarrow Es existiert $w \in W, w \neq 0$ mit $w \in W_- \hat{\oplus} V_0$.

\Rightarrow Es existiert $w_- \in V_-, w_0 \in V_0$ mit $w = w_- + w_0$

$\Rightarrow \gamma(w, w) = \gamma(w_- + w_0, w_- + w_0) = \underbrace{\gamma(w_-, w_-)}_{<0} + \underbrace{\gamma(w_0, w_0)}_{=0} < 0$ Andererseits: $\gamma(w, w) > 0$

wegen $w \in W, w \neq 0$. Somit: $r_+ = s$, insbesondere unabhängig von Basiswahl. \square

Folgerung+Definition 21.14 (Sylvesterscher Trägheitssatz) $A \in M(n \times n, \mathbb{R})$ symmetrisch. Dann existieren $T \in GL(n, \mathbb{R}), r_+, r_- \in \{0, \dots, n\}$ mit

$$T^T A T = \begin{pmatrix} E_{r_+} & & 0 \\ & -E_{r_-} & \\ 0 & & 0 \end{pmatrix}$$

Die Zahlen r_+, r_- sind unabhängig von der Wahl eines solchen T . $\text{Signatur}(A) := (r_+, r_-)$ heißt **Signatur** von A .

Beweis folgt aus 21.13 (analog zum Beweis von 21.7). \square

Anmerkung Ist $S \in GL(n, \mathbb{R})$, dann haben die Matrixen A und $S^T A S$ dieselbe Signatur, denn: Ist $\tilde{T} \in GL(n, \mathbb{R})$ mit

$$\tilde{T}^T (S^T A S) \tilde{T} = \begin{pmatrix} E_{r_+} & & 0 \\ & -E_{r_-} & \\ 0 & & 0 \end{pmatrix}$$

, dann ist

$$(S \tilde{T})^T A (S \tilde{T}) = \begin{pmatrix} E_{r_+} & & 0 \\ & -E_{r_-} & \\ 0 & & 0 \end{pmatrix}$$

Folgerung 21.15 $(V, \gamma_V), (W, \gamma_W)$ quadratische Räume über \mathbb{R} . Dann sind äquivalent:

1. Es gibt einen Isomorphismus quadratischer Räume $(V, \gamma_V) \rightarrow (W, \gamma_W)$
2. $\dim V = \dim W$ und $\text{Signatur}(\gamma_V) = \text{Signatur}(\gamma_W)$

Beweis 1. \Rightarrow 2. Für $\text{Signatur}(\gamma_V) = \text{Signatur}(\gamma_W)$ verwende Charakterisierung von r_+ aus dem Beweis von 21.3.

2. \Rightarrow 1. aus 21.13, analog zum Beweis von 21.11 \square

Anmerkung Man kann Folgerung 21.11/21.15 verwenden, um quadratische Formen über \mathbb{C} beziehungsweise \mathbb{R} bis auf Äquivalenz zu klassifizieren (vergleiche Übungen)

22 Euklidische Räume

Definition 22.1 V -VR, $\gamma : V \times V \rightarrow \mathbb{R}$ symmetrische Bilinearform. γ heißt

- **positiv definit** $\stackrel{\text{Def}}{\iff} \gamma(v, v) > 0 \forall v \in V \setminus \{0\}$
- **positiv semidefinit** $\stackrel{\text{Def}}{\iff} \gamma(v, v) \geq 0 \forall v \in V \setminus \{0\}$
- **negativ definit** $\stackrel{\text{Def}}{\iff} \gamma(v, v) < 0 \forall v \in V \setminus \{0\}$
- **negativ semidefinit** $\stackrel{\text{Def}}{\iff} \gamma(v, v) \leq 0 \forall v \in V \setminus \{0\}$
- **indefinit** $\stackrel{\text{Def}}{\iff} \gamma$ ist weder positiv noch negativ semidefinit.

Eine positiv definite symmetrische Bilinearform nennt man auch ein **Skalarprodukt**.

Beispiel 22.2

1. $V = \mathbb{R}^n, \langle \cdot, \cdot \rangle : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}, \left\langle \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \right\rangle := x_1 y_1 + \cdots + x_n y_n$ ist ein Skalarprodukt auf dem

\mathbb{R}^n . Positiv Definitheit:

$$\left\langle \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \right\rangle = x_1^2 + \cdots + x_n^2 > 0, \text{ falls } \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \neq 0$$

$\langle \cdot, \cdot \rangle$ heißt das **Standardskalarprodukt** auf dem \mathbb{R}^n .

2. $V = \mathcal{C}[0, 1]$

$$\gamma : \mathcal{C}[0, 1] \times \mathcal{C}[0, 1] \rightarrow \mathbb{R}, (f, g) \mapsto \int_0^1 f(t)g(t)dt$$

ist ein Skalarprodukt.

Anmerkung Um die Definitheit einer symmetrischen Bilinearform nachzuweisen, genügt es nicht, das Verhalten auf den Basisvektoren zu untersuchen: Sei $\gamma : \mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}$ gegeben durch

$$\gamma = \Delta \left(\begin{pmatrix} 1 & -1 \\ -2 & 1 \end{pmatrix} \right)$$

das heißt

$$M_{(e_1, e_2)}(\gamma) = \begin{pmatrix} 1 & -2 \\ -2 & 1 \end{pmatrix}$$

Dann ist $\gamma(e_1, e_1) = 1, \gamma(e_2, e_2) = 1$ aber

$$\gamma \left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right) = \begin{pmatrix} 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -2 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = -2 < 0$$

das heißt γ ist indefinit.

Definition 22.3 Ein **Euklidischer Raum** ist ein Paar (V, γ) , bestehend aus einem endlichdimensionalen \mathbb{R} -VR V und einem Skalarprodukt γ auf V . Für den Rest dieses Abschnittes sei (V, γ) ein Euklidischer Raum.

Definition 22.4 $v \in V$

$$\|v\| := \sqrt{\gamma(v, v)}$$

heißt die **Norm** auf V .

$(v_i)_{i \in I}$ Familie von Vektoren aus V heißt **orthonormal** $\stackrel{\text{Def}}{\iff} (v_i)_{i \in I}$ ist orthogonal und $\|v_i\| = 1 \forall i \in I$.

$\mathcal{B} = (v_1, \dots, v_n)$ heißt **Orthonormalbasis** von $V((V, \gamma))$ (ONB) $\iff \mathcal{B}$ ist Basis von V und \mathcal{B} ist orthonormal.

Bemerkung 22.5 (v_1, \dots, v_n) orthogonale Familie von Vektoren aus $V \setminus \{0\}$. Dann gilt:

1. $\left(\frac{v_1}{\|v_1\|}, \dots, \frac{v_n}{\|v_n\|}\right)$ ist eine orthonormale Familie
2. (v_1, \dots, v_n) ist linear unabhängig.

Beweis 1. $\|v_i\|^2 = \gamma(v_i, v_i) \neq 0$, da γ positiv definit und $v_i \neq 0$.

$$\gamma\left(\frac{v_i}{\|v_i\|}, \frac{v_j}{\|v_j\|}\right) = \frac{1}{\|v_i\|\|v_j\|} \gamma(v_i, v_j) = \begin{cases} 0 & i \neq j \\ \frac{\gamma(v_i, v_i)}{\|v_i\|^2} = 1 & i = j \end{cases}$$

2. Sei $\lambda_1 v_1 + \dots + \lambda_n v_n = 0$

$$\begin{aligned} \implies \lambda_1 \gamma(v_1, v_i) + \dots + \lambda_n \gamma(v_n, v_i) &= 0 \\ \implies \lambda_i &= 0 \end{aligned}$$

□

Bemerkung 22.6 Es gilt:

1. (V, γ) besitzt eine Orthonormalbasis
2. γ ist nicht-ausgeartet
3. Es gibt eine Basis \mathcal{B} von V mit $M_{\mathcal{B}}(\gamma) = E_n$, wobei $n = \dim V$

Beweis Der quadratische Raum (V, γ) hat eine Orthogonalbasis (v_1, \dots, v_n)

$$\implies \mathcal{B} := \left(\frac{v_1}{\|v_1\|}, \dots, \frac{v_n}{\|v_n\|}\right)$$

ist eine Orthonormalbasis von (V, γ) . Es ist $M_{\mathcal{B}}(\gamma) = E_n$ (\implies 3.), insbesondere ist $M_{\mathcal{B}}(\gamma)$ invertierbar $\implies \gamma$ nicht ausgeartet \implies 2. □

Bemerkung 22.7 $\mathcal{B} = (v_1, \dots, v_n)$ Orthonormalbasis von (V, γ) , $v \in V$. Dann gilt: Ist $v = \lambda_1 v_1 + \dots + \lambda_n v_n$, dann ist $\lambda_i = \gamma(v, v_i) \forall i = 1, \dots, n$

Beweis $\gamma(v, v_i) = \lambda_1 \gamma(v_1, v_i) + \dots + \lambda_n \gamma(v_n, v_i) = \lambda_i \underbrace{\gamma(v_i, v_i)}_{=1} = \lambda_i$ □

Bemerkung+Definition 22.8 $U \subseteq V$ Untervektorraum.

$$U^\perp := \{v \in V \mid \gamma(v, u) = 0 \forall u \in U\}$$

heißt das **orthogonale Komplement** zu U . U^\perp ist ein Untervektorraum von V .

Beweis leicht nachzurechnen □

Satz+Definition 22.9 $U \subseteq V$ Untervektorraum. Dann gilt:

1. $V = U \oplus U^\perp$
2. $\dim U^\perp = \dim V - \dim U$
3. $(U^\perp)^\perp = U$
4. Ist (u_1, \dots, u_m) eine Orthogonalbasis von $(U, \gamma|_{U \times U})$, und ist $v \in V$ mit $v = u + v', u \in U, v' \in U^\perp$, dass ist

$$u = \sum_{j=1}^m \gamma(v, u_j) u_j$$

Die lineare Abbildung

$$\pi_u : V \rightarrow U, v \mapsto \sum_{j=1}^m \gamma(v, u_j) u_j$$

heißt die **Orthogonalprojektion** von V auf U .

Beweis 1. $U + U^\perp = V$, denn:

Sei (u_1, \dots, u_m) eine Orthogonalbasis von $(U, \gamma|_{n \times n})$, $v \in V$. Setze

$$v' := v - \sum_{j=1}^m \gamma(v, u_j) u_j$$

$$\implies \gamma(v', u_i) = \gamma(v, u_i) - \sum_{j=1}^m \gamma(v, u_j) \gamma(u_j, u_i) = \gamma(v, u_i) - \gamma(v, u_i) = 0 \forall i = 1, \dots, m$$

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

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

$$\implies V = U + U^\perp$$

$$U \cap U^\perp = \{0\}, \text{ denn: } u \in U \cap U^\perp \implies \gamma(u, u) = 0 \implies u = 0 \text{ (da } \gamma \text{ Skalarprodukt)}$$

2. aus 1., 2.

3. Sei $u \in U \implies \gamma(u, w) = 0 \forall w \in U^\perp \implies u \in (U^\perp)^\perp$, das heißt $U \subseteq U^{\perp\perp}$. Wegen $\dim(U^\perp)^\perp = \dim V - \dim U^\perp = \dim V - (\dim V - \dim U) = \dim U$ folgt $U = U^{\perp\perp}$ \square

Anmerkung Insbesondere gilt für alle $v \in V : v - \pi_U(v) \in U^\perp$

Beispiel 22.10

$(V, \gamma) = (\mathbb{R}^2, \langle \cdot, \cdot \rangle)$, $U = \text{Lin}\left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right) \implies U^\perp = \text{Lin}\left(\begin{pmatrix} -1 \\ 1 \end{pmatrix}\right)$, denn $\begin{pmatrix} -1 \\ 1 \end{pmatrix} \in U^\perp$ wegen $\langle \begin{pmatrix} -1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \rangle = 0$, und es ist $\dim U^\perp = 2 - \dim U = 2 - 1 = 1$. Jedes Element aus V lässt sich eindeutig schreiben als

$$v = \lambda \begin{pmatrix} 1 \\ 1 \end{pmatrix} + \mu \begin{pmatrix} -1 \\ 1 \end{pmatrix}$$

das heißt

$$\pi_u : v = \underbrace{\lambda \begin{pmatrix} 1 \\ 1 \end{pmatrix}}_{\in U} + \underbrace{\mu \begin{pmatrix} -1 \\ 1 \end{pmatrix}}_{\in U^\perp} \mapsto \lambda \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \gamma\left(v, \begin{pmatrix} 1 \\ 1 \end{pmatrix}\right) \vec{1}; \vec{1}$$

Frage: Wie bestimmt man explizit eine Orthogonalbasis eines Euklidischen Raumes?

Algorithmus 22.11 (Gram-Schmidt-Verfahren) **Eingabe:** (v_1, \dots, v_n) Basis von V .

Ausgabe: Orthonormalbasis (w_1, \dots, w_n) von (V, γ)

Durchführung:

1. Setze

$$w_1 := \frac{v_1}{\|v_1\|}$$

2. Setze für $k = 2, \dots, n$

$$\tilde{w}_k := v_k - \sum_{i=1}^{k-1} \gamma(v_k, w_i) w_i, \quad w_k := \frac{\tilde{w}_k}{\|\tilde{w}_k\|}$$

3. (w_1, \dots, w_n) ist eine Orthonormalbasis von (V, γ)

Beweis Sei $U_k := \text{Lin}((v_1, \dots, v_k))$ für $k = 1, \dots, n$. Wir zeigen per Induktion nach k , dass (w_1, \dots, w_k) eine Orthogonalbasis von $(U_k, \gamma|_{U_k \times U_k})$ ist (Behauptung folgt dann aus $k = n$).

Induktionsanfang: $k = 1$ klar

Induktionsschritt: Sei $\pi_{k-1} := \pi_{U_{k-1}} : V \rightarrow U_{k-1}$ die orthogonale Projektion.

$$\implies \tilde{w}_k = v_k - \pi_{k-1}(v_k)$$

da (w_1, \dots, w_{k-1}) Orthogonalbasis von U_{k-1} nach Induktionsvoraussetzung. $\implies \tilde{w}_k \in U_{k-1}^\perp$. Außerdem $\tilde{w}_k \neq 0$, da sonst $v_k = \pi_{k-1}(v_k) \in U_{k-1}$ zu (v_1, \dots, v_k) Basis von U_{k-1}

$$\implies w_k = \frac{\tilde{w}_k}{\|\tilde{w}_k\|} \in U_{k-1}^\perp$$

und es ist

$$\gamma(w_k, w_i) = \begin{cases} 0 & i = 1, \dots, k-1 \\ 1 & i = k \end{cases}$$

$\implies (w_1, \dots, w_k)$ Orthogonalbasis von U_k

□

Beispiel 22.12

Wir betrachten $(\mathbb{R}^3, \langle \cdot, \cdot \rangle)$, $U = \text{Lin}((v_1, v_2))$ mit $v_1 := \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}$, $v_2 := \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}$. Gesucht ist eine Orthogonalbasis

von U bezüglich $\langle \cdot, \cdot \rangle$. Setze

$$w := \frac{v_1}{\|v_1\|} = \frac{1}{\sqrt{5}} \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}$$

$$\begin{aligned} \tilde{w}_2 &= v_2 - \langle v_2, w \rangle w = \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} - \left\langle \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}, \frac{1}{\sqrt{5}} \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} \right\rangle \frac{1}{\sqrt{5}} \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} - \frac{1}{5} \left\langle \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} \right\rangle \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} + \frac{2}{5} \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -\frac{1}{5} \\ 1 \\ \frac{2}{5} \end{pmatrix} = \frac{1}{2} \begin{pmatrix} -1 \\ 5 \\ 2 \end{pmatrix} \end{aligned}$$

$$w_2 = \frac{\tilde{w}_2}{\|\tilde{w}_2\|} = \frac{1}{\sqrt{30}} \begin{pmatrix} -1 \\ 5 \\ 2 \end{pmatrix}$$

$$\implies \left(\frac{1}{\sqrt{5}} \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{30}} \begin{pmatrix} -1 \\ 5 \\ 2 \end{pmatrix} \right) \text{ ist eine Orthogonalbasis von } U.$$

Definition 22.13 $A \in M(n \times n, \mathbb{R})$ symmetrisch. A heißt **positiv definit** (Notation: $A > 0$) $\stackrel{\text{Def}}{\iff}$ Die symmetrische Bilinearform

$$\Delta(A) : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}, (x, y) \mapsto x^T A y$$

ist positiv definit.

Bemerkung 22.14 $A \in M(n \times n, \mathbb{R})$ symmetrisch. Dass sind äquivalent:

1. $A > 0$
2. $\exists T \in \text{GL}(n, \mathbb{R}) : A = T^T T$

Beweis 1. \implies 2. Sei $A > 0 \implies (\mathbb{R}^n, \Delta(A))$ Euklidischer Raum. Sei \mathcal{B} Orthogonalbasis von $(\mathbb{R}^n, \Delta(A))$ $T := T_{\mathcal{B}}^{(e_1, \dots, e_n)}$

$$\implies E_n = M_{\mathcal{B}}(\Delta(A)) = \underbrace{\left(T_{(e_1, \dots, e_n)}^{\mathcal{B}}\right)^T}_{=(T^{-1})^T} \underbrace{M_{(e_1, \dots, e_n)}(\Delta(A))}_{=A} \underbrace{T_{(e_1, \dots, e_n)}^{\mathcal{B}}}_{=T^{-1}}$$

$$\implies A = T^T T$$

2. Sei $A = T^T T$ für ein $T \in \text{GL}(n, \mathbb{R})$. Für $x \in \mathbb{R}^n, x \neq 0$ ist

$$\Delta(A)(x, x) = x^t A w = x^t T^t T x = (Tx)^T T x = \langle Tx, Tx \rangle > 0$$

□

Anmerkung 1., 2. sind äquivalent zu

3. Es existiert eine obere Dreiecksmatrix P mit Diagonaleinträgen, sodass $A = P^T P$ (siehe Übungen). Obiges P ist sogar eindeutig bestimmt, eine solche Zerlegung heißt Cholesky-Zerlegung.

Satz 22.15 (Cauchy-Schwarz-Ungleichung) $v, w \in V$. Dann gilt:

$$|\gamma(v, w)| \leq \|v\| \|w\|$$

Gleichheit gilt hierbar genau dann, wenn (v, w) linear abhängig.

Beweis 1. Beweis der Ungleichung: Falls $w = 0$, dass fertig. Im Folgenden sei $w \neq 0$. Für $\lambda, \mu \in \mathbb{R}$ ist

$$0 \leq \gamma(\lambda v + \mu w, \lambda v + \mu w) = \lambda^2 \gamma(v, v) + \mu^2 \gamma(w, w) + 2\lambda \mu \gamma(v, w)$$

Setze $\lambda := \gamma(w, w) > 0$, dividiere durch λ

$$0 \leq \gamma(v, v) \gamma(w, w) + \mu^2 + 2\mu \gamma(v, w)$$

Setze $\mu := -\gamma(v, w)$

$$\begin{aligned} 0 &\leq \gamma(v, v) \gamma(w, w) + \gamma(v, w)^2 - 2\gamma(v, w)^2 \\ \gamma(v, w)^2 &\leq \gamma(v, v) \gamma(w, w) \\ |\gamma(v, w)| &\leq \|v\| \|w\| \end{aligned}$$

2. Gleichheitsaussage: Für $w = 0$: (v, w) linear abhängig und „ $=$ “ gilt. Ab jetzt also $w \neq 0$.

” \Leftarrow “ Sei (v, w) linear abhängig $\implies \exists \lambda \in K : v = \lambda w$

$$\implies |\gamma(v, w)|^2 = |\gamma(\lambda w, w)|^2 = |\lambda|^2 |\gamma(w, w)|^2 = |\gamma(w, w)| |\gamma(\lambda w, \lambda w)| = \|w\|^2 \|\lambda w\|^2$$

$$\implies |\gamma(v, w)| = \|w\| \|\lambda w\| = \|w\| \|\lambda\| \|w\|.$$

” \implies “ Es gelte, sei also $|\gamma(v, w)| = \|v\| \|w\|$. Führe die Rechnung wie in 1. rückwärts durch: Mit $\lambda := \gamma(w, w), \mu = -\gamma(v, w)$ folgt dass

$$\gamma(\lambda v + \mu w, \lambda v + \mu w) = 0 \implies \lambda v + \mu w = 0 \implies (v, w) \text{ linear abhängig} \quad \square$$

Bemerkung 22.16 (Eigenschaften der Norm) $v, w \in V, \lambda \in \mathbb{R}$. Dann gilt:

$$1. \|v\| = 0 \iff v = 0$$

$$2. \|\lambda v\| = |\lambda| \|v\|$$

$$3. \|v + w\| \leq \|v\| + \|w\|$$

Beweis 1. klar, da γ positiv definit

$$2. \|\lambda v\|^2 = \gamma(\lambda v, \lambda v) = \lambda^2 \gamma(v, v) = \lambda^2 \|v\|^2 \implies \|\lambda v\| = |\lambda| \|v\|$$

3.

$$\begin{aligned} \|v + w\|^2 &= \gamma(v + w, v + w) = \|v\|^2 + \|w\|^2 + 2\gamma(v, w) \leq \|v\|^2 + \|w\|^2 + 2|\gamma(v, w)| \\ &\leq \|v\|^2 + \|w\|^2 + 2\|v\| \|w\| = (\|v\| + \|w\|)^2 \\ \implies \|v + w\| &\leq \|v\| + \|w\| \end{aligned} \quad \square$$

Bemerkung 22.17 $v, w \in V$. Dann gilt:

$$1. \|v + w\|^2 = \|v\|^2 + \|w\|^2 \iff \gamma(v, w) = 0 \quad \text{Satz des Pythagoras}$$

$$2. \|v + w\|^2 + \|v - w\|^2 = 2\|v\|^2 + 2\|w\|^2 \quad \text{Parallelogrammgleichung}$$

Beweis 1. $\|v + w\|^2 = \gamma(v + w, v + w) = \|v\|^2 + \|w\|^2 + 2\gamma(v, w) \implies$ Behauptung

$$2. \|v + w\|^2 + \|v - w\|^2 = \gamma(v + w, v + w) + \gamma(v - w, v - w) = 2\|v\|^2 + 2\|w\|^2 \quad \square$$

Anmerkung V \mathbb{R} Vektorraum. Eine Abbildung $\|\cdot\| : V \rightarrow \mathbb{R}_{\geq 0}$ mit den Eigenschaften 1. bis 3. aus 22.16 heißt eine Norm auf V , $(V, \|\cdot\|)$ ein normierter Vektorraum. Man kann zeigen: Ist $(V, \|\cdot\|)$ ein normierter Vektorraum, in dem die Parallelogrammgleichung gilt, dann ist durch

$$\gamma(v, w) := \frac{1}{2} (\|v + w\|^2 - \|v\|^2 - \|w\|^2)$$

ein Skalarprodukt auf V mit $\|v\| = \sqrt{\gamma(v, v)}$, das heißt in diesen Fällen ist (V, γ) ein euklidischer Vektorraum, dessen Norm mit die gegebenen übereinstimmt.

23 Die orthogonale Gruppe

Definition 23.1 $(V, \gamma_V), (W, \gamma_W)$ Euklidische Räume, $\varphi : V \rightarrow W$ lineare Abbildung. φ heißt **orthogonal** $\stackrel{\text{Def}}{\iff} \varphi$ ist ein Homomorphismus quadratischer Räume, das heißt

$$\gamma_W(\varphi(v_1), \varphi(v_2)) = \gamma_V(v_1, v_2) \forall v_1, v_2 \in V$$

Bemerkung 23.2 $(V, \gamma_V), (W, \gamma_W)$ Euklidische Räume, $\varphi : V \rightarrow W$ orthogonale Abbildung. Dann gilt:

1. $\|\varphi(v)\|_W = \|v\|_V \forall v \in V$
2. $v_1 \perp v_2 \iff \varphi(v_1) \perp \varphi(v_2) \forall v_1, v_2 \in V$
3. φ ist injektiv

Beweis 1. $\|\varphi(v)\|_W^2 = \gamma_W(\varphi(v), \varphi(v)) = \gamma_V(v, v) = \|v\|_V^2$

$$2. v_1 \perp v_2 \iff \gamma_V(v_1, v_2) = 0 \iff \gamma_W(\varphi(v_1), \varphi(v_2)) = 0 \iff \varphi(v_1) \perp \varphi(v_2)$$

$$3. \text{ Sei } v \in V \text{ mit } \varphi(v) = 0 \implies \|\varphi(v)\|_W = 0 \implies \|v\|_V = 0 \implies v = 0 \quad \square$$

Bemerkung 23.3 (V, γ) Euklidischer Raum, $n = \dim V$, \mathcal{B} Orthogonalbasis von (V, γ) . Dann ist das Koordinatensystem $\Phi_{\mathcal{B}} : (\mathbb{R}^n, \langle \cdot, \cdot \rangle) \rightarrow (V, \gamma)$ ein orthogonaler Isomorphismus.

Beweis $\Phi_{\mathcal{B}}$ Isomorphismus: klar. $\Phi_{\mathcal{B}}$ orthogonal, denn: Sei $\mathcal{B} = (v_1, \dots, v_n)$ dann ist

$$\gamma(\Phi_{\mathcal{B}}(e_i), \Phi_{\mathcal{B}}(e_j)) = \gamma(v_i, v_j) = \delta_{ij} = \langle e_i, e_j \rangle \quad \square$$

Bemerkung 23.4 (V, γ) Euklidischer Raum, $\varphi \in \text{End}(V)$ orthogonal. Dann gilt:

1. φ ist Isomorphismus
2. φ^{-1} ist orthogonal
3. $\lambda \in \mathbb{R}$ Eigenwert von $\gamma \implies |\lambda| = 1$, das heißt $\lambda \in \{\pm 1\}$

Beweis 1. aus 23.2.3 folgt: φ injektiv $\implies \varphi$ Isomorphismus

$$2. v_1, v_2 \in V \implies \gamma(\varphi^{-1}(v_1), \varphi^{-1}(v_2)) = \gamma(\varphi(\varphi^{-1}(v_1)), \varphi(\varphi^{-1}(v_2))) = \gamma(v_1, v_2) \implies \varphi^{-1} \text{ orthogonal}$$

$$3. \text{ Sei } v \in V \text{ Eigenvektor zum Eigenwert } \lambda \implies \|v\| = \|\varphi(v)\| = \|\lambda v\| = |\lambda| \|v\| \implies |\lambda| = 1 \quad \square$$

Bemerkung 23.5 (V, γ) Euklidischer Raum, $n = \dim V$, \mathcal{B} Orthogonalbasis von V , $\varphi \in \text{End}(V)$, $A = M_{\mathcal{B}}(\varphi)$. Dann sind äquivalent:

1. φ ist orthogonal
2. $A^T A = E_n$

Beweis Wir erhalten kommutierendes Diagramm

$$\begin{array}{ccc}
 (V, \gamma) & \xleftarrow{\Phi_B} & (V, \gamma) \\
 \varphi \downarrow & & \downarrow \varphi \\
 (\mathbb{R}^n, \langle \cdot, \cdot \rangle) & \xleftarrow{\Phi_B} & (\mathbb{R}^n, \langle \cdot, \cdot \rangle)
 \end{array}$$

Da Φ_B orthogonaler Isomorphismus nach 23.3 folgt:

$$\begin{aligned}
 \varphi \text{ orthogonal} &\iff \tilde{A} = \Phi_B^{-1} \circ \varphi = \varphi \circ \Phi_B \text{ orthogonal} \\
 &\iff \forall x, y \in \mathbb{R}^n : \langle Ax, Ay \rangle = \langle x, y \rangle \\
 &\iff \forall x, y \in \mathbb{R}^n : (Ax)^T Ay = x^T y \\
 &\iff \forall x, y \in \mathbb{R}^n : \langle Ax, Ay \rangle = x^T A^T Ay = x^T y \\
 &\iff \Delta(A^T A) = \Delta(E_n) \\
 &\iff A^T A = E_n
 \end{aligned}$$

□

Bemerkung+Definition 23.6 A heißt **orthogonal** $\stackrel{\text{Def}}{\iff} A^T A = E_n$

$$O(n) := \{A \in M(n \times n, \mathbb{R}) \mid A \text{ ist orthogonal}\}$$

$O(n)$ ist bezüglich die Matrixmultiplikation eine Gruppe, die **orthogonale Gruppe** vom Rang n

Beweis Wohldefiniertheit von „ \cdot “ (das heißt Abgeschlossenheit bezüglich „ \cdot “): $A, B \in O(n) \implies (AB)^T AB = B^T A^T AB = B^T B = E_n \implies AB \in O(n)$.

Existenz des neutralen Elements: $E_n \in O(n)$

Assoziativität: klar

Existenz von Inversen: Sei $A \in A(n) \implies A^T A = E_n \implies A^{-1} = A^t \implies (A^{-1})^T A^{-1} = (A^T)^T A^T = AA^T = AA^{-1} = E_n$ □

Anmerkung $A \in O(n) \implies \det(A) \in \{\pm 1\}$, denn $1 = \det(E_n) = \det(A^T A) = \det(A^T) \det(A) = \det(A)^2$

Bemerkung 23.7 $A \in M(n \times n, \mathbb{R})$. Dann sind äquivalent:

1. $A \in O(n)$
2. $AA^T = E_n$
3. $A^T A = E_n$
4. Die Transponierten der Zeilen von A bilden eine Orthogonalbasis von $(\mathbb{R}^n, \langle \cdot, \cdot \rangle)$
5. Die Spalten von A bilden eine Orthogonalbasis von $(\mathbb{R}^n, \langle \cdot, \cdot \rangle)$
6. Die Abbildung $\tilde{A} : (\mathbb{R}^n, \langle \cdot, \cdot \rangle) \rightarrow (\mathbb{R}^n, \langle \cdot, \cdot \rangle)$ ist orthogonal

Beweis 1. \iff 2. \iff 3. \iff klar

$$2. \iff 4., 3. \iff 5.$$

$$1. \iff 6. \text{ aus 23.5 (setze } V = (\mathbb{R}^n, \langle \cdot, \cdot \rangle), \mathcal{B} = (e_1, \dots, e_n))$$

□

Satz 23.8 $\varphi : \mathbb{R}^n \rightarrow \mathbb{R}^n$ (nicht notwendig linear) abstandstreu, das heißt

$$\|\varphi(x) - \varphi(y)\| = \|x - y\| \forall x, y \in \mathbb{R}^n$$

wobei $\|\cdot\|$ die Norm auf $(\mathbb{R}^n, \langle \cdot, \cdot \rangle)$ bezeichne. Dann existieren eindeutig bestimmte $A \in O(n), b \in \mathbb{R}^n$, sodass

$$\varphi(x) = Ax + b$$

für alle $x \in \mathbb{R}^n$

Bemerkung+Definition 23.9 $SO(n) := \{A \in O(n) \mid \det A = 1\}$ ist eine Untergruppe von $O(n)$ (das heißt $SO(n) \subseteq O(n)$ und ist eine Gruppe bezüglich der eingeschränkten Verknüpfung), die **spezielle orthogonale Gruppe** vom Rang n .

Beweis Wohldefiniertheit von „ \cdot “ (= Abgeschlossenheit bezüglich „ \cdot “)

$$A, B \in SO(n) \implies AB \in O(n) \wedge \det(AB) = \det(A) \det(B) = 1 \cdot 1 = 1$$

neutrales Element: $E_n \in SO(n)$

Assoziativität: klar

Existenz von Inversem: $A \in SO(n) \implies A^{-1} \in O(n), \det(A^{-1}) = \det(A)^{-1} = 1 \implies A^{-1} \in SO(n)$ □

Beispiel 23.10

$$n = 1 : O(1) = \{\pm 1\}, SO(1) = \{1\}$$

Bemerkung 23.11 $A \in O(2)$. Dann gilt:

$$1. A \in SO(2) \iff \exists! \alpha \in [0, 2\pi] \text{ mit}$$

$$A = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix}$$

In diesem Fall beschreibt A eine Drehung mit Zentrum 0 um den Winkel α . Außer im Fall $\alpha \in \{0, \pi\}$ besitzt A keine Eigenwerte. Falls $\alpha = 0$:

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

einzigster Eigenwert: 1. Falls $\alpha = \pi$:

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

einzigster Eigenwert: -1 .

$$2. A \in O(2) \setminus SO(2) \iff \exists! \alpha \in [0, 2\pi] \text{ mit}$$

$$A = \begin{pmatrix} \cos \alpha & \sin \alpha \\ \sin \alpha & -\cos \alpha \end{pmatrix}$$

In diesem Fall beschreibt A eine Spiegelung an der Geraden $\text{Lin}\left(\begin{pmatrix} \cos \frac{\alpha}{2} \\ \sin \frac{\alpha}{2} \end{pmatrix}\right)$. A besitzt die Eigenwerte ± 1 , und es existiert eine Orthogonalbasis \mathcal{B} von $(\mathbb{R}^2, \langle \cdot, \cdot \rangle)$ mit

$$M_{\mathcal{B}}(\tilde{A}) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Beweis Sei $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in O(2)$

$$\implies 1 = \|e_1\|^2 = \|Ae_1\|^2 = a^2 + b^2$$

$$\implies 1 = \|e_2\|^2 = \|Ae_2\|^2 = c^2 + d^2$$

Außerdem: $e_1 \perp e_2 \implies Ae_1 \perp Ae_2$

$$\implies \left\langle \begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} c \\ d \end{pmatrix} \right\rangle = 0$$

$$\implies \begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} = 0 \implies \begin{pmatrix} c \\ d \end{pmatrix} \in \text{Lin}\left(\begin{pmatrix} -b \\ a \end{pmatrix}\right)$$

das heißt es existiert $\lambda \in \mathbb{R}$ mit

$$\begin{pmatrix} c \\ d \end{pmatrix} = \lambda \begin{pmatrix} -b \\ a \end{pmatrix}$$

$$\implies A = \begin{pmatrix} a & -\lambda b \\ b & \lambda a \end{pmatrix}, \det A = \lambda(a^2 + b^2) = \lambda \in \{\pm 1\}$$

1. Fall: $\lambda = 1 \iff \det A = 1 \iff A \in SO(2)$ Wegen $a^2 + b^2 = 1$ ist $\begin{pmatrix} a \\ b \end{pmatrix}$ ein Punkt auf dem Einheitskreis. $\implies \exists! \alpha \in [0, 2\pi)$ mit $a = \cos \alpha, b = \sin \alpha$. Somit:

$$A \in SO(2) \iff A = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix}$$

für eindeutig bestimmte $\alpha \in [0, 2\pi)$. Sei $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} \cos \beta \\ \sin \beta \end{pmatrix}$ ein Punkt auf dem Einheitskreis

$$A \begin{pmatrix} \cos \beta \\ \sin \beta \end{pmatrix} = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} \begin{pmatrix} \cos \beta \\ \sin \beta \end{pmatrix} = \begin{pmatrix} \cos \alpha \cos \beta - \sin \alpha \sin \beta \\ \sin \alpha \cos \beta + \cos \alpha \sin \beta \end{pmatrix} = \begin{pmatrix} \cos(\alpha + \beta) \\ \sin(\alpha + \beta) \end{pmatrix}$$

$\implies A$ beschreibt eine Drehung mit Zentrum 0 um den Winkel α . A hat nur Eigenwerte, wenn $\alpha = 0$ beziehungsweise $\alpha = \pi$ (Eigenwert: 1 beziehungsweise -1):

$$\chi_A^{char} = t^2 - \text{sp}(A)t + \det A = t^2 - 2 \cos \alpha + 1$$

Eigenwerte: $\lambda_{1,2} = \cos \alpha \pm \sqrt{\cos^2 \alpha - 1}$, Eigenwert in $\mathbb{R} \iff \cos^2 \alpha - 1 \geq 0 \iff \alpha = 0$ oder $\alpha = \pi$

2. $\lambda = -1 \iff A \in O(2) \setminus SO(2)$:

$$\iff A = \begin{pmatrix} a & b \\ b & -a \end{pmatrix}$$

Wegen $a^2 + b^2 = 1$ existiert genau ein $\alpha \in [0, 2\pi)$ mit $a = \cos \alpha, b = \sin \alpha$. Sei $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} \cos \beta \\ \sin \beta \end{pmatrix}$ ein Punkt auf dem Einheitskreis.

$$\implies A \begin{pmatrix} \cos \beta \\ \sin \beta \end{pmatrix} = \begin{pmatrix} \cos \alpha & \sin \alpha \\ \sin \alpha & -\cos \alpha \end{pmatrix} \begin{pmatrix} \cos \beta \\ \sin \beta \end{pmatrix} = \begin{pmatrix} \cos \alpha \cos \beta + \sin \alpha \sin \beta \\ \sin \alpha \cos \beta - \cos \alpha \sin \beta \end{pmatrix} = (\cos(\alpha - \beta), \sin(\alpha - \beta))$$

$$\implies A \begin{pmatrix} \cos(\frac{\alpha}{2} + \beta) \\ \sin(\frac{\alpha}{2} + \beta) \end{pmatrix} = \begin{pmatrix} \cos(\frac{\alpha}{2} - \beta) \\ \sin(\frac{\alpha}{2} - \beta) \end{pmatrix}$$

$$\implies A \text{ beschreibt Spiegelung an der Geraden } \text{Lin} \left(\begin{pmatrix} \cos \frac{\alpha}{2} \\ \sin \frac{\alpha}{2} \end{pmatrix} \right)$$

$$\chi_A^{\text{char}} = t^2 - \text{sp}(A)t + \det A = t^2 - 1 = (t+1)(t-1)$$

$\implies A$ diagonalisierbar und hat Eigenwert ± 1 . Sei v_1 Eigenvektor von A zum Eigenwert 1 mit $\|v_1\| = 1$, v_2 Eigenvektor von A zum Eigenwert -1 mit $\|v_2\| = 1$

$$\implies \langle v_1, v_2 \rangle = \langle Av_1, Av_2 \rangle = \langle v_1, -v_2 \rangle = -\langle v_1, v_2 \rangle \implies \langle v_1, v_2 \rangle = 0 \iff v_1 \perp v_2$$

Bezüglich der Orthogonalbasis (v_1, v_2) des $(\mathbb{R}^2, \langle \cdot, \cdot \rangle)$ ist $M_{\mathcal{B}}(\tilde{A}) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ \square

Folgerung 23.12 $\varphi : (\mathbb{R}^2, \langle \cdot, \cdot \rangle) \rightarrow (\mathbb{R}^2, \langle \cdot, \cdot \rangle)$ orthogonale Abbildung. Dann existiert eine Orthogonalbasis \mathcal{B} von $(\mathbb{R}^2, \langle \cdot, \cdot \rangle)$, sodass

$$M_{\mathcal{B}}(\varphi) = \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \text{ oder } M_{\mathcal{B}}(\varphi) = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix}, \alpha \in (0, \pi)$$

Die Anzahl der ± 1 sowie α sind unabhängig von der Wahl einer solchen Orthogonalbasis \mathcal{B} (das heißt sind Invarianten von φ).

Beweis Existenz von \mathcal{B} : Sei $\mathcal{C} = (e_1, e_2)$, $A := M_{\mathcal{C}}(\varphi)$, insbesondere $A \in O(2)$.

1. Fall: $A \in SO(2) \implies \exists \beta \in (0, 2\pi), \beta \neq \pi$ mit

$$A = \begin{pmatrix} \cos \beta & -\sin \beta \\ \sin \beta & \cos \beta \end{pmatrix} \text{ oder } A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ oder } A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

Falls $\beta \in (0, \pi)$, setze $\alpha := \beta$, $\mathcal{B} = \mathcal{C}$.

Falls $\beta \in (\pi, 2\pi)$

$$\implies M_{(e_2, e_1)}(\varphi) = \begin{pmatrix} \cos \beta & \sin \beta \\ -\sin \beta & \cos \beta \end{pmatrix}$$

Setze $\alpha := 2\pi - \beta$, $\mathcal{B} := (e_2, e_1) \implies \beta = 2\pi - \alpha \implies \cos \beta = \cos \alpha, \sin \beta = -\sin \alpha$

$$\implies M_{\mathcal{B}}(\varphi) = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix}$$

2. $A \in O(2) \setminus SO(2) \implies \exists$ Orthogonalbasis \mathcal{B} von $(\mathbb{R}^2, \langle \cdot, \cdot \rangle)$ mit $M_{\mathcal{B}}(\varphi) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

Eindeutigkeit: Falls $M_{\mathcal{B}}(\varphi) = \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$, dann Anzahl der $\pm 1 = \mu_{\text{alg}}$ der Eigenwerte ± 1 . Falls $M_{\mathcal{B}}(\varphi) = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix}$, dann $\chi_{\varphi}^{\text{char}} = t^2 - 2 \cos \alpha t + 1 \implies \cos \alpha$ ist unabhängig von der Wahl der Basis \mathcal{B} .
Wegen $\alpha \in (0, \pi)$ ist α unabhängig von \mathcal{B} . \square

Anmerkung Verallgemeinerung von 23.12 auf $(\mathbb{R}^n, \langle \cdot, \cdot \rangle)$ ist möglich.

24 Der Spektralsatz

In diesem Abschnitt sei (V, γ) stets ein Euklidischer Raum.

Bemerkung 24.1 Die Abbildung $\Gamma : V \rightarrow V^*, w \mapsto \gamma(\cdot, w)$ ist ein Isomorphismus.

Beweis γ nicht ausgeartet nach 22.6 $\implies \gamma$ perfekt, das heißt Γ Isomorphismus. \square

Anmerkung Insbesondere ist für einen Euklidischen Vektorraum (V, γ) die Vektorräume V und V^* kanonisch isomorph.

Bemerkung 24.2 $\mathcal{B} = (v_1, \dots, v_n)$ Orthonormalbasis von (V, γ) , $\mathcal{B}^* = (v_1^*, \dots, v_n^*)$ duale Basis zu \mathcal{B} , $U \subseteq V$ Untervektorraum, $\Gamma : V \rightarrow V^*$ kanonische Abbildung aus 24.1. Dass gilt:

1. $\Gamma(U^\perp) = U^0$
2. $\Gamma(v_i) = v_i^*, i = 1, \dots, n$

Beweis 1. $\Gamma(U^\perp) \subseteq U^0$, denn: Für $v \in U^\perp, u \in U$ ist $(\Gamma(v))(u) = \gamma(u, v) = 0 \implies \Gamma(U^\perp) \subseteq U^0$.

$$\dim \Gamma(U^\perp) = \dim U^\perp = \dim V - \dim U = \dim U^0$$

2. Es ist $\Gamma(v_i)(v_j) = \gamma(v_j, v_i) = \delta_{ij} = v_i^*(v_j), j = 1, \dots, n$, das heißt $\Gamma(v_i) = v_i^*$ \square

Bemerkung+Definition 24.3 $(V, \gamma_V), (W, \gamma_W)$ Euklidische Räume, $\varphi : V \rightarrow W$. Dass existiert genau eine lineare Abbildung $\varphi^{ad} : W \rightarrow V$ mit

$$\gamma_W(\varphi(v), w) = \gamma_V(v, \varphi^{ad}(w)) \forall v \in V, w \in W$$

φ^{ad} heißt die zu φ **adjungierte Abbildung**

Beweis Existenz: Wir betrachten das Diagramm

$$\begin{array}{ccc} V & \xrightarrow{\Gamma_V} & W \\ \varphi^{ad} \uparrow & & \uparrow \varphi^* \\ V^* & \xrightarrow{\Gamma_W} & W^* \end{array}$$

und setzen $\varphi^{ad} := \Gamma_V^{-1} \circ \varphi^* \circ \Gamma_W$, φ^{ad} ist linear nach Konstruktion. Es gilt für $v \in V, w \in W$:

$$\begin{aligned} \gamma_W(\varphi(v), w) &= \Gamma_W(w)(\varphi(v)) = (\Gamma_W(w) \circ \varphi)(v) = \varphi^*(\Gamma_W(w))(v) \\ &= ((\varphi^* \circ \Gamma_W)(w))(v) = \left((\Gamma_V \circ \varphi^{ad})(w) \right)(v) = \Gamma_V(\varphi^{ad}(w))(v) \\ &= \gamma_V(v, \varphi^{ad}(w)) \end{aligned}$$

Eindeutigkeit: Damit obige Gleichung für alle $v \in V, w \in W$ gilt, muss das Diagramm kommutieren, das heißt $\Gamma_V \circ \varphi^{ad} = \varphi^* \circ \Gamma_W$, also $\varphi^{ad} = \Gamma_V^{-1} \circ \varphi^* \circ \Gamma_W$. \square

Anmerkung Ist φ orthogonal, dann ist $\varphi^{ad} = \varphi^{-1}$, denn für $v, w \in V$

$$\gamma(\varphi(v), w) = \gamma(\varphi(v), \varphi(\varphi^{-1}(w))) = \gamma(v, \varphi(w))$$

Bemerkung 24.4 $(V, \gamma_V), (W, \gamma_W)$ euklidische Räume, \mathcal{A} Orthonormalbasis von (V, γ_V) , \mathcal{B} Orthonormalbasis von (W, γ_W) , $\varphi : V \rightarrow W$ lineare Abbildung. Dann gilt

$$M_{\mathcal{A}}^{\mathcal{B}}(\varphi^{ad}) = (M_{\mathcal{B}}^{\mathcal{A}}(\varphi))^T$$

Insbesondere ist $(\varphi^{ad})^{ad} = \varphi$

Beweis

$$\begin{aligned} M_{\mathcal{A}}^{\mathcal{B}}(\varphi^{ad}) &= M_{\mathcal{A}}^{\mathcal{B}}(\Gamma_V^{-1} \circ \varphi^* \circ \Gamma_W) = \underbrace{M_{\mathcal{A}}^{\mathcal{A}*}(\Gamma_V^{-1})}_{E_{\dim V}} \underbrace{M_{\mathcal{A}*}^{\mathcal{B}*}}_{(M_{\mathcal{B}}^{\mathcal{A}}(\varphi))^T} \underbrace{M_{\mathcal{B}\mathcal{B}*}^{\mathcal{B}}(\Gamma_W)}_{=E_{\dim W}} \\ &= (M_{\mathcal{B}}^{\mathcal{A}}(\varphi))^T \end{aligned}$$

□

Satz 24.5 $(V, \gamma_V), (W, \gamma_W)$ euklidische Räume, $\varphi : V \rightarrow W$ lineare Abbildung. Dann gilt:

1. $\ker(\varphi^{ad}) = (\operatorname{im} \varphi)^{\perp}$
2. $\operatorname{im}(\varphi^{ad}) = (\ker \varphi)^{\perp}$

Beweis 1. $w \in (\operatorname{im} \varphi)^{\perp} \iff \gamma_W(\varphi(v), w) = 0 \forall v \in V \iff \gamma_V(v, \varphi^{ad}(w)) = 0 \forall v \in V, \gamma$ nicht ausgeartet $\implies \varphi^{ad}(w) = 0 \iff w \in \ker(\varphi^{ad})$

2. $(\operatorname{im}(\varphi^{ad}))^{\perp} = \ker(\varphi^{ad})^{ad} = \ker \varphi \iff (\ker \varphi)^{\perp} = (\operatorname{im}(\varphi^{ad})^{\perp})^{\perp} = \operatorname{im} \varphi^{ad}$

□

Folgerung 24.6 $\varphi \in \operatorname{End}(V)$. Dann gilt:

$$V = \ker \varphi \hat{\oplus} \operatorname{im} \varphi^{ad} \quad \text{sowie} \quad V = \ker \varphi^{ad} \hat{\oplus} \operatorname{im} \varphi$$

Beweis Es ist

$$V = (\ker \varphi) \hat{\oplus} (\ker \varphi)^{\perp} = \ker \varphi \hat{\oplus} \operatorname{im} \varphi^{ad}$$

andere Gleichung analog.

□

Definition 24.7 (Selbstadjungiert) $\varphi \in \operatorname{End}(V)$ heißt **selbstadjungiert** $\iff \varphi = \varphi^{ad}$

Bemerkung 24.8 \mathcal{B} Orthonormalbasis von (V, γ) . Dann sind äquivalent:

1. φ selbstadjungiert
2. $M_{\mathcal{B}}(\varphi)$ symmetrisch

In diesem Fall $V = \ker \varphi \hat{\oplus} \operatorname{im} \varphi$

Beweis φ selbstadjungiert $\iff \varphi = \varphi^{ad} \iff M_{\mathcal{B}}(\varphi) = M_{\mathcal{B}}\varphi^{ad} = (M_{\mathcal{B}}(\varphi))^T$. Nach 24.6 ist dann $V = \ker \varphi \hat{\oplus} \operatorname{im} \varphi^{ad} = \ker \varphi \hat{\oplus} \operatorname{im} \varphi$

□

Satz 24.9 Es gilt:

1. $\varphi \in \text{End}(V)$ selbstadjungiert $\implies \gamma' : V \times V \rightarrow \mathbb{R}, \gamma'(x, y) = \gamma(\varphi(x), y)$ ist eine symmetrische Bilinearform
2. Ist $\gamma' : V \times V \rightarrow \mathbb{R}$ eine symmetrische Bilinearform, dann existiert genau ein selbstadjungierter Endomorphismus $\varphi \in \text{End}(V)$ mit $\gamma'(x, y) = \gamma(\varphi(x), y) \forall x, y \in V$

In diesen Fällen gilt bezüglich jeder Orthonormalbasis \mathcal{B} von (V, γ) :

$$M_{\mathcal{B}}(\gamma') = M_{\mathcal{B}}(\varphi)$$

Beweis 1. φ selbstadjungiert $\implies \gamma'(x, y) = \gamma(\varphi(x), y) = \gamma(x, \varphi(y)) = \gamma(\varphi(y), x) = \gamma'(y, x)$, γ' bilinear klar.

2. Sei $\gamma' : V \times V \rightarrow \mathbb{R}$ symmetrische Bilinearform, $x \in V \implies \rho_x := \gamma'(x, \cdot) : V \rightarrow \mathbb{R}, \gamma \mapsto \gamma'(x, y)$ ist ein Element von V^* . Nach 24.1 ist $\Gamma : V \rightarrow V^*, w \mapsto \gamma(\cdot, w)$ ein Isomorphismus \implies Es existiert genau ein $z \in V$ mit $\Gamma(z) = \rho_x$, das heißt mit

$$\gamma(y, z) = \Gamma(z)(y) = \rho_x(y) = \gamma'(x, y) \forall y \in V$$

Wir definieren $\varphi : V \rightarrow V, x \mapsto z$ mit $\Gamma(z) = \rho_x \implies$ Für alle $x, y \in V$ ist $\gamma(\varphi(x), y) = \gamma(y, \varphi(x)) = \gamma'(x, y)$.

φ ist linear: Seien $x_1, x_2, y \in V, \lambda, \mu \in \mathbb{R}$

$$\begin{aligned} \implies \Gamma(\varphi(\lambda x_1 + \mu x_2) - \lambda \varphi(x_1) - \mu \varphi(x_2))(y) &= \gamma(y, \varphi(\lambda x_1 + \mu x_2) - \lambda \varphi(x_1) - \mu \varphi(x_2)) \\ &= \gamma(y, \varphi(\lambda x_1 + \mu x_2)) - \lambda \gamma(y, \varphi(x_1)) - \mu \gamma(y, \varphi(x_2)) \\ &= \gamma'(x_1 + \mu x_2, y) - \lambda \gamma'(x_1, y) - \mu \gamma'(x_2, y) \\ &= 0 \end{aligned}$$

γ' bilinear

$$= 0$$

Das gilt für alle $y \in V$

$$\begin{aligned} \implies \Gamma(\varphi(\lambda x_1 + \mu x_2) - \lambda \varphi(x_1) - \mu \varphi(x_2)) &= 0 \\ \implies \varphi(\lambda x_1 + \mu x_2) &= \lambda \varphi(x_1) + \mu \varphi(x_2) \end{aligned}$$

φ selbstadjungiert: Für $x, y \in V$ ist

$$\gamma(\varphi(x), y) = \gamma'(x, y) = \gamma'(y, x) = \gamma(\varphi(y), x) = \gamma(x, \varphi(y)) \implies \varphi = \varphi^{ad}$$

φ ist eindeutig: Sei $\tilde{\varphi}$ selbstadjungiert mit $\gamma'(x, y) = \gamma(\varphi(x), y) = \gamma(\tilde{\varphi}(x), y) \forall x, y \in V$

$$\begin{aligned} \implies \Gamma(\varphi(x))(y) &= \Gamma(\tilde{\varphi}(x))(y) \forall x, y \in V \\ \implies \Gamma(\varphi(x)) &= \Gamma(\tilde{\varphi}(x)) \end{aligned}$$

Γ Isomorphismus

$$\begin{aligned} \implies \varphi(x) &= \tilde{\varphi}(x) \forall x \in V \\ \implies \varphi &= \tilde{\varphi} \end{aligned}$$

Darstellungsmatrizen: Sei $\mathcal{B} = (v_1, \dots, v_n)$ Orthonormalbasis von (V, γ) . $A = M_{\mathcal{B}}(\varphi) = (a_{ij})$

$$\implies \gamma'(v_i, v_j) = \gamma(\varphi(v_i), v_j) = \gamma\left(\sum_{k=1}^n a_{ki} v_k, v_j\right) = a_{ji} \stackrel{\varphi \text{ selbstadjungiert}}{=} a_{ij}$$

$$\implies M_{\mathcal{B}}(\gamma') = M_{\mathcal{B}}(\gamma)$$

□

Anmerkung Interpretation für $(\mathbb{R}^n, \langle \cdot, \cdot \rangle)$: Ist $A \in M(n \times n, \mathbb{R})$ symmetrisch, dann ist A

- Darstellungsmatrix bezüglich (e_1, \dots, e_n) des selbstadjungierten Endomorphismus \tilde{A} von \mathbb{R}^n
- Darstellungsmatrix bezüglich (e_1, \dots, e_n) der symmetrischen Bilinearform $\gamma' = \Delta(A) : (x, y) \mapsto x^t A y$

Es ist $\gamma'(x, y) = x^t A y = x^t A^t y = (Ax)^t y = \langle Ax, y \rangle = \langle \tilde{A}(x), y \rangle \forall x, y \in \mathbb{R}^n$. Bezüglich jeder Orthogonalbasis von $(\mathbb{R}^n, \langle \cdot, \cdot \rangle)$ gilt $M_B(\tilde{A}) = M_B(\gamma')$

Bemerkung 24.10 $\varphi \in \text{End}(V)$ selbstadjungiert, $U \subseteq V$ Untervektorraum mit $\varphi(U) \subseteq U$. Dann gilt $\varphi(U^\perp) \subseteq U^\perp$

Beweis Sei $v \in U^\perp \implies \forall u \in U : \gamma(u, \varphi(v)) = \gamma\left(\underbrace{\varphi(u)}_{\in U}, \underbrace{v}_{\in U^\perp}\right) = 0 \implies \varphi(v) \in U^\perp \quad \square$

Bemerkung 24.11 $\varphi \in \text{End}(V)$ selbstadjungiert. Dann zerfällt $\chi_\varphi^{\text{char}}$ über \mathbb{R} in Linearfaktoren.

Beweis Sei \mathcal{B} eine Orthonormalbasis von (V, γ) , $A = M_B(\varphi) \implies \chi_\varphi^{\text{char}} = \chi_A^{\text{char}}, A = A^T$ wegen φ selbstadjungiert. Wir betrachten die \mathbb{C} -lineare Abbildung $\tilde{A}_\mathbb{C} : \mathbb{C}^n \rightarrow \mathbb{C}^n, z \mapsto Az$. Es ist

$$\chi_A^{\text{char}} = \chi_{\tilde{A}_\mathbb{C}}^{\text{char}} = (t - \lambda_1) \cdot \dots \cdot (t - \lambda_n), \lambda_1, \dots, \lambda_n \in \mathbb{C}$$

Behauptung: $\lambda_i \in \mathbb{R} \forall i = 1, \dots, n$, denn: Sei $z = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} \in \mathbb{C}^n$ ein Eigenvektor zum Eigenwert λ_i von $\tilde{A}_\mathbb{C}$.

Wir setzen $\bar{z} := \begin{pmatrix} \bar{z}_1 \\ \vdots \\ \bar{z}_n \end{pmatrix}$ und erhalten

$$\lambda_i z^T \bar{z} = (\lambda_i z)^T \bar{z} = (Az)^T \bar{z} = z^T A^T \bar{z} = z^T A \bar{z} = z^T \overline{Az} = z^T \overline{\lambda_i z} = \bar{\lambda}_i z^T \bar{z}$$

Es ist $z^T \bar{z} = (z_1, \dots, z_n) \begin{pmatrix} \bar{z}_1 \\ \vdots \\ \bar{z}_n \end{pmatrix} = z_1 \bar{z}_1 + \dots + z_n \bar{z}_n = |z_1|^2 + \dots + |z_n|^2 \neq 0 \implies \lambda_i = \bar{\lambda}_i \implies \lambda_i \in \mathbb{R} \quad \square$

Satz 24.12 (Spektralsatz für selbstadjungierte Endomorphismen) $\varphi \in \text{End}(V)$ selbstadjungierter Endomorphismus. Dann existiert eine Orthonormalbasis von (V, γ) aus Eigenvektoren von φ . Sind $\lambda_1, \dots, \lambda_r$ die verschiedenen Eigenwerte von φ , so ist

$$V = \text{Eig}(\varphi, \lambda_1) \hat{\oplus} \dots \hat{\oplus} \text{Eig}(\varphi, \lambda_r)$$

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

Induktionsanfang: $n = 0$: trivial

Induktionsschritt: Sei $n \geq 1$. Nach 24.11 existiert ein Eigenwert λ von φ und es sei w_1 ein Eigenvektor von φ zum Eigenwert λ . Setze

$$v_i := \frac{w_1}{\|w_1\|}, U := \text{Lin}((v_i)) \implies \varphi(U) \subseteq U \implies \varphi(U^\perp) \subseteq U^\perp$$

Wir setzen $\psi := \varphi|_{U^\perp} : U^\perp \rightarrow U^\perp$. ψ ist selbstadjungiert, denn: Für alle $x, y \in U^\perp$ ist

$$\gamma(\psi(x), y) = \gamma(\varphi(x), y) = \gamma(x, \varphi(y)) = \gamma(x, \psi(y))$$

Nach 22.9 ist $V = U \hat{\oplus} U^\perp$, $\dim U^\perp = \dim V - \dim U = n - 1$. Nach Induktionsvoraussetzung existiert eine Orthonormalbasis von (v_2, \dots, v_n) von U^\perp aus Eigenvektoren von $\varphi \implies (v_1, \dots, v_n)$ ist von Orthonormalbasis (V, γ) aus Eigenvektoren von $\varphi \implies V = \text{Eig}(\varphi, \lambda_1) \hat{\oplus} \dots \hat{\oplus} \text{Eig}(\varphi, \lambda_r)$ \square

Folgerung 24.13 $\gamma' : V \times V : \mathbb{R}$ symmetrische Bilinearform, $n = \dim V$. Dann existiert eine Orthonormalbasis \mathcal{B} von (V, γ) bezüglich derer die Darstellungsmatrix von γ' Diagonalgestalt hat:

$$M_{\mathcal{B}}(\gamma') = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

Hierbei sind $\lambda_1, \dots, \lambda_n$ die Eigenwerte (mit Vielfachen) des zu γ' gehörenden eindeutig bestimmten selbstadjungierten Endomorphismus $\varphi \in \text{End}(V)$ mit $\gamma'(x, y) = \gamma(\varphi(x), y)$

Beweis Sei $\varphi \in \text{End}(V)$ der entsprechende Endomorphismus von V nach 24.9. Spektralsatz \implies Es existiert eine Orthonormalbasis \mathcal{B} von (V, γ) aus Eigenvektoren von φ zu Eigenwerten $\lambda_1, \dots, \lambda_n$ (nicht notwendig verschieden)

$$\implies M_{\mathcal{B}}(\gamma') \stackrel{24.9}{=} M_{\mathcal{B}}(\varphi) = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} \quad \square$$

Folgerung 24.14 $A \in M(n \times n, \mathbb{R})$ symmetrisch. Dann existiert ein $T \in O(n)$, sodass

$$T^{-1}AT = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

Hierbei sind $\lambda_1, \dots, \lambda_n$ die Eigenwerte (mit Vielfachheit) von A . Die Spalten von T bilden eine Orthonormalbasis von $(\mathbb{R}^n, \langle \cdot, \cdot \rangle)$ aus Eigenvektoren von A .

Beweis $\tilde{A} : \mathbb{R}^n \rightarrow \mathbb{R}^n$ ist selbstadjungierter Endomorphismus von $(\mathbb{R}^n, \langle \cdot, \cdot \rangle)$. Spektralsatz \implies es existiert eine Orthonormalbasis \mathcal{B} aus Eigenvektoren von A des $(\mathbb{R}^n, \langle \cdot, \cdot \rangle)$ mit

$$M_{\mathcal{B}}(\tilde{A}) = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

Es ist

$$M_{\mathcal{B}}(\tilde{A}) = \underbrace{\left(T_{(e_1, \dots, e_n)}^{\mathcal{B}}\right)^{-1}}_{=T^{-1}} \underbrace{M_{(e_1, \dots, e_n)}^{(e_1, \dots, e_n)}(\tilde{A})}_A \underbrace{T_{(e_1, \dots, e_n)}^{\mathcal{B}}}_{=:T}$$

Es ist $T \in O(n)$, da \mathcal{B} Orthogonalbasis von $(\mathbb{R}^n, \langle \cdot, \cdot \rangle)$ (vergleiche 23.7) \square

Anmerkung Man kann sogar stets $T \in SO(n)$ erreichen (indem man gegebenenfalls eine Spalte v_i von T durch $-v_i$ ersetzt.)

Algorithmus 24.15 (Hauptachsentransformation) Eingabe: $A \in M(n \times n, \mathbb{R})$ symmetrisch

Ausgabe: $T \in O(n)$, sodass $T^{-1}AT$ Diagonalmatrix

Durchführung:

1. Bestimme $\chi_A^{char} \in \mathbb{R}[t]$ sowie eine Zerlegung

$$\chi_A^{char} = (t - \lambda_1)^{T_1} \cdot \dots \cdot (t - \lambda_k)^{T_k}$$

mit $\lambda_1, \dots, \lambda_k$ paarweise verschieden

2. Bestimme für $i = 1, \dots, k$ jeweils eine Basis von $\text{Eig}(\varphi, \lambda_i)$
3. Bestimme mit dem Gram-Schmidt-Verfahren für $i = 1, \dots, k$ eine Orthonormalbasis $\mathcal{B}_i = (v_{i,1}, \dots, v_{i,r_i})$ von $\text{Eig}(\varphi, \lambda_i)$
4. Die Orthonormalbasis $\mathcal{B}_i, i = 1, \dots, k$ bilden zusammen eine Orthonormalbasis

$$\mathcal{B} = (v_{1,1}, \dots, v_{1,r_1}, \dots, v_{k,1}, \dots, v_{k,r_k})$$

des $(\mathbb{R}^n, \langle \cdot, \cdot \rangle)$ aus Eigenvektoren von A

5. Schreibe die Basisvektoren aus \mathcal{B} in Spalten von T . Es ist dann

$$T^{-1}AT = (\lambda_1, \dots, \lambda_1, \dots, \lambda_k, \dots, \lambda_k)E_n$$

Anmerkung Um $T \in SO(n)$ zu erreichen ersetze man gegebenenfalls $v_{1,1}$ durch $-v_{1,1}$.

Beispiel 24.16

$$A = \begin{pmatrix} 2 & -1 & 2 \\ -1 & 2 & 2 \\ 2 & 2 & -1 \end{pmatrix} \in M(3 \times 3, \mathbb{R})$$

Es ist $\chi_A^{char} = t^3 - 3t^2 - 9t + 27 = (t - 3)^2(t + 3)$. Es ist $\text{Eig}(A, 3) = \dots = \text{Lin} \left(\begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} \right)$. Nach

Beispiel 22.12 ist $\left(\frac{1}{\sqrt{5}} \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{30}} \begin{pmatrix} -1 \\ 5 \\ 2 \end{pmatrix} \right)$ eine Orthonormalbasis von $\text{Eig}(A, 3)$.

$\text{Eig}(A, -3) = \text{Lin} \left(\begin{pmatrix} 1 \\ 1 \\ -2 \end{pmatrix} \right) \Rightarrow \left(\frac{1}{\sqrt{6}} \begin{pmatrix} 1 \\ 1 \\ -2 \end{pmatrix} \right)$ ist Orthonormalbasis von $\text{Eig}(A, -3)$.

$$\Rightarrow \left(\frac{1}{\sqrt{5}} \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{30}} \begin{pmatrix} -1 \\ 5 \\ 2 \end{pmatrix}, \frac{1}{\sqrt{6}} \begin{pmatrix} 1 \\ 1 \\ -2 \end{pmatrix} \right)$$

ist Orthonormalbasis von $(\mathbb{R}^3, \langle \cdot, \cdot \rangle)$ aus Eigenvektoren von A . Mit

$$T = \begin{pmatrix} \frac{2}{\sqrt{5}} & -\frac{1}{\sqrt{30}} & \frac{1}{\sqrt{6}} \\ 0 & \frac{5}{\sqrt{30}} & \frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{5}} & \frac{2}{\sqrt{30}} & -\frac{2}{\sqrt{6}} \end{pmatrix} \quad \text{ist} \quad T^{-1}AT = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & -3 \end{pmatrix}$$

Es ist $\det(T) = -1$, also $T \in O(3) \setminus (3)$. Setzt man

$$T' := \begin{pmatrix} -\frac{2}{\sqrt{5}} & -\frac{1}{\sqrt{30}} & \frac{1}{\sqrt{6}} \\ 0 & \frac{5}{\sqrt{30}} & \frac{1}{\sqrt{6}} \\ -\frac{1}{\sqrt{5}} & \frac{2}{\sqrt{30}} & -\frac{2}{\sqrt{6}} \end{pmatrix} \quad \text{ist} \quad T'^{-1}AT' = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & -3 \end{pmatrix}$$

und es ist $T' \in SO(3)$.

25 Unitäre Räume

Definition 25.1 (Sesquilinearform) $V \mathbb{C}$ Vektorraum, $h : V \times V \rightarrow \mathbb{C}, (v, w) \mapsto h(v, w)$ heißt eine **Sesquilinearform** auf V genau dann wenn folgende Bedingungen erfüllt sind:

- (S1) $h(v_1 + v_2, w) = h(v_1, w) + h(v_2, w), h(\lambda v, w) = \lambda(h(v, w))$
- (S2) $h(v, w_1 + w_2) = h(v, w_1) + h(v, w_2), h(v, \lambda w) = \bar{\lambda}h(v, w)$

für alle $v_1, v_2, w_1, w_2, v, w \in V, \lambda \in \mathbb{C}$

Beispiel 25.2

$h : \mathbb{C}^n \times \mathbb{C}^n \rightarrow \mathbb{C}, h(x, y) := x^t \bar{y}$ ist eine Sesquilinearform auf \mathbb{C}^n (beachte $h(x, \lambda y) = x^t \bar{\lambda y} = \bar{\lambda} x^t y = \bar{\lambda} h(x, y)$), aber keine Bilinearform auf $\mathbb{C} * n$

Bemerkung 25.3 $V \mathbb{C}$ Vektorraum, $h : V \times V \rightarrow \mathbb{C}$ Sesquilinearform auf V . Dann induziert h eine „semilineare“ Abbildung

$$\Gamma : V \rightarrow V^*, w \mapsto h(\cdot, w)$$

das heißt $\Gamma(w_1 + w_2) = \Gamma(w_1) + \Gamma(w_2), \Gamma(\lambda w) = \bar{\lambda} \Gamma(w) \forall w_1, w_2, w \in V, \lambda \in \mathbb{C}$

Definition 25.4 (Darstellungsmatrix / Fundamentalmatrix) V endlichdimensional, \mathbb{C} Vektorraum, h Sesquilinearform auf $V, \mathcal{B} = (v_1, \dots, v_n)$ Basis von V

$$M_{\mathcal{B}}(h) = (h(v_i, v_j))_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$$

heißt die **Darstellungsmatrix (Fundamentalmatrix)** von h bezüglich \mathcal{B}

Bemerkung 25.5 V endlichdimensionaler \mathbb{C} Vektorraum, $\mathcal{B} = (v_1, \dots, v_n)$ Basis von V .

$$\text{Sesq}(V) := \{h : V \times V \rightarrow \mathbb{C} \mid h \text{ ist eine Sesquilinearform}\}$$

ist ein \mathbb{C} Vektorraum und Untervektorraum von $\text{Abb}(V \times V, \mathbb{C})$. Dann gilt: Die Abbildung $M_{\mathcal{B}} : \text{Sesq}(V) \rightarrow M(n \times n, \mathbb{C}), h \mapsto M_{\mathcal{B}}(h)$ ist ein Isomorphismus von \mathbb{C} Vektorräumen mit Umkehrabbildung $\Delta^{\mathcal{B}} : M(n \times n, \mathbb{C}) \rightarrow \text{Sesq}(V)$ mit

$$\Delta^{\mathcal{B}}(A)(v, w) = \Phi_{\mathcal{B}}^{-1}(v)^T A \overline{\Phi_{\mathcal{B}}^{-1}(w)}$$

Satz 25.6 V endlichdimensionaler \mathbb{C} Vektorraum, \mathcal{A}, \mathcal{B} Basen von V, h Sesquilinearform auf V . Dann gilt:

$$M_{\mathcal{B}}(h) = (T_{\mathcal{A}}^{\mathcal{B}})^T M_{\mathcal{A}}(h) \overline{T_{\mathcal{B}}^{\mathcal{A}}}$$

Definition 25.7 (hermitesch) $V \mathbb{C}$ Vektorraum, h Sesquilinearform auf V . h heißt **hermitesch** genau dann wenn:

$$h(w, v) = \overline{h(v, w)} \forall v, w \in V$$

Anmerkung In diesem Fall ist $h(v, v) = \overline{h(v, v)}$, das heißt $h(v, v) \in \mathbb{R} \forall v \in V$

Bemerkung 25.8 V endlichdimensionaler \mathbb{C} Vektorraum, h Sesquilinearform auf V, \mathcal{B} Basis von $V, A = M_{\mathcal{B}}(h)$. Dann sind äquivalent:

1. h ist hermitesch
2. $\bar{A}^t = A$

Anmerkung Matrizen $A \in M(n \times n, \mathbb{C})$ mit $\bar{A}^t = A$ heißen **hermitesche Matrizen**.

Definition 25.9 $V \subset \mathbb{C}$ Vektorraum, h hermitesche Form auf V . h heißt **positiv definit** genau dann wenn

$$h(v, v) > 0 \forall v \in V, v \neq 0$$

Eine positiv definite hermitesche Form nennt man auch ein **Skalarprodukt**.

Beispiel 25.10

$V = \mathbb{C}^n, \langle \cdot, \cdot \rangle : \mathbb{C}^n \times \mathbb{C}^n \rightarrow \mathbb{C}, \langle x, y \rangle := x^T \bar{y}$ ist ein Skalarprodukt auf \mathbb{C}^n (das **Standardskalarprodukt** auf \mathbb{C}^n):

- $\langle \cdot, \cdot \rangle$ ist sesquilinear (vergleiche 25.2)
- $\langle \cdot, \cdot \rangle$ ist hermitesch: $\langle y, x \rangle = y^T \bar{x} = (y^T \bar{x})^T = \bar{x}^T y = \overline{x^T \bar{y}} = \overline{\langle x, y \rangle}$
- $\langle \cdot, \cdot \rangle$ ist positiv definit:

$$\begin{aligned} \langle x, x \rangle &= x^T \bar{x} = \begin{pmatrix} x_1 & \dots & x_n \end{pmatrix} \begin{pmatrix} \bar{x}_1 \\ \vdots \\ \bar{x}_n \end{pmatrix} = x_1 \bar{x}_1 + \dots + x_n \bar{x}_n \\ &= |x_1|^2 + \dots + |x_n|^2 > 0 \text{ für } x \neq 0 \end{aligned}$$

Definition 25.11 (Unitärer Raum) Ein **unitärer Raum** ist ein Paar (V, h) , bestehend aus einem endlichdimensionalen \mathbb{C} Vektorraum V und einem Skalarprodukt h auf V .

Für den Rest des Abschnitts sei (V, h) stets ein unitärer Raum.

Anmerkung Analog zu Euklidischen Räumen definiert man die Begriffe: Norm, orthogonal, orthonormal, Orthogonalbasis, Orthonormalbasis, orthogonales Komplement. Es gilt dabei:

- Cauchy-Schwarz-Ungleichung: $|h(v, w)| \leq \|v\| \|w\| \forall v, w \in V$
- Gram-Schmidt-Verfahren (mit h statt γ) liefert Orthonormalbasis
- $V = U \hat{U}^\perp, U^{\perp\perp} = U$ für $U \subseteq V$ Untervektorraum

Definition 25.12 $(V, h_V), (W, h_W)$ unitäre Räume, $\varphi : V \rightarrow W$ lineare Abbildung. φ heißt **unitär** genau dann wenn:

$$h_W(\varphi(v_1), \varphi(v_2)) = h_V(v_1, v_2) \forall v_1, v_2 \in V$$

Bemerkung 25.13 $n = \dim V, \mathcal{B}$ Orthonormalbasis von (V, h) . Dann ist das Koordinatensystem $\Phi_{\mathcal{B}} : (\mathbb{C}^n, \langle \cdot, \cdot \rangle) \rightarrow (V, h)$ ein unitärer Isomorphismus.

Bemerkung 25.14 \mathcal{B} Orthonormalbasis von $(V, h), \varphi \in \text{End}(V), A = M_{\mathcal{B}}(\varphi)$. Dann sind äquivalent:

1. φ ist unitär
2. $\bar{A}^T A = E_n$

Bemerkung+Definition 25.15 $A \in M(n \times n, \mathbb{C})$. A heißt **unitär** genau dann wenn: $\bar{A}^T A = E_n$.

$$U(n) := \{A \in M(n \times n, \mathbb{C}) \mid A \text{ ist unitär}\}$$

$U(n)$ ist eine Gruppe bezüglich „ \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** von Rang n .

Bemerkung 25.16 $\mathcal{B} = (v_1, \dots, v_n)$ Orthonormalbasis von (V, h) , $\mathcal{B}^* = (v_1^*, \dots, v_n^*)$ duale Basis. Dann ist die Abbildung

$$\Gamma : V \rightarrow V^*, w \mapsto h(\cdot, w)$$

ein Semiisomorphismus mit $\Gamma(v_i) = v_i^*$ für $i = 1, \dots, n$.

Satz+Definition 25.17 $(V, h_V), (W, h_W)$ unitäre Räume, $\varphi : V \rightarrow W$ lineare Abbildung, \mathcal{A} Orthonormalbasis von (V, h_V) , \mathcal{B} Orthonormalbasis von (W, h_W) . Dann gilt:

1. Es gibt genau eine lineare Abbildung $\varphi^{ad} : W \rightarrow V$ mit $h_W(\varphi(v), w) = h_V(v, \varphi^{ad}(w)) \forall v \in V, w \in W$, φ^{ad} heißt die **zu φ adjungierte Abbildung**
2. $M_{\mathcal{A}}^{\mathcal{B}}(\varphi^{ad}) = \overline{M_{\mathcal{B}}^{\mathcal{A}}(\varphi)}^T$

Beweis 1. Wie im reellen Fall betrachte man das Diagramm

$$\begin{array}{ccc} V & \xrightarrow{\Gamma_V} & W \\ \varphi^{ad} \uparrow & & \uparrow \varphi^* \\ V^* & \xrightarrow{\Gamma_W} & W^* \end{array}$$

und setzen $\varphi^{ad} := \Gamma_V^{-1} \circ \varphi^* \circ \Gamma_W$. φ^{ad} ist linear, da sowohl Γ_V als auch Γ_W semilinear sind. Rest wie im reellen Fall

2. Sei $\mathcal{A} = (v_1, \dots, v_n), \mathcal{B} = (w_1, \dots, w_m), M_{\mathcal{B}}^{\mathcal{A}}(\varphi) = (a_{ij}), M_{\mathcal{A}}^{\mathcal{B}}(\varphi^{ad}) = (b_{ij})$

$$\begin{aligned} \Rightarrow \varphi(v_j) &= \sum_{k=1}^m a_{kj} w_k, \varphi^{ad} = \sum_{k=1}^n b_{ki} v_k \\ \Rightarrow a_{ij} &= h_W \left(\sum_{k=1}^m a_{kj} w_k, w_i \right) = h_W(\varphi(w_j, w_i)) = h_V(v_j, \varphi^{ad}(w_i)) \\ &= h_V \left(v_j, \sum_{k=1}^n b_{ki} v_k \right) = h_V(v_j, b_{ji} v_j) = \overline{b_{ji}} h(v_j, v_j) = \overline{b_{ji}} \end{aligned} \quad \square$$

Bemerkung 25.18 $\varphi \in \text{End}(V)$. Dann gilt:

1. $\ker \varphi^{ad} = (\text{im } \varphi)^\perp$
2. $\text{im } \varphi^{ad} = (\ker \varphi)^\perp$

Definition 25.19 $\varphi \in \text{End}(V)$. φ heißt *selbstadjungiert genau dann wenn: $\varphi = \varphi^{ad}$

Bemerkung 25.20 $\varphi \in \text{End}(V)$, \mathcal{B} Orthonormalbasis von (V, h) , $A = M_{\mathcal{B}}(\varphi)$. Dann sind äquivalent:

1. φ selbstadjungiert
2. $\bar{A}^T = A$, das heißt A ist hermitesch

Bemerkung 25.21 $\varphi \in \text{End}(V)$ selbstadjungiert. Dann sind alle Eigenwerte von φ reell.

Beweis Sei $\lambda \in \mathbb{C}$ Eigenwert von φ , v Eigenvektor zum Eigenwert λ .

$$\implies \lambda h(v, v) = h(\lambda v, v) = h(\varphi(v), v) = h(v, \varphi^{ad}(v)) = h(v, \varphi(v)) = h(v, \lambda v) = \bar{\lambda} h(v, v)$$

$$\implies \lambda = \bar{\lambda} \implies \lambda \in \mathbb{R}$$

□

Definition 25.22 $\varphi \in \text{End}(V)$. φ heißt **normal** genau dann wenn: $\varphi^{ad} \circ \varphi = \varphi \circ \varphi^{ad}$. $A \in M(n \times n, \mathbb{C})$ heißt **normal** genau dann wenn: $\bar{A}^T A = A \bar{A}^T$

Anmerkung Ist \mathcal{B} eine Orthonormalbasis von (V, h) , dann: φ normal $\iff M_{\mathcal{B}}(\varphi)$ normal.

Bemerkung 25.23 $\varphi \in \text{End}(V)$. Dann gilt:

1. φ unitär $\implies \varphi$ normal
2. φ selbstadjungiert $\implies \varphi$ normal

Für $A \in M(n \times n, \mathbb{C})$ gilt: A unitär $\implies A$ normal, A hermitesch $\implies A$ normal.

Beweis 1. Seien $v, w \in V \implies h(v, \varphi^{-1}(w)) = h(\varphi(v), \varphi(\varphi^{-1}(w))) = h(\varphi(v), w) \implies \varphi^{ad} = \varphi^{-1} \implies \varphi^{ad} \circ \varphi = \varphi^{-1} \circ \varphi = \text{id}_V = \varphi \circ \varphi^{-1} = \varphi \circ \varphi^{ad}$

2. φ selbstadjungiert $\implies \varphi = \varphi^{ad} \implies \varphi^{ad} \circ \varphi = \varphi \circ \varphi = \varphi \circ \varphi^{ad}$

□

Satz 25.24 $\varphi \in \text{End}(V)$ normal. Dann gilt:

1. $\ker \varphi^{ad} = \ker \varphi$
2. $\text{im } \varphi^{ad} = \text{im } \varphi$

Insbesondere ist $V = \ker \varphi \hat{\oplus} \text{im } \varphi$

Beweis 1. Es gilt:

$$\begin{aligned} v \in \ker \varphi &\iff 0 = h(\varphi(v), \varphi(v)) = h(v, \varphi^{ad}(\varphi(v))) = h(v, \varphi(\varphi^{ad}(v))) \\ &= \overline{h(\varphi(\varphi^{ad}(v)), v)} = h(\varphi^{ad}(v), \varphi^{ad}(v)) \iff \varphi^{ad}(v) = 0 \\ &\iff v \in \ker \varphi^{ad} \end{aligned}$$

2. Es ist $\text{im } \varphi^{ad} = (\ker \varphi)^\perp = (\perp \varphi^{ad})^\perp = ((\text{im } \varphi)^\perp)^\perp = \text{im } \varphi$

$$\implies V = \ker \varphi \hat{\oplus} (\ker \varphi)^\perp = \ker \varphi \hat{\oplus} \text{im } (\varphi^{ad}) = \ker \varphi \hat{\oplus} \text{im } \varphi$$

□

Bemerkung 25.25 $\varphi \in \text{End}(V)$ normal, $\lambda \in \mathbb{C}$. Dann gilt:

1. $\varphi - \lambda \text{id}_V$ ist normal
2. $\text{Eig}(\varphi, \lambda) = \text{Eig}(\varphi^{ad}, \bar{\lambda})$

Beweis 1. Setze $\psi := \varphi - \lambda \text{id}_V$. Für $v, w \in V$ ist $h(\lambda v, w) = h(v, \bar{\lambda} w)$, das heißt $(\lambda \text{id}_V)^{ad} = \bar{\lambda} \text{id}_V$

$$\begin{aligned} &\implies \psi^{ad} = \varphi^{ad} - \bar{\lambda} \text{id}_V \\ &\implies \psi^{ad} = \varphi^{ad} - \bar{\lambda} \text{id}_V \\ &\implies \psi^{ad} \circ \psi = (\varphi^{ad} - \bar{\lambda} \text{id}_V) \circ (\varphi - \lambda \text{id}_V) = \underbrace{\varphi^{ad} \circ \varphi}_{=\varphi \circ \varphi^{ad}} - \bar{\lambda} \varphi - \lambda \varphi^{ad} + \lambda \bar{\lambda} \text{id}_V \\ &= (\varphi - \lambda \text{id}_V) \circ (\varphi^{ad} - \bar{\lambda} \text{id}_V) = \psi \circ \psi^{ad} \end{aligned}$$

$$2. \text{Eig}(\varphi, \lambda) = \ker \psi = \ker \psi^{ad} = \ker(\varphi^{ad} - \bar{\lambda} \text{id}_V) = \text{Eig}(\varphi^{ad}, \bar{\lambda}) \quad \square$$

Satz 25.26 (Spektralsatz für normale Endomorphismen) $\varphi \in \text{End}(V)$. Dann sind äquivalent:

1. Es gibt eine Orthonormalbasis von (V, h) aus Eigenvektoren von φ .
2. φ ist normal

Beweis 1. \implies 2. Sei $\mathcal{B} = (v_1, \dots, v_n)$ eine Orthonormalbasis von (V, h) aus Eigenvektoren von φ zu Eigenwerten $\lambda_1, \dots, \lambda_n \in \mathbb{C}$. Es ist $(\varphi \circ \varphi^{ad})(v_i) = \varphi(\varphi^{ad}(v_i)) = \varphi(\bar{\lambda}_i v_i) = \bar{\lambda}_i \varphi(v_i) = \bar{\lambda}_i \lambda_i v_i = (\varphi^{ad} \circ \varphi)(v_i) \forall i = 1, \dots, n \implies \varphi \circ \varphi^{ad} = \varphi^{ad} \circ \varphi$

2. \implies 1. per Induktion nach $n = \dim V$.

Induktionsanfang: $n = 0$: trivial

Induktionsschritt: $n \geq 1$: Sei $\lambda_1 \in \mathbb{C}$ ein Eigenwert von φ . Sei $U = \text{Eig}(\varphi, \lambda_1) = \ker(\varphi - \lambda_1 \text{id}_V)$. Sei (v_1, \dots, v_r) eine Orthonormalbasis von $\left(U, h|_{n \times n}\right)$. Nach 25.25 ist $\psi := \varphi - \lambda_1 \text{id}_V$ normal

$$\begin{aligned} V &= \ker \psi \hat{\oplus} \text{im } \psi \\ &= \text{Eig}(\varphi, \lambda_1) \hat{\oplus} \underbrace{\text{im}(\varphi - \lambda_1 \text{id}_V)}_{=: W} \end{aligned}$$

$$\text{Es ist } \varphi(W) = \varphi(\varphi - \lambda_1 \text{id}_V)(V) = ((\varphi - \lambda_1 \text{id}_V) \circ \varphi)(V) = (\varphi - \lambda_1 \text{id}_V) \left(\underbrace{\varphi(V)}_{\subseteq V} \right) \subseteq \text{im}(\varphi - \lambda_1 \text{id}_V) = W.$$

W. Außerdem:

$$\begin{aligned} \varphi^{ad}(W) &= \varphi^{ad}(\varphi - \lambda_1 \text{id}_V)(V) = (\varphi^{ad} \circ \varphi - \lambda_1 \varphi^{ad})(V) \\ &= (\varphi \circ \varphi^{ad} - \lambda_1 \varphi^{ad})(V) = ((\varphi - \lambda_1 \text{id}_V) \circ \varphi^{ad})(V) \subseteq W \end{aligned}$$

$\varphi|_W^W$ ist normal, denn: Nach Eindeutigkeit der adjungierten Abbildung ist $\left(\varphi|_W^W\right)^{ad} = (\varphi^{ad})|_W^W$

$$\begin{aligned} (\varphi|_W^W)^{ad} \circ \varphi|_W^W &= (\varphi^{ad})|_W^W \circ \varphi|_W^W = (\varphi^{ad} \circ \varphi)|_W^W = (\varphi \circ \varphi^{ad})|_W^W \\ &= \varphi|_W^W \circ (\varphi^{ad})|_W^W = \varphi|_W^W \circ \left(\varphi|_W^W\right)^{ad} \end{aligned}$$

Nach Induktionsanfang existiert eine Orthonormalbasis (v_{r+1}, \dots, v_n) von $\left(V, h|_{W \times W}\right)$ aus Eigenvektoren von $\varphi \implies (v_1, \dots, v_n)$ ist Orthonormalbasis von (V, h) aus Eigenvektoren von φ . \square

Anmerkung Insbesondere gilt:

- Für jedes selbstadjungierten / unitären Endomorphismus existiert eine Orthonormalbasis aus Eigenvektoren
- Jede reelle orthogonale Matrix ist **über** \mathbb{C} diagonalisierbar.

Achtung: Über \mathbb{R} reicht „normal“ nicht aus: Es gibt orthogonale Matrizen, die über \mathbb{R} nicht diagonalisierbar sind

(zum Beispiel $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ (Drehung um $\pi/2$))

Folgerung 25.27 $A \in M(n \times n, \mathbb{C})$. Dann sind äquivalenz:

1. A ist normal
2. Es gibt ein $T \in U(n)$, sodass

$$T^{-1}AT = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

$\lambda_1, \dots, \lambda_n$ Eigenwerte von A

Beweis Wende 25.26 auf $(\mathbb{C}^n, \langle \cdot, \cdot \rangle)$ und $\varphi = \tilde{A}$ an. □

26 Ringe, Ideale und Teilbarkeit

In diesem Abschnitt seien R, S stets kommutative Ringe (bei uns immer mit Eins)

Definition 26.1 (Ringhomomorphismus) $\varphi : R \rightarrow S$ Abbildung. φ heißt **Ringhomomorphismus** genau dann wenn folgende Bedingungen erfüllt sind:

- (RH1) $\varphi(a + b) = \varphi(a) + \varphi(b) \forall a, b \in R$
- (RH2) $\varphi(ab) = \varphi(a)\varphi(b) \forall a, b \in R$
- (RH3) $\varphi(1_R) = 1_S$

Definition 26.2 (Ideal) $I \subseteq R$. I heißt ein **Ideal** in R genau dann wenn die folgenden Bedingungen erfüllt sind:

- (I1) $0 \in I$
- (I2) $a, b \in I \implies a + b \in I$
- (I3) $r \in R, a \in I \implies ra \in I$

Beispiel 26.3

1. $\{0\}, R$ sind Ideale in R
2. Für $n \in \mathbb{Z}$ ist $n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}$ ist ein Ideal

Bemerkung+Definition 26.4 $\varphi : R \rightarrow S$ Ringhomomorphismus. Dann gilt:

1. $J \subseteq S$ Ideal $\implies \varphi^{-1}(J) \subseteq R$ Ideal
2. $\ker \varphi := \{a \in R \mid \varphi(a) = 0\} \subseteq R$ Ideal
3. φ injektiv $\iff \ker \varphi = \{0\}$

4. $I \subseteq R$ Ideal und φ surjektiv $\implies \varphi(I) \subseteq S$ Ideal

5. im $\varphi := \varphi(R)$ ist ein Unterring von S (das heißt ein Ring bezüglich der eingeschränkten Verknüpfungen.)

Beweis 1. (I1): $0 \in \varphi^{-1}(J)$, denn $\varphi(0) = \varphi(0+0) = \varphi(0) + \varphi(0) \implies \varphi(0) = 0 \in J \implies 0 \in \varphi^{-1}(J)$

(I2): $a, b \in \varphi^{-1}(J) \implies \varphi(a), \varphi(b) \in J \implies \varphi(a+b) = \varphi(a) + \varphi(b) \in J \implies a+b \in \varphi^{-1}(J)$

(I3): $r \in R, a \in \varphi^{-1}(J) \implies \varphi(a) \in J \implies \varphi(ra) = \varphi(r)\varphi(a) \in J \implies ra \in \varphi^{-1}(J)$

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

3., 4., 5.: nachrechnen □

Anmerkung 4. wird falsch, wenn man die Voraussetzung φ surjektiv weglässt: Die kanonische Inklusion $i: \mathbb{Z} \rightarrow \mathbb{Q}, x \mapsto x$ ist ein Ringhomomorphismus, \mathbb{Z} ist ein Ideal in \mathbb{Z} , aber $\mathbb{Z} = i(\mathbb{Z})$ ist kein Ideal in \mathbb{Q} , denn:

$$\underbrace{\frac{1}{3}}_{\in \mathbb{Q}} \cdot \underbrace{2}_{\in \mathbb{Z}} = \frac{2}{3} \notin \mathbb{Z}$$

\mathbb{Z} ist zumindest ein Unterring von \mathbb{Q} .

Satz+Definition 26.5 $I \subseteq R$ Ideal. Dann ist durch $r_1 \sim r_2 \stackrel{\text{Def}}{\iff} r_1 - r_2 \in I$ eine Äquivalenzrelation auf R gegeben, welche die zusätzliche Eigenschaft

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

hat („Kongruenzrelation“). Die Äquivalenzklasse von $r \in R$ ist durch

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

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

Beweis 1. „ \sim “ ist Äquivalenzrelation: nachrechnen

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

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

Außerdem:

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

Satz+Definition 26.6 $I \subseteq R$ Ideal. Dann wird R/I mit der Addition

$$+ : R/I \times R/I \rightarrow R/I, \bar{r} + \bar{s} := \overline{r+s}$$

und der Multiplikation

$$\cdot : R/I \times R/I \rightarrow R/I, \bar{r} \cdot \bar{s} := \overline{rs}$$

zu einem kommutativen Ring, dem **Faktorring (Restklassenring)** R/I . Die Abbildung $\pi : R \rightarrow R/I, r \mapsto \bar{r}$ ist ein surjektiver Ringhomomorphismus mit $\ker \pi = I$.

Beweis Wohldefiniertheit von „+“, „·“: Nach 26.5 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 von R .

π ist Ringhomomorphismus nach Konstruktion: $\pi(a + b) = \overline{a + b} = \overline{a} + \overline{b} = \pi(a) + \pi(b)$, analog für „·“, $\pi(1) = \bar{1}$

$\ker \pi = \{r \in R \mid \bar{r} = \bar{0}\} = \{r \in R \mid r \sim 0\} = \{r \in R \mid r - 0 \in I\} = I$ □

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

Beispiel 26.7

Ist $R = \mathbb{Z}, I = n\mathbb{Z}$ mit $n \in \mathbb{N}$, dann erhält man die aus der LA1 bekannten Restklassenringe $\mathbb{Z}/n\mathbb{Z}$ (vergleiche 6.4).

Satz 26.8 (26.8 (Homomorphiesatz für Ring)) $\varphi : R \rightarrow S$ Ringhomomorphismus. Dann gibt es einen Ringisomorphismus

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

Beweis Wohldefiniertheit von Φ : Seien $r_1, r_2 \in R$ mit $\bar{r}_1 = \bar{r}_2$

$$\implies r_1 - r_2 \in \ker \varphi \implies \varphi(r_1 - r_2) = 0 \implies \varphi(r_1) = \varphi(r_2)$$

Φ ist 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 „·“, $\Phi(\bar{1}) = \varphi(1) = 1$

Φ ist injektiv: Sei $r \in R$ mit $\Phi(\bar{r}) = 0$

$$\implies \varphi(r) = 0 \implies r \in \ker \varphi \implies \bar{r} = r + \ker \varphi = \ker \varphi = \bar{0}$$

das heißt $\ker \Phi = \{\bar{0}\}$.

Φ ist surjektiv: nach Konstruktion. □

Beispiel 26.9

K Körper, $R = K[t], \varphi : K[t] \rightarrow K, f \mapsto f(0)$. φ ist Ringhomomorphismus (nachrechnen), $\text{im } \varphi = K, \ker \varphi = \{f \in K[t] \mid \text{im } f(0) = 0\} = \{fg \mid g \in K[t]\} = tK[t]$. Wir erhalten einen Ringisomorphismus

$$\Phi : K[t]/tK[t] \rightarrow K, f + tK[t] \mapsto f(0)$$

Definition 26.10 (26.10) $x \in R$ heißt **Nullteiler** $\stackrel{\text{Def}}{\iff}$ Es existiert $y \in R, y \neq 0$ mit $xy = 0$. R heißt **Nullteiler (Integritätsbereich)** $\stackrel{\text{Def}}{\iff} R \neq 0$ und $0 \in R$ der einzige Nullteiler in R .

Anmerkung $R \neq 0 \implies 0$ ist ein Nullteiler in R (wegen $0 \cdot 1 = 0, 0 \neq 1$)

Beispiel 26.11

1. \mathbb{Z} ist nullteilerfrei

2. $\bar{2} \in \mathbb{Z}/6\mathbb{Z}$ ist Nullteiler wegen $\bar{2} \cdot \bar{3} = \bar{0}$ ist $\mathbb{Z}/6\mathbb{Z}$

3. Analog zu $K[t]$ kann man den Polynomring $R[t]$ erklären. Es gilt dann: R nullteilerfrei $\implies R[t]$ nullteilerfrei. (Übungen)

Bemerkung+Definition 26.12 (Einheit) $v \in R$ heißt **Einheit** $\stackrel{\text{Def}}{\iff}$ es existiert ein $y \in R$ mit $xy = 1$. $R^* := \{x \in R \mid x \text{ ist Einheit}\}$ bildet eine abelsche Gruppe bezüglich „·“.

Beweis nachrechnen. □

Beispiel 26.13

1. $\mathbb{Z}^* = \{1, -1\}$, dann: $1 \cdot 1 = 1, (-1)(-1) = 1, ab = 1 \implies |a||b| = 1 \implies |a| = |b| = 1$
2. K Körper $\implies K^* = K \setminus \{0\}$
3. $R[t]^* = R^*$ (Übungen)

Definition 26.14 $a_1, \dots, a_n \in R, I \subseteq R$ Ideal.

$$(a_1, \dots, a_n) := \left\{ \sum_{i=1}^n a_i r_i \mid r_1, \dots, r_n \in R \right\}$$

heißt das **von** a_1, \dots, a_n **erzeugte Ideal**. I heißt **Hauptideal** $\stackrel{\text{Def}}{\iff}$ es existiert ein $a \in R$ mit $I = (a) = \{ra \mid r \in R\} =: Ra$.

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

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

Bemerkung 26.15 \mathbb{Z} ist ein Hauptidealring. Ist $I \subseteq \mathbb{Z}$ ein Ideal, dann existiert ein eindeutig bestimmtes $n \in \mathbb{N}_0$ mit

$$I = (n) = n\mathbb{Z}$$

Beweis \mathbb{Z} **nullteilerfrei**: klar.

Existenz: Sei $I \subseteq \mathbb{Z}$ Ideal.

1. Fall: $I = \{0\} = (0)$, dann fertig
2. Fall: $I \neq \{0\}$. Mat $a \in I$ ist auch $-a = (-1)a \in I$ somit $I \cap \mathbb{N} \neq \emptyset$. $I \cap \mathbb{N}$ besitzt ein kleinstes Element b . Behauptung: $I = (b)$
 \supseteq „ $x \in (b) \implies$ es existiert ein $r \in \mathbb{Z}$ mit $x = rb \implies x \in I$ “
 \subseteq „Sei $x \in I \implies$ es existieren $q, r \in \mathbb{Z}$ mit $x = qb + r, 0 \leq r < b \implies r = x - qb \in I$. Wegen Minimalität von b in $I \cap \mathbb{N}$ folgt $r = 0 \implies x = qb \in (b)$ “

Eindeutigkeit: Seien $m, n \in \mathbb{N}_0$ mit $(m) = (n)$. Offenbar gilt: $m = 0 \iff n = 0$. Im Folgenden seien $m, n \neq 0$. Wegen $(m) = (n)$ ist $m \in (n), n \in (m) \implies$ es existieren $r_1, r_2 \in \mathbb{Z}$ mit $m = r_1 n$ und $n = r_2 m$

$$\implies m = r_1 n = r_1 r_2 m \implies r_1 r_2 = 1 \implies r_1 = r_2 = 1 \vee r_1 = r_2 = -1 \xrightarrow{m, n \in \mathbb{N}_0}$$

$$r_1 = r_2 = 1 \implies m = n$$

□

Beispiel 26.16

$\mathbb{Z}[t]$ ist kein Hauptidealring: Es gibt $f \in \mathbb{Z}[t]$ mit $(2, t) = (f)$, dann: Annahme: Es existiert $f \in \mathbb{Z}[t]$ mit $2 = hf \implies \deg h = \deg f = 0$, das heißt f ist konstantes Polynom, etwa $f = a$ für ein $a \in \mathbb{Z}$. Außerdem existiert $\tilde{h} \in \mathbb{Z}[t]$ mit $t = \tilde{h}f = \tilde{h}a \implies a = \pm 1 \implies f = \pm 1$. Aber: $\pm 1 \notin (2, t)$, dann andernfalls existieren $u, v \in \mathbb{Z}[t]$ mit $\pm 1 = 2u + tv \xrightarrow{t=0} \pm 1 = 2u(0) + 0 \cdot v(0) = 2u(0)$

Definition 26.17 R nullteilerfrei, $a, b \in R$. b heißt ein **Teiler** von a (Notation: $b \mid a$) $\stackrel{\text{Def}}{\iff}$ es existiert ein $c \in R$ mit $a = bc$.

a, b heißen assoziiert (Notation: $a \hat{=} b$) $\stackrel{\text{Def}}{\iff} a \mid b$ und $b \mid a$

Beispiel 26.18

$$R = \mathbb{Z}, a \in \mathbb{Z} \implies a \stackrel{\wedge}{=} -a$$

Bemerkung 26.19 R nullteilerfrei, $a, b \in R$. Dann sind äquivalent:

1. $a \stackrel{\wedge}{=} b$
2. Es existiert $e \in R^*$ mit $a = be$
3. $(a) = (b)$

Beweis 1. \implies 2. Sei $a \stackrel{\wedge}{=} b \implies a \mid b$ und $b \mid a \implies$ es existieren $c, d \in R$ mit $b = ac, a = bd$

$$\implies b = ac = bdc \implies b(1 - dc) = 0$$

a) Fall: $b = 0 \implies a = bd = 0$. Setze $e := 1$, fertig: $a = b \cdot 1$

b) Fall: $b \neq 0 \implies 1 - dc = 0 \implies dc = 1 \implies c, d \in R^*$. Setze $e := d$, dann $a = bd = bc$

2. Sei $a = be$ mit $e \in R^* \implies a \in (b) \implies (a) \subseteq (b)$. Wegen $e \in R^*$ ist $b = e^{-1}a \implies (b) \subseteq (a)$

3. Sei $(a) = (b) \implies a \in (b) \implies$ es existiert $c \in R$ mit $a = bc \implies b \mid a$. Analog: $a \mid b$ also $a \stackrel{\wedge}{=} b \quad \square$

Definition 26.20 R nullteilerfrei, $a_1, \dots, a_n \in R$. $d \in R$ heißt **größter gemeinsamer Teiler** von $a_1, \dots, a_n \stackrel{\text{Def}}{\iff}$ Die folgenden Bedingungen sind erfüllt:

- (GGT1) $d \mid a_1, \dots, d \mid a_n$
- (GGT2) $c \mid a_1, \dots, c \mid a_n \iff c \mid d$

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

Anmerkung • Seien $d_1, d_2 \in \text{GGT}(a_1, \dots, a_n)$, dann folgt $d_1 \mid d_2$ und $d_2 \mid d_1$, also $d_1 \stackrel{\wedge}{=} d_2$.

- Ist $d \in \text{GGT}(a_1, \dots, a_n)$ und $d' \stackrel{\wedge}{=} d$, dann ist $d' \in \text{GGT}(a_1, \dots, a_n)$
- Ohne zusätzliche Voraussetzungen an R kann man im allgemeinen nicht erwarten, dass $\text{GGT}(a_1, \dots, a_n) \neq \emptyset$. Zum Beispiel ist $R = \mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ ist $\text{GGT}(4, 2 \cdot (1 + \sqrt{-3})) = \emptyset$ (Übungen)

Bemerkung 26.21 R Hauptidealring, $a_1, \dots, a_n \in R$. Dann gilt:

1. $\text{GGT}(a_1, \dots, a_n) \neq \emptyset$
2. $d \in \text{GGT}(a_1, \dots, a_n) \iff (d) = (a_1, \dots, a_n)$

Beweis 1. R Hauptidealring \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): $a_1 \in (a_1, \dots, a_n) = (\tilde{d}) \implies \tilde{d} \mid a_i \forall i = 1, \dots, n$

(GGT2): Wegen $\tilde{d} \in (a_1, \dots, a_n)$ existieren $r_1, \dots, r_n \in R$ mit $\tilde{d} = r_1 a_1 + \dots + r_n a_n$. Ist $c \in R$ mit $c \mid a_1, \dots, c \mid a_n$, dann folgt $c \mid r_1 a_1 + \dots + r_n a_n = \tilde{d}$

2. „ \implies “ $d \in \text{GGT}(a_1, \dots, a_n) \implies d \stackrel{\wedge}{=} \tilde{d} \implies (d) = (\tilde{d}) = (a_1, \dots, a_n)$ „ \iff “ Sei $(d) = (a_1, \dots, a_n) \implies d \in \text{GGT}(a_1, \dots, a_n)$ mit Argument aus dem Beweis von 1. \square

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 $\mathbb{Z}^* = \{\pm 1\}$). Man nennt dann d **den** größten gemeinsamen Teiler von a_1, \dots, a_n

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

- Im Fall $R = K[t]$ (wobei K Körper, in 27, dies ein Hauptidealring), $f_1, \dots, f_n \in K[t]$, nicht alle $f_i = 0$, existiert ein eindeutig bestimmtes normiertes Polynom $d \in K[t]$ mit $d \in \text{GGT}(f_1, \dots, f_n)$ (beachte: $K[t]^* = K^*$). Man nennt

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

den größten gemeinsamen Teiler von f_1, \dots, f_n und setzt

$$\text{ggT}(0, \dots, 0) := 0$$

Folgerung 26.22 R Hauptidealring, $a, b \in R$, $d \in \text{GGT}(a, b)$. Dann existieren $u, v \in R$ mit $d = ua + vb$.

Beweis aus 26.21: $(d) = (a, b)$ □

Definition 26.23 R nullteilerfrei, $p \in R \setminus (R^* \cup \{0\})$

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

Anmerkung p irreduzibel / Primelement, $p' \trianglelefteq p \implies p'$ irreduzibel / Primelement

Beispiel 26.24

irreduzible Elemente in $\mathbb{Z} = \text{Primzahlen } p \text{ aus } \mathbb{N} \text{ sowie deren Negative } -p$. Primelemente in \mathbb{Z} ?

Frage: Zusammenhang zwischen irreduziblen Elementen und Primelementen?

Bemerkung 26.25 R nullteilerfrei, $p \in R \setminus (R^* \cup \{0\})$ Primelement. Dann ist p irreduzibel.

Beweis 1. Wir setzen $S := R/(p)$. Behauptung S ist nullteilerfrei, denn: Wegen $p \notin R^*$ ist $(p) \neq R$, das heißt $S \neq 0$. Sind $\bar{x}, \bar{y} \in S$ mit $\bar{x}\bar{y} = \bar{0}$ und $\bar{y} \neq \bar{0}$, das heißt $xy \in (p)$ und $y \notin (p) \implies p \mid xy$ und $p \nmid y \implies p \mid x \implies \bar{x} = \bar{0}$

2. Sei $p = ab$ mit $a, b \in R$. In $s = R/(p)$ ist $\bar{0} = \bar{p} = \bar{a}\bar{b} \implies \bar{a} = \bar{0} \vee \bar{b} = \bar{0}$. Ohne Einschränkung $\bar{a} = \bar{0} \implies$ Es existierte $d \in R$ mit $a = pd \implies p = ab = pdb \implies p(1 - db) = 0 \implies 1 - db = 0 \implies db = 1 \implies b \in R^*$ □

Anmerkung Es gibt Beispiele für irreduzible Elemente, die keine Primelemente sind (Übungen)

Satz 26.26 R Hauptidealring, $p \in R \setminus (R^* \cup \{0\})$. Dann sind äquivalent:

1. p ist irreduzibel
2. p ist Primelement

Beweis 2. \implies 1. aus 26.25

1. \impliedby 2. Sei p irreduzibel.

- a) Behauptung: Ist $I \subseteq R$ mit $(p) \subsetneq I$, dann ist $I = R$, denn: Sei $(p) \subsetneq I$. Da R Hauptidealring existiert $a \in R$ mit $I = (a) \implies \exists c \in R : p = ac \implies a \in R^* \vee c \in R^*$. Falls $c \in R^*$, dann $(p) = (a) = I$. Also $a \in R^*$, das heißt $(a) = I = R$.
- b) $R/(p)$ ist ein Körper, denn: Sei $\bar{x} \in R/(p)$, $\bar{x} \neq \bar{0} \implies x \notin (p) \implies I := (x, p)$ ist ein Ideal in R mit $(p) \subsetneq I \implies I = R \implies 1 \in I \implies \exists u, v \in R : 1 = ux + vp \implies \bar{1} = \bar{u}\bar{x} + \bar{v}\bar{p} = \bar{u}\bar{x}$
 $\quad \quad \quad \underbrace{\bar{p}}_{=0}$
- c) p ist Primelement, denn: Seien $a, b \in R$ mit $p \mid ab \implies$ in $R/(p)$ ist $\bar{0} = \bar{p} = \bar{a}\bar{b}$. Nach 2. ist $R/(p)$ ein Körper, also nullteilerfrei (6.11) $\implies \bar{a} = \bar{0} \vee \bar{b} = \bar{0} \implies p \mid a \vee p \mid b$ \square

Anmerkung • Beweis hat gezeigt: R Hauptidealring, p irreduzibles Element in R , dann ist $R/(p)$ ein Körper.

- Primelement in \mathbb{Z} = irreduzibles Element in \mathbb{Z}

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

Definition 26.27 R nullteilerfrei. R heißt **faktoriell** $\stackrel{\text{Def}}{\iff}$ Jedes $a \in R \setminus (R^* \cup \{0\})$ lässt sich eindeutig bis auf Reihenfolge und Assoziiertheit als Produkt irreduzibler Elemente aus R schreiben, das heißt es existieren irreduzible Elemente $p_1, \dots, p_r \in R$ mit $a = p_1 \cdot \dots \cdot p_r$ und sind $q_1, \dots, q_s \in R$ irreduzible Elemente mit $a = q_1 \cdot \dots \cdot q_s$, so ist $r = s$ und nach Umordnen ist $p_i \stackrel{\wedge}{=} q_i$ für $i = 1, \dots, r$

Ziel: Hauptidealringe sind faktoriell.

Definition 26.28 R heißt **noethersch** $\stackrel{\text{Def}}{\iff}$ 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 26.29 R Hauptidealring. Dann ist R noethersch.

Beweis Sei $I_1 \subseteq I_2 \subseteq \dots$ eine aufsteigende Kette von Idealen aus R . Setze

$$I := \cup_{k \geq 1} I_k$$

1. I ist ein Ideal in R , dann:

$$(1) 0 \in I_k \forall k \in \mathbb{N} \implies 0 \in I$$

$$(2) \text{ Seien } a, b \in I \implies \exists k, l \in \mathbb{N} : a \in I_k, b \in I_l. \text{ Mit } m := \max\{k, l\} \text{ ist } a, b \in I_m \implies a + b \in I_m \subseteq I$$

$$(3) a \in I, r \in R \implies \exists k \in \mathbb{N} : a \in I_k \implies ra \in I_k \subseteq I$$

2. Wegen 1. und R Hauptidealring existiert ein $a \in R$ mit $I = (a)$, insbesondere $a \in I \implies \exists n \in \mathbb{N} : a \in I_n \implies (a) \subseteq I_n \subseteq I = (a) \implies I_n = I \implies I_k = I = I_n \forall k \geq n$ \square

Satz 26.30 R Hauptidealring. Dann ist R faktoriell.

Beweis 1. Existenz von Zerlegung in irreduzible Elemente. Setze

$$M := \{(a) \mid a \in R \setminus (R^* \cup \{0\}) \mid \text{besitzt keine Faktorisierung in irreduziblen Elementen}\}$$

M ist wohldefiniert, da Bedingung an a invariant unter Assoziativität.

Annahme: $M \neq \emptyset$

Wegen 26.29 existiert bezüglich „ \subseteq “ maximales Element $I \in M$, denn: Anderenfalls existiert zu jedem $I \in M$ ein $I' \in M$ mit $I \subsetneq I'$, das liefert eine unendliche strikt aufsteigende Kette von von Idealen in R \nrightarrow zu R noethersch.

Es existiert $a \in R$ mit $I = (a)$. a ist nicht irreduzibel, denn für a irreduzibel wäre a selbst eine Faktorisierung in irreduzible Elemente $\Rightarrow I = (a) \not\subseteq M \nrightarrow \exists a_1, a_2 \in R \setminus (R^* \cup \{0\})$ mit $a = a_1 a_2 \Rightarrow (a) \subseteq (a_1), (a) \subseteq (a_2)$. Wäre $(a) = (a_1)$, dann existiert $b \in R^*$ mit $a = a_1 b = a_1 a_2 \Rightarrow a_2 = b \in R^* \nrightarrow$. Also $(a) \subsetneq (a_1)$, analog $(a) \subsetneq (a_2) \Rightarrow (a_1), (a_2) \notin M \Rightarrow a_1, a_2$ haben Faktorisierung in irreduzible Elemente also auch $a = a_1 a_2 \nrightarrow$. Also $M = \emptyset \Rightarrow$ Existenz

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

Induktionsanfang: $r = 0 \Rightarrow a = 1 \Rightarrow s = 0$ (sonst $q_1, \dots, q_s \in R^*$)

Induktionsschritt: Behauptung für $0, \dots, r-1$ bewiesen.

$$p_1 \mid p_1 \cdot \dots \cdot p_r = q_1 \cdot \dots \cdot q_s \Rightarrow \exists j \in \{1, \dots, s\} : p_1 \mid q_j$$

Nach Umnummerierung sei $j = 1$ also $p_1 \mid q_1$, etwa $q_1 = c p_1$ mit $c \in R$. Da q_1 irreduzibel folgt $c \in R^*$, also $p_1 \stackrel{\wedge}{=} q_1$.

$$\Rightarrow p_1 \cdot \dots \cdot p_r = c p_1 q_2 \cdot \dots \cdot q_s \Rightarrow p_1(p_2 \cdot \dots \cdot p_r - c q_2 \cdot \dots \cdot q_s) = 0$$

$\Rightarrow p_2 \cdot \dots \cdot p_r = (c q_2) \cdot \dots \cdot q_s$. Wegen $c \in R^*$ ist $c q_2$ irreduzibel $\Rightarrow r-1 = s-1$ ($\Rightarrow r = s$) und nach Umnummerierung

$$p_2 \stackrel{\wedge}{=} c q_2 = q_2, p_3 \stackrel{\wedge}{=} q_3, \dots, p_r \stackrel{\wedge}{=} q_r \quad \square$$

Anmerkung • Fasst man in einer Zerlegung eines Elementes zueinander assoziierter Faktoren zusammen und erlaubt einen Vorfaktor $c \in R^*$, so erhält man eine Darstellung für Elemente $a \in R \setminus (R^* \cup \{0\})$ der Form

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

mit c, p_1, \dots, p_r irreduzibel, $p_i \not\stackrel{\wedge}{=} p_j$ für $i \neq j$, $e_1, \dots, e_r \in \mathbb{N}$. Ist dann $a = d q_1^{f_1} \cdot \dots \cdot q_s^{f_s}$ mit $d \in R^*, q_1, \dots, q_s$ irreduzibel, $q_i \not\stackrel{\wedge}{=} q_j$ für $i \neq j$, $f_1, \dots, f_s \in \mathbb{N}$, dann ist $r = s$ und nach Umnummerierung ist $p_i \stackrel{\wedge}{=} q_i, e_i = f_i$ für $i = 1, \dots, r$.

27 Euklidische Ringe

In diesem Abschnitt sei R stets ein kommutativer Ring.

Definition 27.1 R nullteilerfrei. R heißt **Euklidischer Ring**, wenn es eine Abbildung $\delta : R \setminus \{0\} \rightarrow \mathbb{N}_0$, sodass gilt:

$$\forall f, g \in R, g \neq 0 \exists q, r \in R : f = qg + r \wedge (\delta(r) < \delta(g) \vee r = 0)$$

δ heißt eine **Normabbildung** auf R .

Beispiel 27.2

1. $R = \mathbb{Z}$ mit $\delta = |\cdot|$ ist ein Euklidischer Ring (vergleiche Elementare Zahlentheorie-Skript, Satz 1.3)
2. K Körper $\Rightarrow R = K[T]$ mit $\delta = \deg$ ist ein Euklidischer Ring (vergleiche 7.6)
3. $R = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{C}\} \subseteq \mathbb{C}$ mit $\delta(x + iy) = x^2 + y^2$ ist ein Euklidischer Ring (Ring der ganzen Gaußschen Zahlen) (Übungen)

4. K Körper mit $\delta : K \setminus \{0\} \rightarrow \mathbb{N}_0, x \mapsto 1$ ist ein euklidischer Ring (hier ist stets „ $r = 0$ “)

Satz 27.3 R euklidischer Ring. Dann ist R ein Hauptidealring.

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

„ \supseteq “: Wegen $a \in I$ ist $(a) \subseteq I$

„ \subseteq “: Sei $f \in I \implies \exists q, r : f = qa + r$ und $(\delta(r) < \delta(a) \vee r = 0) \implies r = f - qa \in I$. Wegen $\delta(a)$ minimal folgt $r = 0 \implies f = qa \in (a)$ \square

Folgerung 27.4 R euklidischer Ring. Dann ist R faktoriell.

Beweis R euklidisch $\implies \mathbb{R}$ Hauptidealring $\implies R$ faktoriell. \square

Folgerung 27.5 K Körper, $f \in K[t]$, $f \neq 0$. Dann besitzt f eine bis auf Reihenfolge der Faktoren eindeutige Darstellung

$$f = cp_1^{e_1} \cdot \dots \cdot p_r^{e_r}$$

mit $c \in K^*, r \geq 0, e_1, \dots, e_r \in \mathbb{N}_0$ und paarweise verschiedenen irreduziblen normierten Polynomen p_1, \dots, p_r .

Beweis $K[t]$ ist euklidischer Ring, also faktoriell nach 27.4. Wegen $K[t]^* = K^*$ gilt für $f, g \in K[t] : f \stackrel{\wedge}{=} g \iff \exists \lambda \in K^* : f = \lambda g$. Insbesondere existiert in jeder Äquivalenzklasse bezüglich „ $\stackrel{\wedge}{=}$ “ in $K[t] \setminus \{0\}$ genau ein normiertes Polynom \implies Behauptung. \square

Satz 27.6 (Euklidischer Algorithmus) R euklidischer Ring mit Normabstand $\delta, a, b \in R \setminus \{0\}$. Wir betrachten eine Folge a_0, a_1, \dots von Elementen aus R , die induktiv wie folgt gegeben ist:

$$a_0 := a$$

$$a_1 := b$$

$$a_0 = q_0 a_1 + a_2 \quad \text{mit } \delta(a_2) < \delta(a_1) \text{ oder } a_2 = 0$$

Falls $a_2 \neq 0$:

$$a_1 = q_1 a_2 + a_3 \quad \text{mit } \delta(a_3) < \delta(a_2) \text{ oder } a_3 = 0$$

$$\vdots$$

Falls $a_i \neq 0$:

$$a_{i-1} = q_i a_i + a_{i+1} \quad \text{mit } \delta(a_{i+1}) < \delta(a_i) \text{ oder } a_{i+1} = 0$$

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 (vergleiche 26.22):

$$d = a_n = a_{n-2} q_{n-2} a_{n-1} = \dots = ua + vb$$

mit $u, v \in R$ („erweiterter Euklidischer Algorithmus“).

Beweis 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 \nexists .

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

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

mit geeigneten $u, v \in R$. □

Beispiel 27.7

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

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

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

$$3 = 9 - 1 \cdot 6 = 9 - (15 - 1 \cdot 9) = 2 \cdot 9 - 1 \cdot 15 = 2 \cdot (25 - 1 \cdot 15) - 15 = 2 \cdot 24 - 3 \cdot 15$$

Anmerkung Für Matrizen aus $M(n \times n, R)$ kann man analog zu LA1 (vergleiche 10.5) elementare Zeilen- und Spaltenoperationen erklären.

Satz 27.8 (Gauß-Diagonalisierung für Euklidische Ringe) R Euklidischer Ring, $A \in M(m \times n, R)$. Dann gilt: A lässt sich durch wiederholte Anwendung von elementaren Zeilen- und Spaltenoperationen vom Typ 3 (Addition des λ -fachen einer Zeile/Spalte zu einer anderen Zeile / Spalte, $\lambda \in R$) sowie des Typ 4 (Zeilen / Spaltenvertauschung) in eine Matrix der Gestalt

$$\begin{array}{ccc|c} c_1 & & & 0 \\ & \ddots & & \\ & & c_r & 0 \\ \hline 0 & & & 0 \end{array}$$

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

Beweis (= Algorithmus zur Durchführung). Falls $A = 0$, dann fertig. Im Folgenden sei $A \neq 0$. Sei δ eine Normabberechnung auf R .

1. Schritt: Durch Zeilen und Spaltenvertauschung erreichen wir $a_{11} \neq 0$ und $\delta(a_{11}) \leq \delta(a_{ij}) \forall i, j, a_{ij} \neq 0$.

2. Schritt: Bring A auf die Form

$$\begin{array}{c|c} * & 0 \\ \hline 0 & * \end{array}$$

- a) Fall: In der ersten Spalte / Zeile stehen keine Elemente $\neq 0$ außer a_{11} , dann fertig.
- b) Fall: In der ersten Spalte / Zeile stehen noch Elemente $\neq 0$, ohne Einschränkung $a_{21} \neq 0 \implies \exists q \in R : a_{21} = qa_{11}$ 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 $a'_{21} = 0$ oder $\delta(a'_{21}) < \delta(a_{11})$. Falls $a'_{21} \neq 0$, dann erhalte durch Zeilen sowie gegebenenfalls Spaltenvertauschung eine Matrix $A'' = (a''_{ij})$ mit $a''_{11} \neq 0, \delta(a''_{11}) \leq \delta(a'_{ij})$ für alle i, j mit $a''_{ij} \neq 0$, mit $\delta(a''_{11}) < \delta(a_1 1)$. Dieser Prozess bricht nach endlich vielen Iterationen ab und wir erhalten eine Matrix der Form

$$\begin{array}{c|c} d_{11} & 0 \\ \hline 0 & * \end{array}$$

$$d_{11} \neq 0, \delta(d_{11}) \leq \delta(d_{ij}) \text{ falls } d_{ij} \neq 0, \delta(d_{11}) \leq \delta(a_1 1)$$

3. Schritt: Erreiche $d_{11} \mid d_{ij} \forall i, j$:

- a) Fall: Es gilt bereits $d_{11} \mid d_{ij} \forall i, j$, dann fertig.
- b) Fall: Es existiert i, j mit $d_{11} \nmid d_{ij} \implies$ Es existiert ein $q \in R$ mit $d_{ij} - qd_{11} \neq 0$ und $\delta(d_{ij} - qd_{11}) < d_{11}$. Addiere erste Zeile von D zur i -ten Zeile von D , erhalte:

$$\begin{array}{c|cccccc} d_{11} & 0 & \dots & \dots & \dots & 0 \\ \hline 0 & & & & & \\ \vdots & & & * & & \\ 0 & & & & & \\ a_{11} & d_{iz} & \dots & d_{ij} & \dots & d_{in} \\ 0 & & & & & \\ \vdots & & & & & \\ 0 & & & & * & \end{array}$$

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

$$\begin{array}{c|cccccccc} d_{11} & 0 & \dots & 0 & -qd_{11} & 0 & \dots & \dots & 0 \\ \hline 0 & & & & & & & & \\ \vdots & & & & * & & & & \\ 0 & & & & & & & & \\ a_{11} & * & & d_{ij} - qd_{11} & & & * & & \\ 0 & & & & & & & & \\ \vdots & & & & & & & & \\ 0 & & & & * & & & & \end{array}$$

mit $d'_{ij} = d_{ij} - qd_{11}, \delta(d'_{ij}) < \delta(d_{11}) \leq d_{11}$. Wiederhole die gesamte bisherige Prozedur für die

Matrix D' . Dieser Prozess bricht nach endlich vielen Schritten ab. Wir erhalten eine Matrix

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

mit $c_{11} \neq 0, \delta(c_{11}) \leq \delta(a_1 1), c_{11} \mid c_{ij} \forall i, j$

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

$$\begin{array}{c|c} c_1 & \\ \vdots & \\ c_r & \\ \hline 0 & 0 \end{array}$$

mit $c_1 \mid c_2 \mid c_3 \mid \dots \mid c_r$ bringen. □

Beispiel 27.9

1. $\mathbb{R} = \mathbb{Z}$ mit $\delta = |\cdot|$:

$$A = \begin{pmatrix} 4 & 3 \\ 6 & 5 \end{pmatrix} \rightarrow \begin{pmatrix} 3 & 4 \\ 5 & 6 \end{pmatrix} \rightarrow \begin{pmatrix} 3 & 1 \\ 5 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 3 \\ 1 & 5 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

2. $R = \mathbb{Q}[t]$ mit $\delta = \deg$

$$A = \begin{pmatrix} t-1 & 0 \\ -1 & t-1 \end{pmatrix} \rightarrow \begin{pmatrix} -1 & t-1 \\ t-1 & 0 \end{pmatrix} \rightarrow \begin{pmatrix} -1 & t-1 \\ 0 & (t-1)^2 \end{pmatrix} \rightarrow \begin{pmatrix} -1 & 0 \\ 0 & (t-1)^2 \end{pmatrix}$$

Anmerkung Wir haben bei der Gauß-Diagonalisierung nur elementare Operationen vom Typ 3, 4 verwendet. Umformungen von Typ 1 (Multiplikation von einer Zeile / Spalte mit $\lambda \in R^*$), sowie Typ 2 (Addition einer Zeile / Spalte) auf eine andere Zeile oder Spalte.

Frage: Eindeutigkeitsaussage für c_1, \dots, c_r ?

Bemerkung+Definition 27.10 $GL(n, R) := \{A \in M(n \times n, R) \mid \exists B \in M(n \times n, R) : AB = BA = E_n\}$ ist eine Gruppe bezüglich „ \cdot “, **die allgemeine lineare Gruppe** über R vom Rang n . Es ist

$$GL(n, R) = \{A \in M(n \times n, R) \mid \det(A) \in R^*\}$$

Beweis Gruppeneigenschaft: klar.

$A \in GL(n, R) \iff \det(A) \in R^*$, denn: „ \implies “ $AB = E_n \implies \det(A)\det(B) = 1 \implies \det(A) \in R^*$
 „ \impliedby “ sei $\det(A) \in R^*$. Es ist $AA^\# \in R^*$. Es ist $AA^\# = \det(A)E_n = A^\#A$

$$\implies A \frac{1}{\det(A)} A^\# = E_n = \frac{1}{\det(A)} A^\# A$$

□

Bemerkung+Definition 27.11 $A, B \in M(m \times n, R)$. A heißt **äquivalent** zu B ($A \sim B$)

$$\iff \exists S \in GL(m, R), T \in GL(n, R) : B = SAT^{-1}$$

Falls $m = n$, dann heißt A **ähnlich** zu B ($A \approx B$)

$$\iff \exists S \in GL(n, R) : B = SAS^{-1}$$

\sim, \approx sind Äquivalenzrelationen auf $M(m \times n, R)$ beziehungsweise $M(n \times n, R)$.

Erinnerung: In LA1 gezeigt (vergleiche 16.11): K Körper, $A, B \in M(m \times n, K)$, dann gilt $A \sim B \iff \text{Rang}(A) = \text{Rang}(B)$. Ist $\text{Rang } A = r$, dann

$$A \sim \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$$

Ziel: Klassifikation von Matrizen aus $M(m \times n, R)$, R Euklidischer Ring bis auf Äquivalenz.

Definition 27.12 $A \in M(m \times n, R)$, $1 \leq k \leq m$, $1 \leq l \leq n$. $B \in M(k \times l, R)$ heißt eine **Untermatrix** von $A \stackrel{\text{Def}}{\iff}$ aus A durch Streichen von $m - k$ Zeilen und $n - l$ Spalten. Ist $B \in M(l \times l, R)$ eine quadratische Untermatrix von A , dann heißt $\det(B)$ ein **Minor** l -ter Stufe von A .

$$\text{Fit}_l(A) = (\det(B) \mid B \text{ ist } l \times l\text{-Untermatrix von } A) \subseteq R$$

(das von allen Minoren l -ter Stufe von A erzeugte Ideal in R) heißt das **l -te Fittingideal von A** .

Beispiel 27.13

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

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

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

Satz 27.14 (Fittings Lemma) $A \in M(m \times n, R)$, $S \in \text{GL}(m, R)$, $T \in \text{GL}(n, R)$, $l \leq \min\{m, n\}$. 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: $A = (a_{ij}) \in M(m \times n, R)$, $S = (s_{ij}) \in \text{GL}(m, R)$, $SA = (b_{ij}) \in M(m \times n, R)$. Seien $1 \leq i_1 < i_2 < \dots < i_l \leq m$, $1 \leq j_1 < j_2 < \dots < j_l \leq n$. 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 .

$$\begin{aligned} \implies \det B &= \det \begin{pmatrix} \sum_{r_1=1}^m s_{i_1, r_1} a_{r_1, j_1} & \dots & \sum_{r_1=1}^m s_{i_1, r_1} a_{r_1, j_l} \\ b_{i_2, j_1} & \dots & b_{i_2, j_l} \\ \vdots & 8 & \vdots \\ b_{i_l, j_1} & \dots & b_{i_l, j_l} \end{pmatrix} \\ &= \sum_{r_1=1}^{s_{i_1, r_1}} \det \begin{pmatrix} a_{r_1, j_1} & \dots & a_{r_1, j_l} \\ b_{i_2, j_1} & \dots & b_{i_2, j_l} \\ \vdots & 8 & \vdots \\ b_{i_l, j_1} & \dots & b_{i_l, j_l} \end{pmatrix} \\ &= \sum_{r_l=1}^m \dots \sum_{r_1=1}^m s_{i_1, r_1} \dots s_{i_l, r_l} \det \begin{pmatrix} a_{r_1, j_1} & \dots & a_{r_1, j_l} \\ \vdots & & \vdots \\ a_{r_l, j_1} & \dots & a_{r_l, j_l} \end{pmatrix} \\ &= \sum_{r_l=1}^m \dots \sum_{r_1=1}^m s_{i_1, r_1} \dots s_{i_l, r_l} \det \begin{cases} 0 & \text{falls } i \neq j \text{ existiert mit } r_i = r_j \\ I & \text{ein Minor } l\text{-ter Stufe von } A \end{cases} \\ &\in \text{Fit}_l(A) \end{aligned}$$

2. Wende 1. auf $S^{-1} \in \text{GL}(m, R)$, $SA \in M(m \times n, R)$ an: $\implies \text{Fit}_l(S^{-1}(SA)) \subseteq \text{Fit}_l(SA)$, also $\text{Fit}_l(A) \subseteq \text{Fit}_l(SA)$. Außerdem: $\text{Fit}_l(A) = \text{Fit}_l(A^T)$, also

$$\text{Fit}_l(AT) = \text{Fit}_l((AT)^T) = \text{Fit}_l(T^T A^T) = \text{Fit}_l(A^T) = \text{Fit}_l(A) \quad \square$$

Folgerung 27.15 $A, B \in M(m \times n, R)$ mit $A \sim B$. Dann gilt: $\text{Fit}_l(A) = \text{Fit}_l(B)$ für alle $1 \leq l \leq \min\{m, n\}$.

Beweis $A \sim B \implies \exists S \in \text{GL}(m, R), T \in \text{GL}(n, R) : B = SAT^{-1}$

$$\implies \text{Fit}_l(B) = \text{Fit}_l(SAT^{-1}) = \text{Fit}_l(AT^{-1}) = \text{Fit}_l(A) \quad \square$$

Bemerkung 27.16 R nullteilerfreier Ring,

$$A = \begin{pmatrix} c_1 & & 0 \\ & \ddots & \\ 0 & & c_r \\ & & 0 \end{pmatrix} \in M(m \times n, R)$$

mit $c_1 \mid \dots \mid c_r$. Dann gilt:

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

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

Beweis Für $l > r$ enthält jede $l \times l$ -Untermatrix von A stets eine Nullzeile, das heißt $\text{Fit}_l(1) = (0)$.
 $l \leq r$: Die einzige $l \times l$ Untermatrix von A , die keine Nullzeile enthalten, sind von der Form

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

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

$$\begin{aligned} \implies \text{Fit}_l(A) &= (c_{i_1} \cdot \dots \cdot c_{i_l} \mid 1 \leq i_1 < i_2 < \dots < i_l \leq r) \\ \implies (c_1 \cdot \dots \cdot c_l) &\subseteq \text{Fit}_l(A) \end{aligned}$$

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

$$\begin{aligned} \implies c_1 \mid c_{i_1}, \dots, c_l \mid c_{i_l} &\implies c_1 \cdot \dots \cdot c_l \mid c_{i_1} \cdot \dots \cdot c_{i_l} \implies (c_{i_1} \cdot \dots \cdot c_{i_l}) \subseteq (c_1 \cdot \dots \cdot c_l) \\ \implies \text{Fit}_l(A) &\subseteq (c_1, \dots, c_l) \end{aligned}$$

\implies „=“

□

Satz+Definition 27.17 (Elementarteilersatz über Euklidischen Ringen) R Euklidischer Ring, $A \in M(m \times n, R)$. Dann existieren $c_1, \dots, c_r \in R \setminus \{0\}$ mit $c_1 \mid c_2 \mid \dots \mid c_r$, sodass

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

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

Beweis 1. Nach Gauß-Diagonalisierung 27.8 lässt sich A durch elementare Zeilen- und Spaltenumformungen auf die Form

$$\begin{array}{ccc|c} c_1 & & 0 & \\ & \ddots & & 0 \\ & 0 & c_r & \\ & & 0 & 0 \end{array}$$

mit $c_1, \dots, c_r \in R \setminus \{0\}$, $c_1 \mid c_2 \mid \dots \mid c_r$ bringen. Wie in LA1 (Übungsblatt 8, Aufgabe 3) entsprechen elementare Zeilenoperationen Multiplikation mit speziellen invertierbaren Matrizen von links, Spaltenoperationen mit speziellen invertierbaren Matrixen von rechts $\implies \exists S \in \text{GL}(m, R), T \in \text{GL}(n, R)$:

$$SAT^{-1} = \begin{array}{ccc|c} c_1 & & 0 & \\ & \ddots & & 0 \\ & 0 & c_r & \\ & & 0 & 0 \end{array} \iff A \sim \begin{array}{ccc|c} c_1 & & 0 & \\ & \ddots & & 0 \\ & 0 & c_r & \\ & & 0 & 0 \end{array}$$

2. Eindeutigkeit von r : Sei

$$A \sim \begin{array}{ccc|c} c_1 & & 0 & \\ & \ddots & & 0 \\ & 0 & c_r & \\ & & 0 & 0 \end{array}, A \sim \begin{array}{ccc|c} d_1 & & 0 & \\ & \ddots & & 0 \\ & 0 & d_s & \\ & & 0 & 0 \end{array}$$

mit $c_1, \dots, c_r, d_1, \dots, d_s \in R \setminus \{0\}$, $c_1 \mid \dots \mid c_r, d_1 \mid \dots \mid d_s$.

$$\implies \text{Fit}_l(A) = \begin{cases} (c_1 \cdot \dots \cdot c_l) & l \leq r \\ (0) & l > r \end{cases} = \begin{cases} (d_1 \cdot \dots \cdot d_l) & l \leq s \\ (0) & l > s \end{cases}$$

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

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

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

Induktionsanfang: $\text{Fit}_1(A) = (c_1) = (d_1) \implies c_1 \hat{=} d_1$.

Induktionsschritt: $\text{Fit}_l(A) = (c_1 \cdot \dots \cdot c_l) = (d_1 \cdot \dots \cdot d_l) \implies c_1 \cdot \dots \cdot c_l \hat{=} d_1 \cdot \dots \cdot d_l \implies c_l \hat{=} d_l$

□

Satz 27.18 (27.18) R Euklidischer Ring, $A, B \in M(m \times n, R)$. Dann sind äquivalent:

1. $A \sim B$
2. Die Elementarteiler von A und B stimmen bis auf Assoziiertheit überein.
3. $\text{Fit}_l(A) = \text{Fit}_l(B) \forall 1 \leq l \leq \min\{m, n\}$

Beweis 1. \implies 2. aus 27.18

3. 2. Seien c_1, \dots, c_r beziehungsweise d_1, \dots, d_s die Elementarteiler von A beziehungsweise B . Insbesondere

$$A \sim \begin{array}{ccc|c} c_1 & & 0 & \\ & \ddots & & 0 \\ & 0 & c_r & \\ & & 0 & 0 \end{array}, B \sim \begin{array}{ccc|c} d_1 & & 0 & \\ & \ddots & & 0 \\ & 0 & d_s & \\ & & 0 & 0 \end{array}$$

Argumentiere nun wie im Beweis von 27.17 in 2., 3.. 27.17 in 2., 3..

2. \implies 1. Sei

$$A \sim \begin{array}{ccc|c} c_1 & & 0 & \\ & \ddots & & \\ 0 & & c_r & \\ & 0 & & 0 \end{array}, B \sim \begin{array}{ccc|c} d_1 & & 0 & \\ & \ddots & & \\ 0 & & d_r & \\ & 0 & & 0 \end{array}$$

mit $c_1 \stackrel{\wedge}{=} d_1, \dots, c_r \stackrel{\wedge}{=} d_r$, etwa $d_1 = \lambda_1 c_1, \dots, d_r = \lambda_r c_r$ mit $\lambda_1, \dots, \lambda_r \in R^*$.

$$\begin{array}{ccc|c} d_1 & & 0 & \\ & \ddots & & \\ 0 & & d_r & \\ & 0 & & 0 \end{array} = \begin{pmatrix} \lambda_1 & & & \\ & \ddots & & \\ & & \lambda_r & \\ & & & 1 \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix} \begin{array}{ccc|c} c_1 & & 0 & \\ & \ddots & & \\ 0 & & c_r & \\ & 0 & & 0 \end{array}$$

$$\implies A \sim \begin{array}{ccc|c} c_1 & & 0 & \\ & \ddots & & \\ 0 & & c_r & \\ & 0 & & 0 \end{array} \sim \begin{array}{ccc|c} d_1 & & 0 & \\ & \ddots & & \\ 0 & & d_r & \\ & 0 & & 0 \end{array} \sim B$$

□

Beispiel 27.19

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in M(2 \times 2, \mathbb{Z}) \implies \text{Fit}_1(A) = (1), \text{Fit}_2(A) = (2)$$

\implies Elementarteiler von A : 1, 2, insbesondere $A \sim \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$. Sei

$$B = \begin{pmatrix} 4 & 3 \\ 2 & 2 \end{pmatrix} \in M(2 \times 2, \mathbb{Z}) \implies \text{Fit}_1(B) = (2, 3, 4) = (1), \text{Fit}_2(B) = (2)$$

$\implies A \sim B$

28 Normalformen von Endomorphismen

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

Ziel: $A, B \in M(n \times n, K)$

- Wann ist $A \approx B$?
- Suche möglichst einfache Vertreter der Äquivalenzklasse bezüglich „ \approx “ (\rightarrow Normalformen)

In Termen von Endomorphismen: Gegeben sei $\varphi \in \text{End}(V)$, V endlichdimensionaler K -Vektorraum. Wir suchen Basis \mathcal{B} von V , sodass $M_{\mathcal{B}}(\varphi)$ möglichst einfach ist.

Definition 28.1 $A \in M(n \times n, K)$.

$$P_A := tE_n - A \in M(n \times n, K[t])$$

heißt die charakteristische Matrix von A .

Anmerkung Insbesondere ist $\chi_A^{char} = \det(P_A)$.

Satz 28.2 (Satz von Frobenius) $A, B \in M(n \times n, K)$. Dann sind äquivalent:

1. $A \approx B$ (in $M(n \times n, K)$)
2. $P_A \sim P_B$ (in $M(n \times n, K[t])$)

Beweis 1. \implies 2. Sei $A \approx B \implies \exists S \in GL(n, K) : B = SAS^{-1}$

$$\begin{aligned} \implies P_B &= tE_n - B = tE_n - SAS^{-1} = StE_nS^{-1} - SAS^{-1} \\ &= S \underbrace{(tE_n - A)}_{=P_A} S^{-1} \\ \implies P_B &\approx P_A \implies P_B \sim P_A \end{aligned}$$

2. \implies 1. Sei $P_A \sim P_B$:

a) Wir konstruieren $R \in M(n \times n, K)$ mit $AR = RB$:

$$\implies \exists S, T \in GL(n, K[t]) : P_A = SP_B T^{-1}, \text{ das heit } SP_B = P_A T$$

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

Wir schreiben S, T in der folgenden Form:

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

$$\begin{aligned} \implies S(tE_n - B) &= \sum_{i=0}^m t^i S_i (tE_n - B) = \sum_{i=0}^m (t^{i+1} S_i - t^i S_i B) \\ (tE_n - A)T &= (tE_n - A) \sum_{i=0}^m t^i T_i = \sum_{i=0}^m (t^{i+1} T_i - t^i A T_i) \\ \implies \sum_{i=0}^{m+1} (S_{i-1} - S_i B) t^i &= \sum_{i=0}^{m+1} (T_{i-1} - A T_i) t^i \end{aligned}$$

wobei $S_{-1}, T_{-1}, S_{m+1}, T_{m+1} = 0$

$$\begin{aligned}
 &\implies S_{i-1} - S_i b = T_{i-1} - a T_i \quad 0 \leq i \leq m+1 \\
 &\implies A^i S_{i-1} - A^i S_i B = A^i T_{i-1} - A^{i+1} T_i \quad 0 \leq i \leq m+1 \\
 &\implies \sum_{i=0}^{m+1} (A^i S_{i-1} - A^i S_i B) = \sum_{i=0}^{m+1} (A^i T_{i-1} - A^{i+1} T_i) \\
 &\quad = (A^0 T_{-1} - A T_0) + (A T_0 - A^2 T_1) + \cdots + (A^{m+1} T_m - A^{m+2} T_{m+1}) \\
 &\quad = A^0 T_{-1} - A^{m+2} T_{m+1} = 0 \\
 &\implies \sum_{i=0}^{m+1} A^i S_{i-1} = \sum_{i=0}^{m+1} A^i S_i B \\
 &\implies \sum_{i=1}^{m+1} A^i S_{i-1} = \sum_{i=0}^m A_i S_i B \\
 &\implies A \left(\sum_{i=0}^m A^i S_i \right) = \left(\sum_{i=0}^m A^i S_i \right) B \\
 &\implies R := \sum_{i=0}^m A^i S_i
 \end{aligned}$$

dann $AR = RB$.

- a) Wir zeigen $R \in \text{GL}(n, K)$ (wegen $AR = RB$ ist dann $A = RBR^{-1}$, also $A \approx B$, fertig.) Nach Voraussetzung ist $S \in \text{GL}(n, K[t]) \implies \exists M \in \text{GL}(n, K[t]) : SM = E_n, M = \sum_{i=0}^m t^i M_i$ mit $M_i \in M(n \times n, K)$, ohne Einschränkung dasselbe n wie vorhin. Behauptung: Mit

$$N := \sum_{j=0}^m B^j M_j \in M(n \times n, K)$$

gilt $RN = E_n$ also $R \in \text{GL}(n, K)$, denn: Es ist

$$RN = \sum_{j=0}^m RB^j M_j$$

Wegen $RB = AR$ folgt $RB^j = RBB^{j-1} = ARB^{j-1} = \cdots = A^j R$

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

Wegen $SM = E_n$ folgt

$$\left(\sum_{i=0}^m t^i S_i \right) \left(\sum_{j=0}^m t^j M_j \right) = E_n$$

$$\begin{aligned}
&\Rightarrow S_0 M_0 + \sum_{k=1}^{2m} \left(\sum_{i+j=k} S_i M_j \right) t^k = E_n \\
&\Rightarrow S_0 M_0 = E_n, \quad \sum_{i+j=k} S_i M_j = 0 \quad k \geq 1 \\
&\Rightarrow RN = \sum_{i,j=0}^m A^{i+j} S_i M_j = S_0 M_0 + \sum_{k=1}^{2m} A^k \underbrace{\sum_{i+j=k} S_i M_j}_{=0} = S_0 M_0 = E_n \quad \square
\end{aligned}$$

Bemerkung+Definition 28.3 $A \in M(n \times n, K)$. Dann gilt:

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

$$P_A \sim \begin{pmatrix} c_1(A) & & 3 \\ & \ddots & \\ 0 & & c_n(A) \end{pmatrix}, \quad c_1(A) \mid c_2(A) \mid \dots \mid c_n(A)$$

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

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

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

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 1. Existenz: $K[t]$ ist ein euklidischer Ring. Elementarteilersatz $\Rightarrow \exists \tilde{c}_1, \dots, \tilde{c}_r \in K[t]$:

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

Es ist $\text{Fit}_n(P_A) = (\det(P_A)) = (\chi_A^{\text{char}}) \neq (0) \rightarrow r = 0$ und

$$\text{Fit}_n(P_A) = (\tilde{c}_1 \cdot \dots \cdot \tilde{c}_n)$$

Da $\tilde{c}_1, \dots, \tilde{c}_n \neq 0$ eindeutig bis auf Assoziiertheit, existieren eindeutig bestimmte normierte Polynome $c_1(A), \dots, c_n(A)$ mit $c_1(A) \stackrel{\wedge}{=} \tilde{c}_1, \dots, c_n(A) \stackrel{\wedge}{=} \tilde{c}_n$.

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

2. $K[t]$ Hauptidealring $\implies \text{Fit}_l(P_A), l = 1, \dots, n$ sind Hauptideale und nach 27.16 ist $\text{Fit}_l(P_A) = (c_1(A) \cdot \dots \cdot c_l(A))$ für $l = 1, \dots, n$, insbesondere $\text{Fit}_l(P_A) \neq (0)$. Erzeuger der Hauptideale $\text{Fit}_l(P_A)$ sind eindeutig bis auf Assoziiertheit. \implies Es existieren eindeutig bestimmte normierte Polynome $d_1(A), \dots, d_n(A) \in K[t]$ mit $\text{Fit}_l(P_A) = (d_l(A))$ für $l = 1, \dots, n$. $\$$

$$\implies \text{Fit}_l(P_A) = (\det(B) \mid B \text{ ist } l \times l\text{-Untermatrix von } A) = (d_l(A))$$

mit $d_l(A)$ normiert und $\text{ggT}(\dots)$ normiert \implies Behauptung. \square

Anmerkung Also:

- Invariantenteiler von A = normierte Elementarteiler von P_A
- Determinantenteiler von A = normierte Erzeuger der Fittingideale von P_A .

Folgerung 28.4 $A \in M(n \times n, K)$. Dann gilt: $d_l(A) = c_1(A) \cdot \dots \cdot c_l(A) \forall l = 1, \dots, n$. Insbesondere gilt:

$$\chi_A^{\text{char}} = d_n(A) = c_1(A) \cdot \dots \cdot c_n(A)$$

sowie

$$d_1(A) \mid \dots \mid d_n(A)$$

Satz 28.5 (Invariantenteilersatz) $A, B \in M(n \times n, K)$. Dann sind äquivalent:

1. $A \approx B$
2. Die Invariantenteiler von A stimmen mit den Invariantenteilern von B überein:

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

3. Die Determinantenteiler von A stimmen mit den Determinantenteilern von B überein:

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

Beweis aus Satz von Probenius und Satz 27.18 \square

Beispiel 28.6

Sei

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

Es ist

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

Bestimmung der Determinantenteiler von A : $d_1(A) = \text{ggT}(-1, \dots) = 1$

$$\begin{aligned} d_2(A) &= \text{ggT}((-1) \cdot 4 - (-3)(t-1), (-3)(-1) - 2(t-1), \dots) \\ &= \text{ggT}(3t-7, -2t+5, \dots) = 1 \end{aligned}$$

$$d_3(A) = \chi_A^{\text{char}} = (t-2)^3$$

$$\implies c_1(A) = 1, c_2(A) = 1, c_3(A) = (t-2)^3$$

Sei

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

Bestimme Invariantenteiler von B :

$$\begin{aligned} P_B &= \begin{pmatrix} t-1 & -1 & -2 \\ -1 & t-1 & 2 \\ 1 & -1 & t-4 \end{pmatrix} \sim \begin{pmatrix} -1 & t-1 & 2 \\ t-1 & -1 & -2 \\ 1 & -1 & t-4 \end{pmatrix} \\ &\sim \begin{pmatrix} -1 & t-1 & 2 \\ 0 & (t-1)^2 - 1 & -2 + 2(t-1) \\ 0 & t-2 & t-2 \end{pmatrix} \sim \begin{pmatrix} -1 & 0 & 0 \\ 0 & t^2 - 2t & 2t - 4 \\ 0 & t-2 & t-2 \end{pmatrix} \\ &\sim \begin{pmatrix} -1 & 0 & 0 \\ 0 & t-2 & t-2 \\ 0 & t^2 - 2t & 2t - 4 \end{pmatrix} \sim \begin{pmatrix} -1 & 0 & 0 \\ 0 & t-2 & 0 \\ 0 & t^2 - 2t & -t^2 + 3t - 4 \end{pmatrix} \\ &\sim \begin{pmatrix} -1 & 0 & 0 \\ 0 & t-2 & 0 \\ 0 & 0 & -(t-2)^2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & t-2 & 0 \\ 0 & 0 & (t-2)^2 \end{pmatrix} \\ \implies c_1(B) &= 1, c_2(B) = t-2, c_3(B) = (t-2)^2 \\ d_1(B) &= 1, d_2(B) = t-2, d_3(B) = (t-2)^3 \end{aligned}$$

Bemerkung 28.7 (28.7) $A, B \in M(n \times n, K)$, K Teilkörper eines Körpers L , dann sind folgende Aussagen äquivalent

1. $A \approx B$ in $M(n \times n, K)$
2. $A \approx B$ in $M(n \times n, L)$

Beweis Übung □

Ziel: Such möglichst einfache Matrizen, die vorgegebene Invarianten- beziehungsweise Determinantenteiler haben.

Definition 28.8 $g = t^2 + a_{n-1}t^{n-1} + \dots + a_1t + a_0 \in K[t], n \geq 1$

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

heißt die **Begleitmatrix** zu g .

Bemerkung 28.9 $g \in K[t]$ nicht konstant, normiert. Dann ist $c_1(B_g) = \dots = c_{n-1}(B_g) = 1, c_n(B_g) = g$, also

$$P_{B_g} \sim \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & g \end{pmatrix}$$

$$d_1(B_g) = \dots = d_{n-1}(B_g) = 1, d_n(B_g) = \chi_{B_g}^{char} = g$$

Beweis Sei $g = t^n + a_{n-1}t^{n-1} + \dots + a_0$

$$\Rightarrow P_{B_g} = \begin{pmatrix} t & & & a_0 \\ -1 & t & & a_1 \\ & -1 & \ddots & \vdots \\ & & \ddots & t & a_{n-2} \\ & & & -1 & t + a_{n-1} \end{pmatrix}$$

streiche erste Zeile, letzte Spalte von P_{B_g} , erhalte Untermatrix

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

mit $\det(C) = (-1)^{n-1} \Rightarrow d_{n-1}(B_g) = 1 \Rightarrow d_1(B_g) = \dots = d_{n-1}(B_g) = 1$, sowie $c_1(B_g) = \dots = c_{n-1}(B_g) = 1$. Wir zeigen per Induktion nach n , dass $d_n(B_g) = \chi_{B_g}^{char} = g$.

Induktionsanfang: $n = 1$: $g = t + a_0$, $B_g = (-a_0) \Rightarrow \chi_{B_g}^{char} = t + a_0 = g$

Induktionsschritt:

$$\begin{aligned} \chi_{B_g}^{char} &= \det \begin{pmatrix} t & & & a_0 \\ -1 & \ddots & & \vdots \\ & \ddots & t & a_{n-2} \\ & & -1 & t + a_{n-1} \end{pmatrix} \\ &= t \cdot \det \begin{pmatrix} t & & & a_1 \\ -1 & \ddots & & \vdots \\ & \ddots & t & a_{n-2} \\ & & -1 & t + a_{n-1} \end{pmatrix} + (-1)^{n+1} a_0 \det \begin{pmatrix} -1 & t & & \\ & \ddots & \ddots & \\ & & \ddots & t \\ & & & -1 \end{pmatrix} \\ &\quad \underbrace{= a_1 + a_2 t + \dots + a_{n-1} t^{n-2} + t^{n-1} =: \tilde{g}}_{= a_1 t + a_2 t^2 + \dots + a_{n-1} t^{n-1} + t^n + a_0 = g} \quad \underbrace{= (-1)^{n-1}}_{= (-1)^{n-1}} \\ &= a_1 t + a_2 t^2 + \dots + a_{n-1} t^{n-1} + t^n + a_0 = g \end{aligned} \quad \square$$

Bemerkung+Definition 28.10 $g_1, \dots, g_r \in K[t]$ normiert, nichtkonstant mit $g_1 \mid g_2 \mid \dots \mid g_r$, $n := \deg(g_1) + \dots + \deg(g_r)$

$$B_{g_1, \dots, g_r} := \begin{pmatrix} B_{g_1} & & \\ & B_{g_2} & \\ & & \ddots \\ & & & B_{g_r} \end{pmatrix} \in M(n \times nK)$$

Dann gilt:

$$\begin{aligned} c_1(B_{g_1, \dots, g_r}) &= 1, \dots, c_{n-1}(B_{g_1, \dots, g_r}) = 1 \\ c_{n-r+1}(B_{g_1, \dots, g_r}) &= g_1, \dots, c_n(B_{g_1, \dots, g_r}) = g_r \end{aligned}$$

Beweis

$$P_{B_{g_1}, \dots, g_r} = \begin{pmatrix} P_{B_{g_1}} & & \\ & \ddots & \\ & & P_{B_{g_r}} \end{pmatrix} \sim \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & g_1 & \\ & & & & \ddots & \\ & & & & & 1 & \\ & & & & & & \ddots & \\ & & & & & & & 1 & \\ & & & & & & & & g_r \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & g_1 & \\ & & & & \ddots & \\ & & & & & g_r \end{pmatrix}$$

□

Satz 28.11 (Frobenius-Normalform) $A \in M(n \times n, K)$. Dann existiert ein eindeutig bestimmtes $r \in \mathbb{N}$ sowie eindeutig bestimmte normierte nichtkonstante Polynome $g_1, \dots, g_r \in K[t]$ mit $g_1 \mid \dots \mid g_r$ und $A \approx B_{g_1, \dots, g_r}$. g_1, \dots, g_r sind genau die nichtkonstanten Invariantenteiler von A . B_{g_1, \dots, g_r} heißt die **Frobenius-Normalform** (FNF) von A .

Beweis 1. Existenz: Setze

$$\begin{aligned} k &:= \max\{l \in \{1, \dots, n\} \mid c_l(A) = 1\} \\ r &:= n - k \\ g_i &:= g_{k+i}(A) \forall i = 1, \dots, r \\ \implies n &= \deg(\chi_A^{\text{char}}) = \deg(d_n(A)) = \deg(c_1(A) \cdot \dots \cdot c_n(A)) = \deg(g_1 \cdot \dots \cdot g_r) \\ &= \deg(g_1) + \dots + \deg(g_r) \end{aligned}$$

\implies Die Invariantenteiler von A stimmen mit den Invariantenteilern von B_{g_1, \dots, g_r} überein $\implies A \approx B_{g_1, \dots, g_r}$

2. Eindeutigkeit: $A \approx B_{g_1, \dots, g_r} \approx B_{k_1, \dots, k_s} \implies r = s \wedge g_1 = k_1, \dots, g_r = k_r$

□

Beispiel 28.12

1.

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

$$\implies c_1(A) = 1, c_2(A) = 1, c_3(A) = (t-2)^3 = t^3 - 6t^2 + 12t - 8 =: g_1$$

$$\implies A \approx B_{g_1} = \begin{pmatrix} 0 & 0 & 8 \\ 1 & 0 & -12 \\ 0 & 1 & 6 \end{pmatrix}$$

2.

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

$$\Rightarrow c_1(A) = 1, c_2(A) = t - 2 =: g_1, c_3(A) = (t - 2)^2 = t^2 - 4t + 4 =: g_2$$

$$\Rightarrow A \approx B_{g_1, g_2} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & -4 \\ 0 & 1 & 4 \end{pmatrix}$$

3.

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

$$c_1(A) = 1, c_2(A) = 1, c_3(A) = t - 3 =: g_1, c_4(A) = (t - 3)^3(t - 2) = t^4 - 8t^3 + 21t^2 - 18t =: g_2$$

$$\Rightarrow A \approx B_{g_1, g_2} = \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 18 \\ 0 & 1 & 0 & -21 \\ 0 & 0 & 1 & 8 \end{pmatrix}$$

Bemerkung 28.13 $A \in M(n \times n, K)$. Dann ist $c_n(A) = \chi_A^{\min}$

Beweis Übung. □

Bemerkung 28.14 $g \in K[t], g = h_1 \cdot \dots \cdot h_k$ mit $h_1, \dots, h_k \in K[t]$ normiert, nicht konstant, paarweise teilerfremd

$$\Rightarrow B_g \approx \begin{pmatrix} B_{h_1} & & \\ & \ddots & \\ & & B_{h_k} \end{pmatrix}$$

Beweis 1. Sei C definiert als die rechte Seite, dann ist

$$P_c = \begin{pmatrix} P_{B_{h_1}} & & \\ & \ddots & \\ & & B_{B_{h_k}} \end{pmatrix} \sim \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & h_1 & \\ & & & & \ddots \\ & & & & & 1 \\ & & & & & & \ddots \\ & & & & & & & 1 \\ & & & & & & & & h_k \end{pmatrix} \sim \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & h_1 & \\ & & & & \ddots \\ & & & & & h_k \end{pmatrix} =: H$$

$$P_{B_g} \sim \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & g \end{pmatrix} =: G$$

2. G, H haben dieselben Fittingideale, denn: Sei $n = \deg(g)$, insbesondere $G, H \in M(n \times n, K[t])$
- $\text{Fit}_n(H) = (\det(H)) = (h_1 \cdot \dots \cdot h_k) = (g) = (\det(G)) = \text{Fit}_n(G)$
 - $\text{Fit}_1(G) = \dots = \text{Fit}_{n-1}(G) = (1)$
 - $\text{Fit}_{n-1}(H) \supseteq (h_1 \cdot \dots \cdot h_{i-1} \cdot h_{i+1} \cdot \dots \cdot h_k \mid i = 1, \dots, k) = (1)$, also $\text{Fit}_{n-1}(H) = (1)$ (da h_1, \dots, h_k paarweise teilerfremd. Analog: $\text{Fit}_{n-k+i}(H) = (1)$ für $i = 1, \dots, k-2$. Klar: $\text{Fit}_l(H) = (1)$ für $l = 1, \dots, n-k$
3. Wegen 2. ist $G \sim H \implies P_{B_g} \sim P_c \implies B_g \approx C$. \square

Satz+Definition 28.15 (Weierstrass-Normalform) $A \in M(n \times n, K)$. Dann existieren eindeutig bestimmte $m \in \mathbb{N}$, Polynome $h_1, \dots, h_m \in K[t]$, die Potenzen von irreduziblen, normierten Polynomen sind, sodass

$$A \approx B_{h_1, \dots, h_m}$$

h_1, \dots, h_m sind bis auf Reihenfolge eindeutig bestimmt und heißen **Weierstrassteiler** von A . B_{h_1, \dots, h_m} heißt eine **Weierstrass-Normalform** von A (WNF). h_1, \dots, h_m sind die Potenzen irreduzibler Polynome, die in den Primfaktorzerlegung der nichtkonstanten Invariantenteiler von A auftauchen.

Beweis 1. Existenz: (Algorithmus zur Herstellung der Weierstrassnormalform)

Seien $g_1, \dots, g_r \in K[t]$ die nichtkonstanten Invariantenteiler von A (mit $g_1 \mid \dots \mid g_r$)

$$A \approx B_{g_1, \dots, g_r} = \begin{pmatrix} B_{g_1} & & \\ & \ddots & \\ & & B_{g_r} \end{pmatrix}$$

Nach 27.5 ist $K[t]$ ein faktorieller Ring, das heißt für $i = 1, \dots, r$ existieren paarweise teilerfremde Polynome $h_{i,1}, \dots, h_{i,k_i}$, die Potenzen irreduzibler Polynome sind, sodass $g_i = h_{i,1} \cdot \dots \cdot h_{i,k_i}$

$$\xrightarrow{28.14} A \approx \begin{pmatrix} B_{h_{1,1}} & & & \\ & \ddots & & \\ & & B_{h_{1,k_1}} & \\ & & & \ddots & \\ & & & & B_{h_{r,1}} & \\ & & & & & \ddots & \\ & & & & & & B_{h_{r,k_r}} \end{pmatrix}$$

2. Eindeutigkeit von m sowie von h_1, \dots, h_m bis auf Reihenfolge. Sei

$$A \approx \begin{pmatrix} B_{h_1} & & \\ & \ddots & \\ & & B_{h_m} \end{pmatrix}$$

wobei h_1, \dots, h_m Potenzen irreduzibler Polynome. Wir sortieren h_1, \dots, h_m so, dass $h_1 = p_1^{e_1}, \dots, h_k = p_k^{e_k}, p_1, \dots, p_k$ irreduzibel, normiert, paarweise verschieden, sodass alle weiteren h_i Potenzen von p_1, \dots, p_k sind mit kleinerem oder gleichem Exponenten. Setze $f_1 := \text{kgV}(h_1, \dots, h_m) = h_1 \cdot \dots \cdot h_k, h_1, \dots, h_k$ paarweise teilerfremd, f_1 normiert vom Grad ≥ 1 .

$$A \approx \begin{pmatrix} B_{f_1} & & \\ & B_{h_{k+1}} & \\ & & \ddots & \\ & & & B_{h_m} \end{pmatrix}, f_1 \cdot h_{k+1} \cdot \dots \cdot h_m = h_1 \cdot \dots \cdot h_m$$

Wende dieses Verfahren auf die Matrix

$$\begin{pmatrix} B_{h_{k+1}} & & \\ & \ddots & \\ & & B_{h_m} \end{pmatrix}$$

an: Nach Umsortieren von h_{k+1}, \dots, h_m wie oben erhalten wir $f_2 \in K[t]$ mit

$$A \approx \begin{pmatrix} B_{f_1} & & & \\ & B_{f_2} & & \\ & & B_{h_l} & \\ & & & \ddots \\ & & & & B_{h_m} \end{pmatrix}, f_2 \mid f_1, f_1 f_2 h_l \cdot \dots \cdot h_m = h_1 \cdot \dots \cdot h_m$$

f_2 normiert vom Grad ≥ 1 . Iteriere dieses Verfahren, dies bricht ab, erhalte normierte Polynome f_1, \dots, f_r vom Grad ≥ 1 , sodass $f_r \mid f_{r-1} \mid \dots \mid f_1, f_1 \cdot \dots \cdot f_r = h_1 \cdot \dots \cdot h_m$ und

$$A \approx \begin{pmatrix} B_{f_1} & & \\ & \ddots & \\ & & B_{f_r} \end{pmatrix} \approx \begin{pmatrix} B_{f_r} & & \\ & \ddots & \\ & & B_{f_1} \end{pmatrix} = B_{f_r, \dots, f_1}$$

Eindeutigkeit der Frobeniusnormalform $\implies f_1, \dots, f_r$ eindeutig bestimmt. Über die Faktoren von f_1, \dots, f_r bekommt man m und h_1, \dots, h_n (bis auf Reihenfolge) zurück. $\implies m$ eindeutig bestimmt, h_1, \dots, h_m eindeutig bis auf Reihenfolge. \square

Beispiel 28.16

1.

$$A = \begin{pmatrix} -2 & 1 & 5 \\ 1 & 1 & -2 \\ 3 & 1 & 6 \end{pmatrix} \in M(3 \times 3, \mathbb{Q})$$

$\implies c_1(A) = 1, c_2(A) = 1, c_3(A) = (t-1)(t-2)^2$. Mit $h_1 = t-1, h_2 = (t-2)^2 = t^2 - 4t + 4$ ist

$$A \approx B_{h_1, h_2} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -4 \\ 0 & 1 & 4 \end{pmatrix}$$

(Weierstrassnormalform von A)

2. (vergleiche 28.6.2)

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

$\implies c_1(A) = 1, c_2(A) = 1, c_3(A) = t-3, c_4(A) = (t-3)^2(t-2)$. Mit $h_1 := t-3, h_2 := (t-3)^2 = t^2 - 6t + 9, h_3 := t-2$ ist

$$A = B_{h_1, h_2, h_3} = \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 0 & -9 & 0 \\ 0 & 1 & 6 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$$

(Weierstrassnormalform von A)

Ziel: Einfachere Normalform, falls χ_A^{char} in Linearfaktoren zerfällt (und damit alle Weierstrasssteiler Potenzen linearer Polynome sind.)

Bemerkung+Definition 28.17 $\lambda \in K, f = (t - \lambda)^e \in K[t]$. Dann gilt:

$$B_f \approx \begin{pmatrix} \lambda & & & 0 \\ & \ddots & & \\ 1 & & \ddots & \\ & & \ddots & \ddots \\ 0 & & & 1 & \lambda \end{pmatrix} =: J(\lambda, e) \in M(e \times e, K)$$

($e = 1 : J(\lambda, 1) = (\lambda)$). Eine Matrix der Form $J(\lambda, e)$ heißt **Jordanmatrix** über K .

Beweis Sei $J := J(\lambda, e)$

$$\Rightarrow P_J = \begin{pmatrix} t - \lambda & & & \\ & -1 & \ddots & \\ & & \ddots & \ddots \\ & & & -1 & t - \lambda \end{pmatrix} \Rightarrow d_e(J) = (t - \lambda)^e$$

Es ist

$$\det \left(\begin{pmatrix} t - \lambda & & & \\ & -1 & \ddots & \\ & & \ddots & \ddots \\ & & & -1 & t - \lambda \end{pmatrix} \right) = (-1)^{e-1} \Rightarrow d_{e-1} = 1$$

$\xrightarrow{28.4} d_1(J) = \dots = d_{e-2}(J) = 1. \Rightarrow$ Determinantenteiler von J stimmen mit Determinatenteilern von B_f überein $\xrightarrow{\text{Invariantenteilersatz}} B_f \approx J$ \square

Satz+Definition 28.18 (Jordansche Normalform) $A \in M(n \times n, K)$, χ_A^{char} zerfalle in $K[t]$ in Linearfaktoren. Dann existieren Jordanmatrixen $J_1 = J(\lambda_1, e_1), \dots, J_m = J(\lambda_m, e_m)$ über K , sodass

$$A \approx \begin{pmatrix} J_1 & & \\ & \ddots & \\ & & J_m \end{pmatrix} =: J$$

Hierbei sind $\lambda_1, \dots, \lambda_m$ die (nicht notwendigerweise verschiedenen) Eigenwerte von A (= Nullstellen von χ_A^{char}). J_1, \dots, J_m sind bis auf Reihenfolge eindeutig bestimmt. Die Matrix J heißt eine **Jordansche Normalform** (JNF) von A .

Beweis 1. Existenz: Es ist $\chi_A^{char} = d_n(A) = c_1(A) \cdot \dots \cdot c_n(A) \Rightarrow c_1(A), \dots, c_n(A)$ zerfallen alle in Linearfaktoren. \Rightarrow Alle Weierstrasssteiler h_1, \dots, h_m von A sind Potenzen von linearen Polynomen $h_i = (t - \lambda_i)^{e_i}$ für ein $\lambda_i \in K, e_i \in \mathbb{N}$. Wegen $h_1 \cdot \dots \cdot h_m = c_1(A) \cdot \dots \cdot c_n(A) = \chi_A^{char}$ sind die λ_i genau die Eigenwerte von A . Setze $J_i := J(\lambda_i, e_i) \xrightarrow{28.17} B_{h_i} \approx J(\lambda_i, e_i) \forall i = 1, \dots, m$.

$$\Rightarrow A \approx \begin{pmatrix} B_{h_1} & & \\ & \ddots & \\ & & B_{h_m} \end{pmatrix} \approx \begin{pmatrix} J_1 & & \\ & \ddots & \\ & & J_m \end{pmatrix}$$

2. Eindeutigkeit von J_1, \dots, J_m bis auf Reihenfolge: folgt aus Eindeutigkeit der Weierstrassnormalform bis auf Reihenfolge von h_1, \dots, h_m \square

Anmerkung • Üblicherweise gruppiert man in der Jordanschen Normalform Jordanmatrizen zu gleichen Eigenwerten zusammen. (zu einem Block mit aufsteigenden e_i 's)

- Es gilt: A diagonalisierbar \iff Jordansche Normalform von A ist eine Diagonalmatrix (denn: „ \Leftarrow “ trivial „ \Rightarrow “ da Diagonalmatrizen bereits in Jordanscher Normalform sind) (mit 1×1 -Jordanmatrizen)

Algorithmus 28.19 (Algorithmus zur Jordanschen Normalform) **Eingabe:** $A \in M(n \times n, K)$, sodass χ_A^{char} in Linearfaktoren zerfällt.

Ausgabe: Jordansche Normalform von A .

Durchführung:

1. Bestimme die nicht konstanten Invariantenteiler von g_1, \dots, g_r von A .

2. Bestimme die Primfaktorzerlegung

$$g_i = (t - \lambda_{i,1})^{m_{i,1}} \cdot \dots \cdot (t - \lambda_{i,k_i})^{m_{i,k_i}}$$

3. Erhalte:

$$A \approx \begin{pmatrix} J(\lambda_{1,1}, m_{1,1}) & & \\ & \ddots & \\ & & J(\lambda_{r,k_r}, m_{r,k_r}) \end{pmatrix}$$

4. Gruppiere Jordanmatrizen zu gleichen Eigenwerten zusammen (jeweils nach aufsteigender Größe geordnet.)

Beispiel 28.20 (28.20)

1. (vergleiche 28.16.2)

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

$\implies c_1(A) = 1, c_2(A) = 1, c_3(A) = t - 1 =: g_1, c_4(A) = (t - 3)^2(t - 2) =: g_2$. Weierstrasteiler von A : $h_1 = t - 3, h_2 = (t - 3)^2, h_3 = t - 2$

$$\implies A \approx B_{h_1, h_2, h_3} = \begin{pmatrix} B_{h_1} & & \\ & B_{h_2} & \\ & & B_{h_3} \end{pmatrix} \approx \begin{pmatrix} J(3, 1) & & \\ & J(3, 2) & \\ & & J(2, 1) \end{pmatrix} = \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 1 & 3 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$$

2. (vergleiche 28.6)

$$A = \begin{pmatrix} 0 & 1 & 3 \\ 3 & 1 & -4 \\ -2 & 1 & 5 \end{pmatrix} \in M(3 \times 3, \mathbb{Q}) \implies c_1(A) = 1, c_2(A) = 1, c_3(A) = (t - 2)^3$$

\implies Weierstrasteiler von A : $h_1 = (t - 2)^3$

$$\implies A \approx B_{h_1} = J(2, 3) = \begin{pmatrix} 2 & 0 & 0 \\ 1 & 2 & 0 \\ 0 & 1 & 2 \end{pmatrix}$$

3.

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

$$\implies c_1(A) = 1, c_2(A) = t - 2, c_3(A) = (t - 2)^2 \implies \text{Weierstrasteiler von } A: h_1 = t - 2, h_2 = (t - 2)^2$$

$$\implies A \approx B_{h_1, h_2} = \begin{pmatrix} B_{h_1} & \\ & B_{h_2} \end{pmatrix} \approx \begin{pmatrix} J(2, 1) & \\ & J(2, 2) \end{pmatrix} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 1 & 2 \end{pmatrix}$$

29 Moduln

In diesem Abschnitt sei R sets ein kommutativer Ring.

Definition 29.1 (Modul) Eine Menge M zusammen mit einer Verknüpfung

$$+ : M \times M \rightarrow M, (x, y) \mapsto x + y$$

(genannt **Addition**) und einer äußeren Verknüpfung

$$\cdot : R \times M \rightarrow M, (a, x) \mapsto ax$$

(genannt **skalare Multiplikation**) heißt ein **R-Modul**, wenn gilt:

- (M1) $(M, +)$ ist eine abelsche Gruppe, Das neutrale Element bezeichnen wir mit 0, das Inverse zu $x \in M$ mit $-x$.
- (M2) Die skalare Multiplikation ist in folgender Weise mit den Verknüpfungen auf M und R verträglich:
 - $(a + b)x = ax + bx$
 - $a(x + y) = ax + ay$
 - $(ab)x = a(bx)$
 - $1 \cdot x = x$

$$\forall a, b \in R, x, y \in M$$

Beispiel 29.2

1. K Körper, V K -Vektorraum $\implies V$ ist ein K -Modul.
2. $(G, +)$ abelsche Gruppe wird zum \mathbb{Z} -Modul durch

$$\mathbb{Z} \times G \rightarrow G, (n, g) \mapsto \begin{cases} \underbrace{g + \dots + g}_{n\text{-mal}} & n \in \mathbb{N} \\ 0 & n = 0 \\ -\underbrace{(g + \dots + g)}_{n\text{-mal}} & -n \in \mathbb{N} \end{cases}$$

Umgekehrt ist jeder \mathbb{Z} -Modul eine abelsche Gruppe bezüglich „+“.

3. $I \subseteq R$ Ideal $\implies I$ ist ein R -Modul (Addition: auf I eingeschränkte Addition von R , skalare Multiplikation: $R \times I \rightarrow I, (a, x) \mapsto ax$). Insbesondere ist R ein R -Modul.

4. $I \subseteq R$ Ideal $\implies R/I$ ist ein R -Modul (skalare Multiplikation: $R \times R/I \rightarrow R/I, (a, \bar{x}) \mapsto \overline{ax}$)

5. K Körper, V K -Vektorraum, $\varphi \in \text{End}(V) \implies V$ ist $K[t]$ -Modul via skalare Multiplikation:

$$K[t] \times V \rightarrow V, (f, v) \mapsto f(\varphi)(v)$$

Definition 29.3 M, N R -Moduln, $\varphi : M \rightarrow N$. φ heißt R -Modul-**Homomorphismus** $\stackrel{\text{Def}}{\iff}$ Für alle $x, y \in M, a \in R$ gilt:

$$\begin{aligned}\varphi(x + y) &= \varphi(x) + \varphi(y) \\ \varphi(ax) &= a\varphi(x)\end{aligned}$$

φ heißt $(R\text{-Modul})$ -**Isomorphismus** $\stackrel{\text{Def}}{\iff} \varphi$ ist ein bijektiver R -Modul-Homomorphismus. \exists ein Isomorphismus zwischen M, N , so schreiben wir $M \cong N$.

Definition 29.4 M R -Modul, $N \subseteq M$. N heißt ein **Untermodul** von M $\stackrel{\text{Def}}{\iff}$ Folgende Bedingungen sind erfüllt:

- (U1) $0 \in N$
- (U2) $x, y \in N \implies x + y \in N$
- (U3) $a \in R, x \in N \implies ax \in N$

Beispiel 29.5

1. K Körper, V K -Vektorraum \implies Untermoduln von V = Untervektorräume von V
2. $M = R$ als R -Modul \implies Untermodul von M = Ideale in R .

Bemerkung+Definition 29.6 M R -Modul, $N \subseteq M$ Untermodul. Dann gilt: Durch $x \sim y \stackrel{\text{Def}}{\iff} x - y \in N$ eine Äquivalenzrelation definiert. Die Äquivalenzklasse \bar{x} von $x \in M$ ist gegeben durch

$$\bar{x} = x + N = \{x + y \mid y \in N\}$$

Die Menge aller Äquivalenzklassen bezeichnen wir mit M/N . M/N wird mit den Verknüpfungen

$$\begin{aligned}+ : M/N \times M/N &\rightarrow M/N, \bar{x} + \bar{y} := \overline{x + y} \\ \cdot : R \times M/N &\rightarrow M/N, a \cdot \bar{x} := \overline{ax}\end{aligned}$$

zu einem R -Modul, dem **Faktormodul** M/N . Die **kanonische Projektion**

$$\pi : M \rightarrow M/N, x \mapsto \bar{x}$$

ist ein surjektiver R -Modulhomomorphismus

Beweis analog zu K -Vektorraum, vergleiche 13.7, 13.8 □

Bemerkung+Definition 29.7 M, N R -Moduln, $\varphi : M \rightarrow N$ Homomorphismus. Dann gilt:

1. $\ker \varphi := \{x \in M \mid \varphi(x) = 0\}$ ist ein Untermodul von M .
2. φ ist injektiv $\iff \ker \varphi = \{0\}$
3. $\text{im } \varphi := \varphi(M)$ ist ein Untermodul von N .

4. $\text{coker } \varphi := N/\text{im } \varphi$ heißt der **Cokern** von φ , es gilt: φ surjektiv $\iff \text{coker } \varphi = \{0\}$
5. (Homomorphiesatz) φ induziert einen Isomorphismus

$$\Phi : M/\ker \varphi \rightarrow \text{im } \varphi, x + \ker \varphi \mapsto \varphi(x)$$

Beweis analog wie für K-Vektorraum. □

Bemerkung+Definition 29.8 M R-Modul, $(M_i)_{i \in I}$ Familie von Untermoduln von M . Dann gilt:

1.

$$\sum_{i \in I} M_i := \left\{ \sum_{i \in I} x_i \mid x_i \in M_i, x_i = 0 \text{ für fast alle } i \in I \right\}$$

ist ein Untermodul von M und heißt die **Summe** der $M_i, i \in I$.

2.

$$\cap_{i \in I} M_i$$

ein Untermodul von M .

Beweis nachrechnen. □

Bemerkung+Definition 29.9 $(M_i)_{i \in I}$ Familie von R-Moduln. Dann gilt:

1.

$$\prod_{i \in I} M_i := \{(x_i)_{i \in I} \mid x_i \in M_i\}$$

wird mit komponentenweiser Addition und skalarer Multiplikation ein R-Modul, das **direkte Produkt** der $M_i, i \in I$

2.

$$\oplus_{i \in I} M_i := \{(x_i)_{i \in I} \mid x_i \in M_i, x_i = 0 \text{ für fast alle } i \in I\}$$

wird mit komponentenweiser Addition und skalarer Multiplikation ein R-Modul, die **direkte Summe** der $M_i, i \in I$

Falls I endlich, dann ist

$$\prod_{i \in I} M_i = \oplus_{i \in I} M_i$$

Spezialfall:

$$R^n = \oplus_{i=1}^n R$$

Beweis nachrechnen. □

Anmerkung Zusammenhang zur direkten Summe von Untervektorräumen aus LA1: Sei M R-Modul, $M_1, M_2 \subseteq M$ Untermoduln

$$M_1 \oplus M_2 = \{(m_1, m_2) \mid m_1 \in M_1, m_2 \in M_2\}$$

\implies Erhalte surjektiven Homomorphismus

$$\varphi : M_1 \oplus M_2 \rightarrow M_1 + M_2, (m_1, m_2) \mapsto m_1 + m_2$$

ist $M_1 \cap M_2 = \{0\}$, dann ist

$$\ker \varphi = \{(m_1, m_2) \in M_1 \oplus M_2 \mid m_1 + m_2 = 0\} = \{0\}$$

denn: $m_1 + m_2 = 0 \implies m_1 = -m_2 \in M_1 \cap M_2 = \{0\}$, also $m_1 = m_2 = 0$. das heißt wir erhalten einen Isomorphismus von R-Moduln $M_1 \oplus M_2 \cong M_1 + M_2$. Insbesondere: ist $M_1 + M_2 = M$, $M_1 \cap M_2 = \{0\}$, dann ist $M_1 \oplus M_2 \cong M$.

Bemerkung+Definition 29.10 $I \subseteq R$ Ideal, M R -Modul, $(x_i)_{i \in I}$ Familie von Elementen aus M . Dann gilt:

1.

$$JM := \left\{ \sum_{i=1}^n a_i \cdot x_i \mid a_i \in I, x_i \in M, n \in \mathbb{N} \right\}$$

ist ein Untermodul von M .

2.

$$\text{Lin}((x_i)_{i \in I}) := \left\{ \sum_{i \in I} a_i x_i \mid a_i \in R, a_i = 0 \text{ für fast alle } i \in I \right\}$$

ist ein Untermodul von M , die **lineare Hülle** von $(x_i)_{i \in I}$.

Definition 29.11 M R -Modul, $(x_i)_{i \in I}$ Familie von Elementen aus M . $(x_i)_{i \in I}$ heißt

• **Erzeugendensystem** von $M \xLeftrightarrow{\text{Def}} M = \text{Lin}((x_i)_{i \in I})$.

• **linear unabhängig** $\xLeftrightarrow{\text{Def}}$ aus

$$\sum_{i \in I} a_i x_i = 0$$

wobei $a_i \in R, a_i = 0$ für fast alle $i \in I$ folgt $a_i = 0 \forall i \in I$

• **Basis** von $M \xLeftrightarrow{\text{Def}} (x_i)_{i \in I}$ ist ein linear unabhängiges Erzeugendensystem von M .

M heißt

• **endlich erzeugt** $\xLeftrightarrow{\text{Def}}$ M besitzt ein endliches Erzeugendensystem

• **frei** $\xLeftrightarrow{\text{Def}}$ M besitzt eine Basis

• **endlichfrei** $\xLeftrightarrow{\text{Def}}$ M besitzt eine endliche Basis

Beispiel 29.12

1. K Körper \implies Jeder K -Vektorraum ist frei

2. R ist freier R -Modul ((1) ist eine Basis)

3. Sei $n \in \mathbb{N}, n > 1$

• $\mathbb{Z}/n\mathbb{Z}$ ist endlich erzeugtes \mathbb{Z} -Modul, denn:

– $\mathbb{Z}/n\mathbb{Z}$ ist als abelsche Gruppe ein \mathbb{Z} -Modul.

– $\text{Lin}((\bar{1})) = \{r \cdot \bar{1} \mid r \in \mathbb{Z}\} = \{\bar{r} \mid r \in \mathbb{Z}\} = \mathbb{Z}/n\mathbb{Z}$. $(\bar{1})$ ist ein Erzeugendensystem von \mathbb{Z} als \mathbb{Z} -Modul.

– $\mathbb{Z}/n\mathbb{Z}$ ist kein freier \mathbb{Z} -Modul, denn: Sei $x = \bar{a} \in \mathbb{Z}/n\mathbb{Z} \implies nx = n\bar{a} = \overline{na} = \bar{0}$, aber $n \neq 0$. $\implies (x)$ linear abhängig \implies Jede Familie $\neq ()$ von $\mathbb{Z}/n\mathbb{Z}$ ist linear abhängig. Insbesondere kann $\mathbb{Z}/n\mathbb{Z}$ keine Basis als \mathbb{Z} -Modul haben.

Beachte: Als $\mathbb{Z}/n\mathbb{Z}$ -Modul ist $\mathbb{Z}/n\mathbb{Z}$ frei (siehe 2.)

Fazit: Es gibt Moduln, die keine Basis haben.

Bemerkung 29.13 M freier R -Modul, $\mathcal{B} = (x_i)_{i \in I}$ Basis von M . Dann existiert ein Modulisomorphismus

$$\Phi_{\mathcal{B}} : \bigoplus_{i \in I} R \rightarrow M, (a_i)_{i \in I} \mapsto \sum_{i \in I} a_i x_i$$

(beachte: $a_i = 0$ für fast alle $i \in I$)

Beweis • $\Phi_{\mathcal{B}}$ Homomorphismus: klar

- $\Phi_{\mathcal{B}}$ surjektiv, denn: \mathcal{B} Erzeugendessystem von M
- $\Phi_{\mathcal{B}}$ injektiv, denn: \mathcal{B} linear unabhängig □

Anmerkung • Man kann zeigen: Sind $(x_i)_{i \in I}, (y_j)_{j \in J}$ Basen des freien R -Moduls M , dass existiert eine Bijektion $I \rightarrow J$, das heißt $|I| = |J|$. Wir werden obige Aussage in 30 für endlich freie Moduln über Hauptidealringe zeigen.

- Man kann zeigen: M endlich erzeugt $\iff M$ endlich frei
- Achtung: Es gilt im Allgemeinen kein Analogon des Basisauswahlsatzes: $(2, 3)$ ist ein Erzeugendensystem des freien \mathbb{Z} -Moduls \mathbb{Z} wegen $1 = (-1) \cdot 2 + 1 \cdot 3$, aber weder (2) noch (3) sind Basen von \mathbb{Z} .

Anmerkung Man kann zeigen: Sind M, N endlich freie R -Moduln, dann kann man analog zu LA1 jeden Modulhomomorphismus $\varphi : M \rightarrow N$ nach Wahl von Basen \mathcal{A} von M, \mathcal{B} von N durch eine Darstellungsmatrix $M_{\mathcal{B}}^{\mathcal{A}}(\varphi)$ beschreiben. Es gilt die Basiswechselformel

$$M_{\mathcal{B}'}^{\mathcal{B}'}(\varphi) = T_{\mathcal{B}'}^{\mathcal{B}} M_{\mathcal{A}}^{\mathcal{A}'} T_{\mathcal{A}}^{\mathcal{A}'}$$

wobei $T_{\mathcal{A}}^{\mathcal{A}'} = M_{\mathcal{A}}^{\mathcal{A}'}(\text{id}_M), T_{\mathcal{B}'}^{\mathcal{B}} = M_{\mathcal{B}'}^{\mathcal{B}}(\text{id}_M)$ (Beweis analog zu LA1).

Bemerkung 29.14 M, N R -Moduln, $\varphi : M \rightarrow N$ Homomorphismus, sodass $\ker(\varphi), \text{im}(\varphi)$ endlich erzeugt. Dann ist M ein endlich erzeugtes R -Modul.

Beweis Sei (x_1, \dots, x_m) ein Erzeugendensystem von $\ker \varphi \subseteq M, (y_1, \dots, y_n)$ ein Erzeugendensystem von $\text{im} \varphi \subseteq N$. Wir wählen $\tilde{y}_i \in \varphi^{-1}(\{y_i\})$ für $i = 1, \dots, n$. Behauptung: $(x_1, \dots, x_m, \tilde{y}_1, \dots, \tilde{y}_n)$ ist ein Erzeugendensystem von M , denn: Sei $m \in M \implies \varphi(m) \in \text{im} \varphi$, das heißt $\exists a_1, \dots, a_n \in R$, sodass

$$\begin{aligned} \varphi(m) &= a_1 y_1 + \dots + a_n y_n = a_1 \varphi(\tilde{y}_1) + \dots + a_n \varphi(\tilde{y}_n) \\ &= \varphi(a_1 \tilde{y}_1 + \dots + a_n \tilde{y}_n) \\ \implies m - (a_1 \tilde{y}_1 + \dots + a_n \tilde{y}_n) &\in \ker \varphi \end{aligned}$$

$$\begin{aligned} \implies \exists b_1, \dots, b_m \in R : m - (a_1 \tilde{y}_1 + \dots + a_n \tilde{y}_n) &= b_1 x_1 + \dots + b_m x_m \\ \implies m &= b_1 x_1 + \dots + b_m x_m + a_1 \tilde{y}_1 + \dots + a_n \tilde{y}_n \end{aligned} \quad \square$$

Bemerkung+Definition 29.15 M R -Modul. $x \in M$ heißt ein **Torsionselement** von $M \stackrel{\text{Def}}{\iff} \exists a \in R, a \text{ kein Nullteiler, mit } ax = 0$.

$$T(M) = \{x \in M \mid x \text{ ist ein Torsionselement}\}$$

ist ein Untermodul von M , der **Torsionsuntermodul** von M . M heißt

Torsions-R-Modul $\stackrel{\text{Def}}{\iff} T(M) = M$

torsionsfreier R-Modul $\stackrel{\text{Def}}{\iff} T(M) = \{0\}$

Beweis U1: $0 \in T(M)$ wegen $1_R \cdot 0 = 0$.

U2: $x, y \in T(M) \implies \exists a, b \in R, a, b \text{ keine Nullteiler mit } ax = 0, by = 0$.

$$\implies abx = 0, aby = 0 \implies ab(x + y) = 0$$

Wegen a, b keine Nullteiler ist ab auch kein Nullteiler $\implies x + y \in T(M)$.

U3: Sei $x \in T(M), a \in R \implies \exists b \in R, b \text{ kein Nullteiler mit } bx = 0$

$$\implies b(ax) = 0 = (ba)x = (ab)x = a \underbrace{(bx)}_{=0} = 0 \implies ax \in T(M)$$

□

Anmerkung Falls R nullteilerfrei, dann $T(M) = \{x \in M \mid \exists a \in R, a \neq 0 : ax = 0\}$

Beispiel 29.16

1. K Körper, V K -Vektorraum $\implies V$ ist torsionsfreier K -Modul, denn:

$$T(V) = \{x \in V \mid \exists \lambda \in K, \lambda \neq 0 : \lambda x = 0\} = \{0\}$$

2. \mathbb{Z} ist ein torsionsfreier \mathbb{Z} -Modul, denn:

$$T(\mathbb{Z}) = \{x \in \mathbb{Z} \mid \exists a \in \mathbb{Z}, a \neq 0 : ax = 0\} = \{0\}$$

3. Für $n \in \mathbb{N}, n > 1$ ist $\mathbb{Z}/n\mathbb{Z}$ ein Torsions- \mathbb{Z} -Modul, denn für alle $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ ist

$$n \cdot \bar{a} = \overline{na} = \bar{0}$$

das heißt

$$T(\mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$$

Bemerkung 29.17 F freier R -Modul. Dann ist F torsionsfrei, das heißt $T(F) = \{0\}$

Beweis Sei $(x_i)_{i \in I}$ eine Basis von $F, y \in T(F), a \in R$ kein Nullteiler mit $ay = 0$. $\implies \exists b_{i_1}, \dots, b_{i_s} : y = b_{i_1}x_{i_1} + \dots + b_{i_s}x_{i_s}$.

$$\implies 0 = ay = ab_{i_1}x_{i_1} + \dots + ab_{i_s}x_{i_s} \implies ab_{i_1} = \dots = ab_{i_s} = 0$$

$$\implies b_{i_1} = \dots = b_{i_s} = 0 \implies y = 0, \text{ also } T(F) = \{0\}$$

□

Anmerkung Die Umkehrung ist falsch: \mathbb{Q} ist torsionsfreier \mathbb{Z} -Modul, aber kein freier \mathbb{Z} -Modul.

- \mathbb{Q} ist torsionsfreier \mathbb{Z} -Modul, denn: $T(\mathbb{Q}) = \{x \in \mathbb{Q} \mid \exists a \in \mathbb{Z}, a \neq 0 : ax = 0\} = \{0\}$
- \mathbb{Q} ist kein freier \mathbb{Z} -Modul, denn:
 - Sind $a, b \in \mathbb{Q}$, dann ist die Familie (a, b) \mathbb{Z} -linear abhängig, da: Ist $a = m_1/n_1 \neq 0, b = m_2/n_2 \neq 0$, dann ist

$$m_2n_1a - m_1n_2b = 0$$
 - Leere Familie, beziehungsweise einelementige Familien sind keine Erzeugendensysteme von \mathbb{Q} als \mathbb{Z} -Modul.

Definition 29.18 (Länge) M R -Modul.

$l_R(M) := \sup\{l \in \mathbb{N}_0 \mid M_0 = \{0\} \subsetneq M_1 \subsetneq M_2 \subsetneq \dots \subsetneq M_l = M \text{ ist eine Kette von Untermoduln von } M\} \in \mathbb{N}_0 \cup \{\infty\}$

heißt die **Länge** von M .

Beispiel 29.19

1. K Körper, V K -Vektorraum $\implies L_K(V) = \dim_K(V)$, denn:

- $\dim_K(V) = n < \infty \implies$ Wähle Basis (v_1, \dots, v_n) von V , dann ist

$$M_0 = \{0\} \subsetneq \text{Lin}(v_1) \subsetneq \text{Lin}(v_1, v_2) \subsetneq \dots \subsetneq \text{Lin}(v_1, \dots, v_n) = V$$

eine Kette von Untervektorräumen von $V \implies l_K(V) \geq n$.

Ist $M_0 = \{0\} \subsetneq M_1 \subsetneq \dots \subsetneq M_l = V$ eine Kette von Untermoduln, dann ist $0 < \dim M_1 < \dots < \dim M_l = \dim V = n$, insbesondere $\dim V = \dim M_l \geq l$, also $l_K(V) \leq n$.

- $\dim_K(V) = \infty \implies l_K(V) = \infty$.

2. $l_{\mathbb{Z}}(\mathbb{Z}) = \infty$, dann: für alle $n \in \mathbb{N}$ ist $0 \subsetneq 2^n \mathbb{Z} \subsetneq 2^{n-1} \mathbb{Z} \subsetneq \dots \subsetneq 2 \mathbb{Z} \subsetneq \mathbb{Z}$ eine Kette von Untermoduln von \mathbb{Z} .

3. $l_{\mathbb{Z}}(\mathbb{Z}/6\mathbb{Z}) = 2$, dann: Für $\bar{a} \in \mathbb{Z}/6\mathbb{Z}$ ist

$$\text{Lin}(\bar{a}) = \begin{cases} \mathbb{Z}/6\mathbb{Z} & \bar{a} \in \{\bar{1}, \bar{5}\} \\ \{\bar{0}\} & \bar{a} = \bar{0} \\ \{\bar{0}, \bar{3}\} & \bar{a} = \bar{3} \\ \{\bar{0}, \bar{2}, \bar{4}\} & \bar{a} \in \{\bar{2}, \bar{4}\} \end{cases}$$

\implies Die beiden Ketten $\{0\} \subsetneq \text{Lin}(\{\bar{3}\}) \subsetneq \mathbb{Z}/6\mathbb{Z}$, $\{\bar{0}\} \subsetneq \text{Lin}(\bar{2}) \subsetneq \mathbb{Z}/6\mathbb{Z}$ können nicht weiter verfeinert werden, also $l_{\mathbb{Z}}(\mathbb{Z}/6\mathbb{Z}) = 2$

4. $l_R(M) = 0 \iff M = \{0\}$

Bemerkung 29.20 M R -Modul, $N \subseteq M$ Untermodul. Dann gilt: $l_R(N) \leq l_R(M)$.

Beweis Ist $0 \subsetneq N_1 \subsetneq N_2 \subsetneq \dots \subsetneq N_l = N$ eine Kette von Untermoduln von N , dann ist $0 \subsetneq N_1 \subsetneq \dots \subsetneq N_l = N \subseteq M$ eine Kette von Untermoduln von M gleicher oder größerer Länge. \square

Bemerkung 29.21 M', M'' R -Moduln. Dann gilt: $l_R(M' \oplus M'') = l_R(M') + l_R(M'')$.

Beweis 1. Es genügt zu zeigen: M R -Modul, $M', M'' \subseteq M$ Untermoduln mit $M = M' \oplus M''$, dann ist

$$l_R(M) = l_R(M') + l_R(M'')$$

(Setze $M = M' \oplus M''$, ersetze M', M'' durch isomorphen Moduln $M' \oplus \{0\}$, $\{0\} \oplus M''$, M ist die direkte Summe dieser Untermoduln)

2. Beweis von „ \geq “

Seien $\{0\} \subsetneq M'_1 \subsetneq \dots \subsetneq M'_r = M'$, $\{0\} \subsetneq M''_1 \subsetneq \dots \subsetneq M''_s = M''$ Ketten von Untermoduln von M' beziehungsweise von M'' .

$$\implies \{0\} \subsetneq M'_1 \oplus \{0\} \subsetneq \dots \subsetneq M'_r \oplus \{0\} \subsetneq M'_r \oplus M''_1 \subsetneq \dots \subsetneq M'_r \oplus M''_s = M$$

ist eine Kette von Untermoduln von M .

3. Beweise von „ \leq “

Sei $0 \subsetneq M_1 \subsetneq \dots \subsetneq M_l = M$ eine Kette von Untermoduln von M . Wir betrachten die Abbildung

$$\pi : M = M' \oplus M'' \rightarrow M'', a + b \mapsto b$$

Behauptung: Für alle $0 \leq i < l$ gilt:

$$M_i \cap M' \subsetneq M_{i+1} \cap M' \text{ oder } \pi(M_i) \subsetneq \pi(M_{i+1})$$

Annahme: Es existiert i mit $M_i \cap M' = M_{i+1} \cap M'$ und $\pi(M_i) = \pi(M_{i+1})$. \implies Für alle $a \in M_{i+1} \exists b \in M_i : \pi(a) = \pi(b)$.

$$\implies a - b \in \ker \pi = M' \implies a - b \in M_{i+1} \cap M' = M_i \cap M' \subseteq M_i$$

$$a = (a - b) + b \in M_i \implies M_{i+1} \subseteq M_i \subseteq M_{i+1} \implies M_{i+1} = M_i$$

Wegen der Behauptung gibt es in den Ketten $0 \subseteq \pi(M_1) \subseteq \dots \subseteq \pi(M_l) = M''$ und $0 \subseteq M_1 \cap M' \subseteq \dots \subseteq M_l \cap M' = M'$ zusammen mindestens l echte Inklusionen, höchstens aber $l_R(M'') + l_R(M')$ echte Inklusionen. $\implies l \leq l_R(M') + l_R(M'')$ \square

30 Moduln über Hauptidealringen

In diesem Abschnitt sei R stets ein Hauptidealring.

Ziel: Struktursatz für endlich erzeugte R -Moduln.

Bemerkung+Definition 30.1 F endlich freier R -Modul. Dann gilt: Je zwei Basen von F haben dieselbe Kardinalität. Diese heißt **Rang** von F .

Beweis 1. Falls R Körper, dann F endlichdimensionaler R -Vektorraum, Behauptung folgt aus 9.8. Im Folgenden sei R kein Körper.

2. Da F endlich frei, existiert endliche Basis (v_1, \dots, v_s) von F . Sei $(w_i)_{i \in I}$ eine beliebige Basis von F

$$\implies F \cong R^s, \quad F \cong \bigoplus_{i \in I} R =: M$$

$$\implies \exists R\text{-Modulisomorphismus } \rho : R^s \rightarrow M.$$

3. Es existiert irreduzibles Element $p \in R$. dann: R kein Körper $\implies \exists a \in R \setminus (R^* \cup \{0\}) \implies a$ lässt sich als Produkt irreduzibler Elemente schreiben \implies es existieren irreduzible Elemente $p \in R$.

4. Wir betrachten Abbildung $\bar{\rho} : R^s \rightarrow M/pM, x \mapsto \rho(x) + pM$

- $\bar{\rho}$ ist Homomorphismus, da ρ Homomorphismus

- $\bar{\rho}$ ist surjektiv, da ρ surjektiv

- $\ker \bar{\rho} = pR^s$, denn: „ \supseteq “: Sei $x \in pR^s \exists y \in R^s : x = py \implies \bar{\rho}(x) = \rho(x) + pM = \rho(py) + pM = \underbrace{p\rho(y)}_{\in pM} + pM \implies x \in \ker \bar{\rho}$

„ \subseteq “ Sei $x \in \ker \bar{\rho} \implies \rho(x) \in pM \implies \exists y \in M : \rho(x) = py \implies \exists \tilde{y} \in R^s :$

$$y = \rho(\tilde{y}) \implies \rho(x) = p\rho(\tilde{y}) = \rho(p\tilde{y}) \implies x = p\tilde{y} \in pR^s$$

Nach Homomorphiesatz erhalten wir einen Isomorphismus

$$R^s/pR^s \rightarrow M/pM$$

von R -Moduln

5. Die Abbildung $\theta : R^s/pR^s \rightarrow (R/pR)^s, (x_1, \dots, x_s) + pR^s \mapsto (x_1 + pR, \dots, x_s + pR)$ ist ein Isomorphismus von R -Moduln:

- θ Homomorphismus: klar
- θ surjektiv: klar
- θ injektiv: Sei $\theta((x_1, \dots, x_s) + pR^s) = 0 = (pR, \dots, pR) \implies (x_1 + pR, \dots, x_s + pR) = (pR, \dots, pR) \implies x_1, \dots, x_s \in pR \implies (x_1, \dots, x_s) + pR^s = pR^s$.

Analog ist

$$M/pM = \bigoplus_{i \in I} R/p \oplus_{i \in I} R \cong \bigoplus_{i \in I} R/pR$$

6. Aus 4., 5. erhalten wir Isomorphismus $\Phi : \left(R/pR\right)^s \rightarrow \bigoplus_{i \in I} R/pR$ von R -Moduln. Da p irreduzibel, ist $K := R/pR$ ein Körper (Anmerkung nach 26.26). Quelle / Ziel von Φ sind K -Vektorräume via skalarer Multiplikation.

$$K \times \left(R/pR\right)^s \rightarrow \left(R/pR\right)^s, (a + pR) \cdot (x_1 + pR, \dots, x_s + pR) := (ax_1 + pR, \dots, ax_s + pR) = a(x_1 + pR, \dots, x_s + pR),$$

analog für $\bigoplus_{i \in I} R/pR$. Φ ist auch ein Isomorphismus von K -Vektorräumen, denn

$$\begin{aligned} \Phi((a + pR)(x_1 + pR, \dots, x_s + pR)) &= \Phi(a(x_1 + pR, \dots, x_s + pR)) = a\Phi(x_1 + pR, \dots, x_s + pR) \\ &= (a + pR)\Phi(x_1 + pR, \dots, x_s + pR) \end{aligned}$$

7. Wegen 6. ist $\Phi : K^s \rightarrow \bigoplus_{i \in I} K$ ein K -Vektorraum-Isomorphismus. Wegen 1. folgt $|I| = s$. □

Satz+Definition 30.2 $A \in M(m \times n, R)$. Dann existieren $r \in \mathbb{N}_0, c_1, \dots, c_r \in R \setminus \{0\}$, sodass

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

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

Beweis 1. Eindeutigkeit: Wie im Beweis von 27.17 über Fittingideale

2. Existenz: Wir gehen ähnlich vor wie bei Gauß-Diagonalisierung (vergleiche Beweis von 27.8) und modifizieren das Verfahren wie folgt: Setze $\delta : R \setminus \{0\} \rightarrow \mathbb{N}_0, a \mapsto \text{Anzahl der Primfaktoren von } a \text{ (mit Vielfachheit gerechnet)}$. (insbesondere $\delta(a) = 0$ für $a \in R^*$)

- Schritt: Erreiche durch Zeilen- und Spaltenvertauschung, dass $\delta(a_{11}) \leq \delta(a_{ij}) \forall i, j$ mit $a_{ij} \neq 0$
- Schritt: Bringe A auf die Form

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

Falls $a_{11} \mid a_{1i}$ und $a_{11} \mid a_{j1}$ für alle i, j , dann erreiche obige Form durch elementare Zeilen- und Spaltenumformungen. Andernfalls: Ohne Einschränkung gelte $a_{11} \nmid a_{i1}$ für ein $i > 1$. Da R Hauptidealring, ist $\text{GGT}(a_{i1}, a_{11}) \neq \emptyset$. Sei $\beta \in \text{GGT}(a_{i1}, a_{11})$. Da $a_{11} \nmid a_{i1}$ ist $\delta(\beta) < \delta(a_{11})$

(β kann nicht gleich viele Primteiler wie a_{11} haben, sonst $\beta \stackrel{\wedge}{=} a_{11} \implies a_{11} \mid a_{i1}$) Nach 26.22 existieren $u, v \in R$ mit $\beta = ua_{11} + va_{i1}$, und es existieren $\tilde{u}, \tilde{v} \in R$ mit

$$a_{11} = \beta\tilde{u}, a_{i1} = \beta\tilde{v} \implies \beta = u\beta\tilde{u} + v\beta\tilde{v} = \beta(u\tilde{u} + v\tilde{v}) \implies \beta(1 - (u\tilde{u} + v\tilde{v})) = 0 \\ \implies u\tilde{u} + v\tilde{v} = 1. \text{ Es ist}$$

$$\underbrace{\begin{pmatrix} u & & & v & & & \\ & 1 & & & & & \\ & & \ddots & & & & \\ & & & 1 & & & \\ -\tilde{v} & & & & \tilde{u} & & \\ & & & & & 1 & \\ & & & & & & \ddots \\ & & & & & & & 1 \end{pmatrix}}_{=:B} \begin{pmatrix} u & & & -v & & & \\ & 1 & & & & & \\ & & \ddots & & & & \\ & & & 1 & & & \\ \tilde{v} & & & & \tilde{u} & & \\ & & & & & 1 & \\ & & & & & & \ddots \\ & & & & & & & 1 \end{pmatrix} = \begin{pmatrix} 1 & & & & 0 & & \\ & 1 & & & & & \\ & & \ddots & & & & \\ & & & 1 & & & \\ 0 & & & & 1 & & \\ & & & & & 1 & \\ & & & & & & \ddots \\ & & & & & & & 1 \end{pmatrix}$$

das heißt $B \in \text{GL}(n, R)$. Multiplikation von B von links bewirkt folgende Zeilenoperationen:

- neue erste Zeile = u -faches der alten ersten Zeile + v -faches der alten i -ten Zeile
- neue i -te Zeile = $-\tilde{v}$ -faches der alten ersten Zeile + \tilde{u} -faches der alten i -ten Zeile

In der Matrix BA steht links oben das Element β mit $\delta(\beta) < \delta(a_{11})$. Erhalte durch Zeilen-/Spaltenvertauschung an $A' = BA$ eine Matrix $A'' = (a''_{ij})$ mit $\delta(a''_{11}) < \delta(a''_{ij})$ für alle $i, j, a''_{ij} \neq 0$ und $\delta(a''_{11}) < \delta(a_{11})$. Dieser Prozess bricht nach endlich vielen Iterationen ab. Wir erhalten eine Matrix der Form

$$D = \left(\begin{array}{c|c} d_{11} & 0 \\ \hline 0 & * \end{array} \right), d_{11} \neq 0, \delta(d_{11}) \leq \delta(a_{11}), \delta(d_{11}) \leq \delta(d_{ij}) \forall i, j, d_{ij} \neq 0$$

- c) Schritt: Führe das Verfahren analog zu der Gauß-Diagonalisierung über Euklidischen Ringen weiter (mit Modifikationen analog zu oben). \square

Bemerkung 30.3 R Hauptidealring, $a \in R \setminus (R^* \cup \{0\})$, $a = p_1 \cdot \dots \cdot p_r$ mit irreduziblen Elementen p_1, \dots, p_r (nicht notwendig paarweise verschieden). Dann ist

$$l_R(R/aR) = r$$

insbesondere ist $l_R(R/aR) < \infty$

Beweis 1. Nach Übungen induziert die kanonische Projektion $\pi : R \rightarrow R/aR$ eine Bijektion

$$\Phi : \{\text{Ideale } I \subseteq R, I \supseteq aR\} \rightarrow \{\text{Ideale von } R/aR\}$$

Hierbei: Ideale in $R/aR = R/aR$ -Untermoduln von $R/aR = R$ -Untermoduln von R/aR (skalare Multiplikation: $R \times R/aR \rightarrow R/aR, (b, x + aR) \mapsto bx + aR$)

2. Aus 1. folgt:

$$\begin{aligned} l_R(R/aR) &= \sup\{l \in \mathbb{N}_0 \mid (a) \subsetneq I_1 \subsetneq \dots \subsetneq I_l = R, I_k \text{ Ideale in } R\} \\ &= \sup\{l \in \mathbb{N}_0 \mid (a) \subsetneq (a_1) \subsetneq \dots \subsetneq (a_l) = R, a_i \in R\} \\ &= \sup\{l \in \mathbb{N}_0 \mid a_l \mid a_{l-1} \mid \dots \mid a_1 \mid a_0 := a, a_i \in R, a_l \in R^*, a_i \not\stackrel{\wedge}{=} a_{i+1}, i = 0, \dots, l-1\} \end{aligned}$$

3. Wegen $1 \mid p_1 \mid p_1 p_2 \mid \cdots \mid p_1 \cdot \dots \cdot p_r = a$ folgt $l_R(R/aR) \geq r$

Da R Hauptidealring und insbesondere faktoriell, hat a bis auf Assoziiertheit nur endlich viele Teiler, insbesondere $l_R(R/aR) < \infty$. Annahme:

$$l_R(R/aR) = s > r \implies \exists a_1, \dots, a_s \in R \setminus \{0\} : a_s \mid a_{s-1} \mid \cdots \mid a_1 \mid a_0 = 0$$

ohne Einschränkung $a_s = 1, a_i \nmid a_{i+1}$ für $i = 0, \dots, s-1$. $\implies \exists c_1, \dots, c_s \in R \setminus (R^* \cup \{0\})$ mit

$$a = c_1 a_1 = c_1 c_2 a_2 = \cdots = c_1 \cdot \dots \cdot c_{s-1} a_{s-1} = c_1 \cdot \dots \cdot c_s \cdot$$

zu $a = p_1 \cdot \dots \cdot p_r$, R faktoriell. □

Bemerkung 30.4 $c_1, \dots, c_r \in R \setminus (R^* \cup \{0\})$ mit $c_1 \mid c_2 \mid \cdots \mid c_r$. M R -Modul mit

$$M \cong \bigoplus_{i=1}^r R/c_i R$$

Dann gilt: r ist eindeutig bestimmt, c_1, \dots, c_r sind eindeutig bestimmt bis auf Assoziiertheit durch M .

Beweis Sei

$$M \cong \bigoplus_{i=1}^s R/(\alpha_i) \cong \bigoplus_{j=1}^t R/(\beta_j)$$

mit

$$\alpha_s \mid \alpha_{s-1} \mid \cdots \mid \alpha_1, \alpha_i \in R \setminus (R^* \cup \{0\})$$

$$\beta_t \mid \beta_{t-1} \mid \cdots \mid \beta_1, \beta_i \in R \setminus (R^* \cup \{0\})$$

1. Behauptung: Für alle $k \leq \min\{s, t\}$ ist $(\alpha_k) = (\beta_k)$, das heißt $\alpha_k \stackrel{\wedge}{=} \beta_k$, denn:

Annahme: Dies gilt nicht, ohne Einschränkung sei $k \leq \min\{s, t\}$ mit $(\alpha_k) \neq (\beta_k)$. \implies für $1 \leq i \leq k$ ist $(\alpha_i) = (\beta_i)$.

$$\implies \alpha_k M \cong \bigoplus_{i=1}^s \alpha_k R/(\alpha_i) = \bigoplus_{i=1}^{k-1} \alpha_k R/(\alpha_i)$$

denn für $i = k, \dots, s$ ist $\alpha_i \mid \alpha_k$ und somit $(\alpha_k) \subseteq (\alpha_i)$. Andererseits:

$$\begin{aligned} \alpha_k M &\cong \bigoplus_{j=1}^t \alpha_k R/(\beta_j) = \bigoplus_{j=1}^{k-1} \alpha_k R/(\beta_j) \oplus \bigoplus_{j=k}^t \alpha_k R/(\beta_j) \\ &= \bigoplus_{j=1}^{k-1} \alpha_k R/(\alpha_j) \oplus \bigoplus_{j=k}^t \alpha_k R/(\beta_j) \end{aligned}$$

Es ist

$$l_R(\alpha_k M) \leq l_R(M) = \sum_{i=1}^r l_R(R/c_i R) < \infty$$

\implies Längen aller auftretenden Moduln sind endlich. Es ist

$$l_R(\alpha_k M) = \sum_{i=1}^{k-1} l_R(\alpha_k R/(\alpha_i)) = \sum_{j=1}^{k-1} l_R(\alpha_k R/(\alpha_j)) + \sum_{j=k}^t l_R(\alpha_k R/(\beta_j))$$

$$\implies l_R(\alpha_k R/(\beta_j)) = 0, \quad j = k, \dots, t$$

$$\implies \alpha_k R/(\beta_j) = 0 \quad j = k, \dots, t$$

insbesondere $\alpha_k R/(\beta_k) = 0 \implies (\alpha_k) \subseteq (\beta_k)$ Durch Vertauschen der Rollen von α_i, β_i im obigen Beweis erhalten wir $(\beta_k) \subseteq (\alpha_k) \implies (\alpha_k) = (\beta_k)$

2. Nach 1. ist $(\alpha_i) = (\beta_i)$, das heißt $\alpha_i \stackrel{\wedge}{=} \beta_i \forall 1 \leq i \leq \min\{s, t\}$, ohne Einschränkung $s \leq t$. Annahme:
 $s < t$

$$\implies M \cong \bigoplus_{i=1}^s R/(\alpha_i) \oplus \bigoplus_{j=s+1}^t R/(\beta_j) \cong \bigoplus_{i=1}^s R/(\alpha_i)$$

$$\implies 0 = l_R\left(\bigoplus_{j=s+1}^t R/(\beta_j)\right) = \sum_{j=s+1}^t l_R(R/(\beta_j)) \implies R/(\beta_j) = 0 \quad j = s+1, \dots, t$$

$$\implies \beta_{s+1}, \dots, \beta_t \in R^* \text{. Also } s = t. \quad \square$$

Satz+Definition 30.5 (Elementarteilersatz) F endlich freier R -Modul, $M \subseteq R$ Untermodul. Dann existiert eine Basis (x_1, \dots, x_m) von F sowie $s \in \mathbb{N}_0, c_1, \dots, c_s \in R \setminus \{0\}$ mit folgenden Eigenschaften

1. $(c_1 x_1, \dots, c_s x_s)$ ist eine Basis von M .

2. $c_1 \mid c_2 \mid \dots \mid c_s$

s ist eindeutig, c_1, \dots, c_s sind eindeutig bis aus Assoziiertheit durch M bestimmt. (sind insbesondere unabhängig von der Wahl der Basis (x_1, \dots, x_m)) und heißen die **Elementarteiler** von $M \subseteq F$.

Beweis Existenz: Sei (y_1, \dots, y_m) eine Basis von F .

1. Behauptung: M ist endlich erzeugt, denn: Beweis per Induktion nach m

$m = 1$: dann existiert ein Isomorphismus $\varphi : F \rightarrow R, \varphi(M) \subseteq R$ ist ein Untermodul, insbesondere endlich erzeugt, da R Hauptidealring $\implies M$ endlich erzeugt.

$m > 1$: Wir setzen $F' := \text{Lin}((y_1, \dots, y_{m-1}))$, $F'' := \text{Lin}((y_m))$. Wir betrachten die Projektionsabbildung $\pi : F = F' \oplus F'' \rightarrow F'', a + b \mapsto b$ sowie $\pi|_M$. Es ist $\ker(\pi|_M) = \ker(\pi) \cap M = F' \cap M \subseteq F'$, $\text{im}(\pi|_M) = \pi(M) \subseteq F''$. Nach Induktionsvoraussetzung sind die Untermoduln $\ker(\pi|_M) \subseteq F'$, sowie $\text{im}(\pi|_M) \subseteq F''$ endlich erzeugt $\implies M$ endlich erzeugt.

2. Sei (z_1, \dots, z_n) ein endliches Erzeugendensystem von M . Wir betrachten den R -Modulhomomorphismus $\varphi : R^n \rightarrow F, e_j \mapsto z_j, j = 1, \dots, n$ mit e_1, \dots, e_n wie üblich. im $\varphi = \text{Lin}((z_1, \dots, z_n)) = M$. Setze

$$A := M_{(y_1, \dots, y_m)}^{(e_1, \dots, e_n)}(\varphi) = (\alpha_{ij}) \implies z_j = \sum_{i=1}^m \alpha_{ij} y_i \quad j = 1, \dots, n$$

nach 30.2 existieren S, T invertierbare Matrizen über $R, c_1, \dots, c_s \in R \setminus \{0\}$ mit

$$SAT^{-1} = \left(\begin{array}{ccc|c} c_1 & & & 0 \\ & \ddots & & \\ & & c_s & 0 \\ \hline & & & 0 \end{array} \right), \quad c_1 \mid \dots \mid c_s$$

\implies Es existieren Basen (x_1, \dots, x_m) von $F, (v_1, \dots, v_n)$ von R^n mit

$$M_{(x_1, \dots, x_m)}^{(v_1, \dots, v_n)}(\varphi) = \left(\begin{array}{ccc|c} c_1 & & & 0 \\ & \ddots & & \\ & & c_s & 0 \\ \hline & & & 0 \end{array} \right)$$

$\implies (c_1 x_1, \dots, c_s x_s)$ ist ein Erzeugendensystem von $\text{im } \varphi = M$.

3. (c_1x_1, \dots, c_sx_s) ist linear unabhängig, denn: Sei

$$\lambda_1c_1x_1 + \dots + \lambda_sc_sx_s = 0 \implies \lambda_1c_1 = \dots = \lambda_sc_s = 0$$

R nullteilerfrei $\implies \lambda_1 = \dots = \lambda_s = 0$. Somit: (c_1x_1, \dots, c_sx_s) ist eine Basis von M .

*Eindeutigkeitsaussage: Setze $T' := \text{Lin}((x_1, \dots, x_s))$

1. Behauptung: $F' = \{a \in F \mid \exists \lambda \in R \setminus \{0\} : \lambda a \in M\}$, insbesondere hängt F' nur von M ab, denn:
 „ \subseteq “ Sei $x \in \text{Lin}((x_1, \dots, x_s)) = F'$, etwa $x = \lambda_1x_1 + \dots + \lambda_sx_s$. $\implies c_sx = \lambda_1c_sx_1 + \dots + \lambda_sc_sx_s$.
 Wegen $c_1 \mid c_2 \mid \dots \mid c_s$ existiert $\mu_i \in R$ mit $c_s = \mu_i c_i, i = 1, \dots, s$.

$$\implies c_sx = \lambda_1\mu_1c_1x_1 + \dots + \lambda_s\mu_{s-1}c_{s-1}x_{s-1} + \lambda_sc_sx_s \in \text{Lin}((c_1x_1, \dots, c_sx_s)) = M$$

„ \supseteq “ Sei $a \in F$, etwa $a = \mu_1x_1 + \dots + \mu_mx_m$ und $\lambda \in R \setminus \{0\}$, sodass $\lambda a \in M$.

$$\implies \lambda a = \lambda\mu_1x_1 + \dots + \lambda\mu_mx_m \in M = \text{Lin}((c_1x_1, \dots, c_sx_s)) \subseteq \text{Lin}((x_1, \dots, x_s)) = F'$$

$$\implies \exists \delta_1, \dots, \delta_s \in R \text{ mit}$$

$$\lambda a = \delta_1x_1 + \dots + \delta_sx_s$$

$$\implies 0 = (\lambda\mu_1 - \delta_1)x_1 + \dots + (\lambda\mu_s - \delta_s)x_s + \lambda\mu_{s+1}x_{s+1} + \dots + \lambda\mu_mx_m$$

$$\implies \lambda\mu_{s+1} = \dots = \lambda\mu_m = 0 \implies \mu_{s+1} = \dots = \mu_m = 0 \implies a = \mu_1x_1 + \dots + \mu_sx_s \in F'$$

2. Wir betrachten die Abbildung

$$\psi : F' = \text{Lin}((x_1, \dots, x_s)) \rightarrow \bigoplus_{i=1}^s R/c_iR, \alpha_1x_1 + \dots + \alpha_sx_s \mapsto (\alpha_1 + c_1R, \dots, \alpha_s + c_sR)$$

ψ ist ein wohldefinierter Homomorphismus, ψ ist surjektiv.

$$\ker \psi = \{\alpha_1x_1 + \dots + \alpha_sx_s \in F' \mid c_1 \mid \alpha_1, \dots, c_s \mid \alpha_s\} \text{Lin}((c_1x_1, \dots, c_sx_s)) = M$$

\implies Erhalten Isomorphismus

$$\bar{\psi} : F'/M \rightarrow \bigoplus_{i=1}^s R/c_iR$$

von R -Moduln, die linke Seite ist wegen 1. nur von M abhängig. Ist $c_1 \in R^*$, dann ist $c_1R = R$, also $R/c_1R = 0$. Wegen 30.4 sind damit die Nichteinheiten unter c_1, \dots, c_s eindeutig bestimmt bis auf Assoziiertheit, ihre Anzahl ist eindeutig bestimmt. Da (c_1x_1, \dots, c_sx_s) Basis von M , ist $s = \text{Rang}(M)$ eindeutig bestimmt. \implies Anzahl der Einheiten unter c_1, \dots, c_s eindeutig bestimmt, Einheiten unter c_1, \dots, c_s sind eindeutig bis auf Assoziiertheit. \square

Folgerung 30.6 F endlich freier R -Modul, $M \subseteq F$ Untermodul. Dann ist M endlich frei und $\text{Rang}(M) \leq \text{Rang}(F)$.

Anmerkung • Aus $M \subsetneq F$ folgt nicht $\text{Rang}(M) < \text{Rang}(F)$: zum Beispiel ist \mathbb{Z} ein freier \mathbb{Z} -Modul vom Rang 1, $2\mathbb{Z} \subsetneq \mathbb{Z}$ ist ein freier \mathbb{Z} -Modul, aber $\text{Rang}(2\mathbb{Z}) = 1 = \text{Rang}(\mathbb{Z})$.

- Man kann zeigen (unter Verwendung des Auswahlaxiom): F freier R -Modul, $M \subseteq F$ Untermodul $\implies M$ frei (R Hauptidealring!)
- ohne die Voraussetzung, dass R ein Hauptidealring ist, wird 30.6 falsch: Beispiel: $F = \mathbb{Q}[X, Y]$ als $F = \mathbb{Q}[X, Y]$ -Modul (R ist kein Hauptidealring!), $M = \text{Lin}((X, Y))$ ist **nicht** frei als R -Modul.

Satz+Definition 30.7 (Hauptsatz für endlich erzeugte Moduln über Hauptidealringen, Variante 1) M endlich erzeugt. Dann gilt:

1. Es gibt einen endlich freien Untermodul $F \subseteq M$, etwa $F \cong R^d$ mit $M = F \oplus T(M)$. Hierbei ist $d = \text{Rang } F$ eindeutig bestimmt.
2. Es gibt $s \in \mathbb{N}_0$, $c_1, \dots, c_s \in R \setminus (R^* \cup \{0\})$ mit

$$T(M) \cong \bigoplus_{j=1}^s R/c_j R$$

mit $c_1 \mid c_2 \mid \dots \mid c_s$

3. Die Zahl s ist eindeutig bestimmt, c_1, \dots, c_s sind eindeutig bestimmt bis auf Assoziiertheit und heißen die **Elementarteiler** von M .

Also:

$$M \cong R^d \oplus R/c_1 R \oplus \dots \oplus R/c_s R$$

Beweis 1. Existenz: Setze (z_1, \dots, z_m) ein endliches Erzeugendensystem von M . Wir betrachten den R -Modulhomomorphismus

$$\varphi : R^m \rightarrow M, e_i \mapsto z_i, i = 1, \dots, m$$

φ ist surjektiv \implies

$$M \cong R^m / \ker \varphi$$

Nach Elementarteiler-Satz für $\ker \varphi \subseteq R^m$ existiert eine Basis (x_1, \dots, x_m) von R^m , sowie $c_1, \dots, c_t \in R \setminus \{0\}$, sodass $(c_1 x_1, \dots, c_t x_t)$ eine Basis von $\ker \varphi$ ist. Setze $c_{t+1} = \dots = c_m := 0$, außerdem

$$\rho : R^m \rightarrow R/(c_1) \oplus \dots \oplus R/(c_m), \alpha_1 x_1 + \dots + \alpha_m x_m \mapsto (\alpha_1 + (c_1), \dots, \alpha_m + (c_m))$$

$\implies \rho$ ist wohldefinierter R -Modulhomomorphismus, ρ ist surjektiv mit $\ker \rho = \text{Lin}((c_1 x_1, \dots, c_t x_t)) = \ker \varphi$.

$$\implies M \cong R^m / \ker \varphi = R^m / \ker \rho \cong R/(c_1) \oplus \dots \oplus R/(c_m) \cong R/(c_1) \oplus R/(c_t) \oplus R^{m-t}$$

Setze $d := m - t$. Für $c_i \in R^*$ ist $c_i R = R$, also $R/(c_i) = 0$. Nach Weglassen der Einheiten aus c_1, \dots, c_t und Umordnen zu $c_1, \dots, c_s \in R \setminus (R^* \cup \{0\})$ mit $c_1 \mid \dots \mid c_s$ ist

$$M \cong R^d \oplus R/(c_1) \oplus \dots \oplus R/(c_s)$$

2. Eindeutigkeit: Wir betrachten die Abbildung:

$$\delta : M \xrightarrow[\gamma]{\cong} R^d \oplus R/(c_1) \oplus \dots \oplus R/(c_s) \xrightarrow[\text{kan. Proj.}]{\pi} R^d$$

σ ist surjektiver R -Modulhomomorphismus mit

$$\begin{aligned} \ker(\delta) &= \gamma^{-1}(\ker \pi) = \gamma^{-1}\left(R/(c_1) \oplus \dots \oplus R/(c_s)\right) \gamma^{-1}\left(T\left(R/(c_1) \oplus \dots \oplus R/(c_s) \oplus R^d\right)\right) \\ &= T(M) \end{aligned}$$

Homomorphiesatz: $M/T(M) \cong R^d \implies d$ eindeutig bestimmt. Wegen $T(M) \cong R/(c_1) \oplus \dots \oplus R/(c_s)$ sind nach 30.4 auch s eindeutig bestimmt sowie c_1, \dots, c_s eindeutig bis auf Assoziiertheit.

3. Existenz (Teil 2): Es ist

$$M = \gamma^{-1}\left(R^d \oplus R/(c_1) \oplus \dots \oplus R/(c_s)\right) = \underbrace{\gamma^{-1}(R^d)}_{=: F} \oplus \underbrace{\gamma^{-1}\left(R/(c_1) \oplus \dots \oplus R/(c_s)\right)}_{=: T(M)} \quad \square$$

Anmerkung Ohne Voraussetzung „ M endlich erzeugt“ wird die Aussage falsch: \mathbb{Q} ist ein (nicht endlich erzeugter) \mathbb{Z} -Modul mit $T(\mathbb{Q}) = \{0\}$, aber \mathbb{Q} ist kein freier \mathbb{Z} -Modul (vergleiche Annahme nach 29.17)

Folgerung 30.8 M R -Modul. Dann sind äquivalent:

1. M ist endlich erzeugt und frei
2. M ist endlich frei

Beweis 2. \implies 1. trivial

1. \implies 2. Nach Hauptsatz existiert endlich freier Untermodul $F \subseteq M$ mit $M = F \oplus T(M)$. Wegen 29.17 ist $T(M) = \{0\}$, also $M = F \implies M$ endlich frei. \square

Folgerung 30.9 (Hauptsatz über endlich erzeugte abelsche Gruppen, Variante 1) G endlich erzeugte abelsche Gruppe (= endlich erzeugter \mathbb{Z} -Modul). Dann existiert ein Isomorphismus

$$G \cong \mathbb{Z}^d \oplus \mathbb{Z}/c_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/c_s\mathbb{Z}$$

mit $d \in \mathbb{N}_0, c_1, \dots, c_s \in \mathbb{N}_{>1}, c_1 \mid \dots \mid c_s, d$ sowie s, c_1, \dots, c_s sind eindeutig bestimmt. Es ist G endlich $\iff d = 0$. In diesem Fall ist $|G| = c_1 \cdot \dots \cdot c_s$

Beispiel 30.10

1. abelsche Gruppen mit 4 Elementen bis auf Isomorphie:

a) Fall: $s = 1, c_1 = 4 : \mathbb{Z}/4\mathbb{Z}$

b) Fall: $s = 2, c_1 = 2, c_2 = 2 : \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

\implies bis auf Isomorphie gibt es 2 abelsche Gruppen mit 4 Elementen.

2. abelsche Gruppen mit 24 Elementen bis auf Isomorphie

a) Fall: $s = 1, c_1 = 24 : \mathbb{Z}/24\mathbb{Z}$

b) Fall: $s = 2, c_1 = 2, c_2 = 12 : \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$

c) Fall: $s = 3, c_1 = 2, c_2 = 2, c_3 = 6 : \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$

\implies Bis auf Isomorphie gibt es 3 abelsche Gruppen mit 24 Elementen.

Frage: $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ ist ebenfalls eine abelsche Gruppe mit 24 Elementen. Zu welcher der Gruppen aus der Liste von 30.16.b ist diese isomorph?

Bemerkung 30.11 (Spezialfall des Chinesischen Restsatzes) $a \in R \setminus (R^* \cup \{0\}), a = cp_1^{n_1} \cdot \dots \cdot p_r^{n_r}$ mit $c \in R^*, p_1, \dots, p_r$ irreduzibel, paarweise nicht-assoziiert.

$$\pi_i : R \rightarrow R/(p_i^{n_i}), b \mapsto b + (p_i^{n_i})$$

kanonische Projektion für $i = 1, \dots, r$. Dann ist die Abbildung

$$\varphi : R \rightarrow R/(p_1^{n_1}) \times \dots \times R/(p_r^{n_r}), b \mapsto (\pi_1(b), \dots, \pi_r(b))$$

ein surjektiver Ringhomomorphismus mit $\ker \varphi = (a)$, das heißt wir erhalten einen Ringisomorphismus

$$\Phi : R/(a) \xrightarrow{\cong} R/(p_1^{n_1}) \times \dots \times R/(p_r^{n_r})$$

Hierbei ist $R/(p_1^{n_1}) \times \dots \times R/(p_r^{n_r})$ via komponentenweiser Addition und Multiplikation ein Ring. Insbesondere erhalten wir einen Isomorphismus von R -Moduln

$$R/(a) \cong R/(p_1^{n_1}) \times \dots \times R/(p_r^{n_r})$$

Beweis 1. φ Ringhomomorphismus, da π_1, \dots, π_r Ringhomomorphismus

2. φ surjektiv: Es ist $1 \in \text{GGT}(p_j^{n_j}, p_i^{n_i} \cdot \dots \cdot p_{j_1}^{n_{j_1}-1} p_{j+1}^{n_{j+1}} \cdot \dots \cdot p_r^{n_r})$.

$$\implies \exists u_j, v_j \in R : 1 = \underbrace{u_j p_j^{n_j}}_{=: d_j} + \underbrace{v_j p_i^{n_i} \cdot \dots \cdot p_{j_1}^{n_{j_1}-1} p_{j+1}^{n_{j+1}} \cdot \dots \cdot p_r^{n_r}}_{e_j}$$

$$\implies \pi_i(e_j) = \bar{0} \text{ für } i \neq j, \pi_j(e_j) = \pi_j(1 - d_j) = \pi_j(1) - \pi_j(d_j) = \bar{1} - \bar{0} = \bar{1}$$

$$\implies \varphi(e_j) = (\bar{0}, \dots, \bar{0}, \bar{1}, \bar{0}, \dots, \bar{0})$$

Für $(\bar{a}_1, \dots, \bar{a}_r) \in R/(p_1^{n_1}) \times \dots \times R/p_r^{n_r}$ ist

$$\varphi(a_1 e_1 + \dots + a_r e_r) = \underbrace{\varphi(a_1) \varphi(e_1)}_{(\bar{a}_1, \bar{0}, \dots, \bar{0})} + \dots + \underbrace{\varphi(a_r) \varphi(e_r)}_{=(\bar{0}, \dots, \bar{0}, \bar{a}_r)} = (\bar{a}_1, \dots, \bar{a}_r)$$

3.

$$\ker \varphi = \{a \in R \mid p_1^{n_1} \mid a, \dots, p_r^{n_r} \mid a\} = \{a \in R \mid p_1^{n_1} \cdot \dots \cdot p_r^{n_r} \mid a\} = (p_1^{n_1} \cdot \dots \cdot p_r^{n_r}) = (pp_1^{n_1} \cdot \dots \cdot p_r^{n_r}) = (a)$$

4. Rest aus Homomorphiesatz für Ringe □

Beispiel 30.12

Nach 30.11 ist $\mathbb{Z}/24\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$

Satz 30.13 (Hauptsatz für endlich erzeugte Moduln über Hauptidealringen, Variante 2) M endlich erzeugter R -Modul, \mathbb{P} sei ein Vertretersystem der Primelemente von R bis auf Assoziiertheit, für $p \in \mathbb{P}$ sei

$$M_p := \{x \in M \mid \exists n \in \mathbb{N} : p^n x = 0\} \subseteq T(M)$$

(ist offenbar ein Untermodul). Dann gilt:

1. Es gibt einen endlich erzeugten freien Untermodul $F \subseteq M$, sodass $M = F \oplus T(M)$, $d := \text{Rang } F$ ist eindeutig bestimmt.
2. $T(M) = \bigoplus_{p \in \mathbb{P}} M_p$, wobei $M_p = 0$ für fast alle $p \in \mathbb{P}$
3. Für jedes $p \in \mathbb{P}$ mit $M_p \neq 0$ gibt es eindeutig bestimmte natürliche Zahlen $1 \leq n_{p,1} \leq \dots \leq n_{p,s_p}$ mit

$$M \cong R^d \oplus \bigoplus_{p \in \mathbb{P}} \left(R/p^{n_{p,1}} R \oplus \dots \oplus R/p^{n_{p,s_p}} R \right)$$

Beweis 1. folgt aus 30.10

2., 3.:

1. Nach Hauptsatz für endlich erzeugte R -Moduln (Variante 1) ist $M = F \oplus T(M)$, $T(M) \cong R/(c_1) \oplus \dots \oplus R/(c_s)$ mit $c_1, \dots, c_s \in R \setminus (R^* \cup \{0\})$, $c_1 \mid \dots \mid c_s$. Wir faktorisieren c_1, \dots, c_s in R : $\{p_1, \dots, p_r\} \subseteq \mathbb{P}$ sei die Menge der Primteiler von c_s (bis auf Assoziiertheit). Sei $c_j = \varepsilon_j p_1^{n_{1,j}} \cdot \dots \cdot p_r^{n_{r,j}}$, $\varepsilon_j \in R^*$, $n_{1,j}, \dots, n_{r,j} \in \mathbb{N}_0$ ($j = 1, \dots, r$).

$$\implies T(M) \cong \bigoplus_{j=1}^s R/(c_j) \cong \bigoplus_{j=1}^s \bigoplus_{i=1}^r R/p_i^{n_{i,j}} \cong \bigoplus_{i=1}^r \bigoplus_{j=1}^s R/p_i^{n_{i,j}}$$

2. Es sei ein Isomorphismus $\gamma : T(M) \rightarrow \bigoplus_{i=1}^r \bigoplus_{j=1}^s R/(p_i^{n_{i,j}})$ fixiert. Behauptung:

$$\gamma(M_{p_i}) = \bigoplus_{j=1}^s R/(p_i^{n_{i,j}})$$

denn: „ \subseteq “ Sei $a \in M_{p_i}$, etwa $p_i^m a = 0 \implies \gamma(p_i^m a) = 0 \implies p_i^m \gamma(a) = 0$. Es ist $\gamma(a)$ von der Form

$$\gamma(a) = \begin{pmatrix} \bar{x}_{1,1}, \dots, \bar{x}_{1,s}, \dots, \bar{x}_{r,1}, \dots, \bar{x}_{r,s} \\ \downarrow \quad \quad \downarrow \quad \quad \downarrow \quad \quad \downarrow \\ R/(p_i^{n_{1,1}}) \quad R/(p_i^{n_{1,s}}) \quad R/(p_i^{n_{r,1}}) \quad R/(p_i^{n_{r,s}}) \end{pmatrix}$$

Für $j \neq i$ ist $1 \in \text{GGT}(p_i^m, p_j^{n_{j,k}}), k \in \{1, \dots, r\} \implies \exists u_1, v_i \in R : 1 = u_i p_i^m + v_i p_j^{n_{j,k}}$. In $R/(p_j^{n_{j,k}})$ ist $\bar{1} = \bar{u}_i \bar{p}_i^m$, das heißt \bar{p}_i^m ist Einheit in $R/(p_j^{n_{j,k}})$. Aus $p_i^m \gamma(a) = 0$ folgt für $j \neq i, k = 1, \dots, s : p_i^m \bar{x}_{j,k} = 0 \implies \bar{p}_i^m \bar{x}_{j,k} = 0 \implies \bar{x}_{j,k} = 0$

$$\implies \gamma(a) \in \bigoplus_{j=1}^s R/(p_i^{n_{i,j}})$$

„ \supseteq “ Sei $x \in \bigoplus_{j=1}^s R/(p_i^{n_{i,j}})$. Setze $m := \max\{n_{i,1}, \dots, n_{i,s}\} = n_{i,s}$, dann $p_i^m x = 0$. Setze $y := \gamma^{-1}(x)$. Dann ist $p_i^m y = p_i^m y^{-1}(x) = \gamma^{-1}(p_i^m x) = 0 \implies y \in M_{p_i}$ und $\gamma(y) = x$, das heißt $x \in \gamma(M_{p_i})$.

3. Aus 2. folgt:

$$T(M) = \gamma^{-1}\left(\bigoplus_{i=1}^r \bigoplus_{j=1}^s R/(p_i^{n_{i,j}})\right) = \gamma^{-1}(\bigoplus_{i=1}^r \gamma(M_{p_i})) = \bigoplus_{i=1}^r M_{p_i}$$

Behauptung: $M_p = 0$ für $p \neq p_1, \dots, p_r$, denn: Sei $p \neq p_1, \dots, p_r \implies 1 \in \text{GGT}(p^m, c_j)$ für $j = 1, \dots, s, m \in \mathbb{N} \implies p^m + (c_j) \in (R/(c_j))^*$ für $j = 1, \dots, s$

\implies Aus $p^m x = 0$ für $x \in \bigoplus_{j=1}^s R/(c_j)$ folgt $x = 0$

\implies Aus $p^m x = 0$ für $x \in T(M)$ folgt $x = 0$

\implies Aus $p^m x = 0$ für $x \in M$ folgt $x = 0$

$\implies M_p = 0$ für $p \neq p_1, \dots, p_r, p \in \mathbb{P} \implies M_p = 0$ für fast alle $p \in \mathbb{P}$ und $T(M) = \bigoplus_{p \in \mathbb{P}} M_p$

4. Nach Umbenennung erhalten wir

$$M_p \cong \bigoplus_{j=1}^{s_p} R/(p^{n_{p,j}})$$

mit $1 \leq n_{p,1} \leq \dots \leq n_{p,s_p}$, falls $s_p \neq 0$. M_p mit $p \neq 0$ hängt nur von M, p b. Die Zahlen $n_{p,1}, \dots, n_{p,s_p}$ sind wegen 30.4 eindeutig bestimmt. \square

Folgerung 30.14 (Hauptsatz für endlicherzeugte abelsche Gruppen, Variante 2) G endlich erzeugte Gruppe, \mathbb{P} Menge der Primzahlen in \mathbb{N} . Dann existiert ein Isomorphismus

$$G \cong \mathbb{Z}^d \oplus \bigoplus_{p \in \mathbb{P}} \left(\mathbb{Z}/(p^{n_{p,1}}) \oplus \dots \oplus \mathbb{Z}/(p^{n_{p,s_p}}) \right), 1 \leq n_{p,1} \leq \dots \leq n_{p,s_p}$$

Die Zahlen $d, s_p, n_{p,i}$ sind eindeutig bestimmt. Es ist $s_p = 0$ für fast alle $p \in \mathbb{P}$. Es ist G endlich $\iff d = 0$. In diesem Fall ist $|G| = \prod_{p \in \mathbb{P}} p^{n_{p,1} + \dots + n_{p,s_p}}$.

Beispiel 30.15

Endliche abelsche Gruppen mit 24 Elementen, bis auf Isomorphie: Es ist $24 = 2^3 \cdot 3 = 2 \cdot 2^2 \cdot 3 = 2 \cdot 2 \cdot 2 \cdot 3$
 \implies Isomorphietypen:

$$\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$$

Es ist

$$\begin{aligned} \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} &\cong \mathbb{Z}/24\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} &\cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z} \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} &\cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \end{aligned}$$