Lineare Algebra 2

UNI HEIDELBERG

Mit Liebe gemacht von:
NIKOLAUS SCHÄFER

Inhaltsverzeichnis

1. Eigenwerte

In diesem Abschnitt sei $n \in \mathbb{N}$, V ein K-VR und $\varphi \in End_K(V)$
Frage: V endlich dimensional, existiert eine Basis $B = (v_1, \dots, v_n)$ von V, sodass $M_B(\varphi)$ eine Diagonalmatrix ist, d.h. $M_B(\varphi) = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$ mit $\lambda_1, \dots, \lambda_n \in K$? Für $i = 1, \dots, n$ wäre dann $\varphi(v_i) = \lambda_i v_i$.

Definition 1.1. $\lambda \in K, v \in V$
λ heißt Eigenwert von $\varphi \Leftrightarrow$ Es existiert ein $v \in V, v \neq 0$ mit $\varphi(v) = \lambda v$
v heißt Eigenvektor zum Eigenwert $\lambda \Leftrightarrow v \neq 0$ und $\varphi(v) = \lambda v$
φ heißt diagonalisierbar $\Leftrightarrow V$ besitzt eine Basis aus EV von φ
(Falls V endlichdimensional, ist dies äquivalent zu: Es gibt eine Basis B von V und $\lambda_1, \dots, \lambda_n \in K$ mit $M_B(\varphi) = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$ Eigenwerte/Eigenvektoren/Diagonalisierbarkeit einer Matrix $A \in M(n \times n, K)$ sind über den Endomorphismus $\tilde{A} : K^n \to K^n$ definiert.

Bemerkung 1.2. $A \in M(n \times n, K)$. Dann sind äquivalent:
(i) A ist diagonalisierbar.
(ii) Es gibt eine Basis von K^n aus Eigenvektoren von A
(iii) Es gibt ein $S \in GL(n, K)$, $\lambda_1, \dots, \lambda_n \in K$ mit $SAS^{-1} = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$
(iv) 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).

Beispiel 1.3. $K = \mathbb{R}, V = \mathbb{R}^2$
(a) $\varphi : \mathbb{R}^2 \to \mathbb{R}^2, \binom{x_1}{x_2} \mapsto \binom{x_2}{x_1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$
Es ist $\varphi(\binom{1}{1}) = \binom{1}{1} = 1 \cdot \binom{1}{1}$, d.h. $\binom{1}{1}$ ist EV von φ zum EW 1.
$\varphi(\binom{1}{-1}) = \binom{-1}{1} = -1 \cdot \binom{1}{-1}$, d.h. $\binom{1}{-1}$ ist EV von φ zum EW -1.
Somit: $(\binom{1}{1}, \binom{1}{-1})$ ist eine Basis des $\mathbb{R}^2$ aus EV von φ, d.h. φ ist diagnoalisierbar.
In Termen von Matrizen: $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in M(2 \times 2, \mathbb{R})$ ist diagonalisierbar, und mit $S = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{-1}$ ist dann $SAS^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Achtung: Das φ diagonalisierbar ist, heißt nicht, dass jeder Vektor aus $V = \mathbb{R}^2, v \neq 0$ ein EV von φ ist, z.B. ist $\varphi(\binom{1}{2}) = \binom{2}{1} \neq \lambda \binom{1}{2}$ für alle $\lambda \in \mathbb{R}$.
(b) $\varphi : \mathbb{R}^2 \to \mathbb{R}^2, \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} -x_2 \\ x_1 \end{pmatrix}$ (=Drehung um $\pi/2$) hat keinen EW. Beweis dafür später.

Ziel: Suche Kriterium für Diagonalisierbarkeit

Bemerkung 1.4. $v_1, \dots, v_m$ 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.

Folgerung 1.5. V endlichdimensional, φ habe n paarweise verschiedene EW, wobei $n = \dim V$
Dann ist φ diagonalisierbar.

Definition 1.6. $\lambda \in K$
$Eig(\varphi, \lambda) := \{v \in V | \varphi(v) = \lambda v\}$ heißt Eigenraum von φ bzgl. λ
$\mu_{geo}(\varphi, \lambda) := \dim Eig(\varphi, \lambda)$ heißt die geometrische Vielfachheit von λ
Für $A \in M(n \times n, K)$ setzen wir $Eig(A, \lambda) := Eig(\tilde{A}, \lambda)$, $\mu_{geo}(A, \lambda) := \mu_{geo}(\tilde{A}, \lambda)$.

Bemerkung 1.7. $\lambda \in K$. Dann gilt:
(a) $Eig(\varphi, \lambda)$ ist ein UVR von V.
(b) λ ist EW von $\varphi \Leftrightarrow Eig(\varphi, \lambda) \neq \{0\}$
(c) $Eig(\varphi, \lambda) \setminus \{0\}$ ist die Menge der zu λ gehörenden EV von φ.
(d) $Eig(\varphi, \lambda) = \ker(\lambda id_V - \varphi)$, insbesondere ist $Eig(A, \lambda) = \ker(\lambda E_n - A) = \text{Lös}(\lambda E_n - A, 0)$ für $A \in M(n \times n, K)$
(e) Sind $\lambda_1, \lambda_2 \in K$ mit $\lambda_1 \neq \lambda_2$, dann $Eig(\varphi, \lambda_1) \cap Eig(\varphi, \lambda_2) = \{0\}$

Bemerkung 1.8. V endlichdimensional, $\lambda \in K$. Dann sind äquivalent:
(i) λ ist EW von φ
(ii) $\det(\lambda id_V - \varphi) = 0$

Definition 1.9. K Körper, $A = (a_{ij}) \in M(n \times n, K)$

$$\chi_A^{char} := \det(tE_n - A) = \det \begin{pmatrix} t - a_{11} & -a_{12} & \dots & -a_{1n} \\ -a21 & t - a_{22} & & \vdots \\ \vdots & & \ddots & \vdots \\ -a_{nn} & \dots & \dots & t - a_{nn} \end{pmatrix} \in K[t]$$

heißt das charakteristische Polynom von A.

Anmerkung: Hierfür nötig: Determinante von Matrizen mit Einträgen in einem kommutativen Ring (Anmerkung in LA 1).

Beispiel 1.10. $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in M(2 \times 2, \mathbb{R}) \Rightarrow \chi_A^{char} = \det \begin{pmatrix} t-1 & -2 \\ -3 & t-4 \end{pmatrix} = (t-1)(t-4) - 6 = t^2 - 5t - 2$

Bemerkung 1.11. $A, B \in M(n \times n, K), A \approx B$
Dann ist $\chi_A^{char} = \chi_B^{char}$.

Definition 1.12. V endlichdimensional, $n = \dim V, B$ Basis von V, $\varphi \in End(V), A = M_B(\varphi)$
$\chi_\varphi^{char} := \chi_A^{char} = \det(tE_n - A) \in K[t]$ heißt das charakteristische Polynom von φ.

Anmerkung: χ_φ^{char} ist wohldefiniert, denn: Ist B' eine weitere Basis von V, $A' = M_{B'}(\varphi)$, dann ist $A \approx A'$ und deshalb nach Bem. 1.11: $\chi_A^{char} = \chi_{A'}^{char}$.

Satz 1.13. V endlichdimensional, $n = \dim V$. Dann gilt:
(a) χ_φ^{char} ist ein normiertes Polynom vom Grad n: $\chi_\varphi^{char} = t^n + c_{n-1}t^{n-1} + \ldots + c_0$ mit $c_0 = (-1)^n \det \varphi$, $c_{n-1} = -sp(\varphi)$ (vgl. Ü zur Spur)
(b) Die Nullstellen von χ_φ^{char} sind genau die EW von φ: $\lambda \in K$ ist EW von $\varphi \Leftrightarrow \chi_A^{char}(\lambda) = 0$

Definition 1.14. $\lambda \in K$
$\mu_{alg}(\varphi, \lambda) := \mu(\chi_\varphi^{char}, \lambda)$ heißt die algebraische Vielfachheit von λ.

Beispiel 1.15. (vgl. Bsp. 1.3)
(a) $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$, $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}_{=:A} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$.

Es ist $\chi_\varphi^{char} = \chi_A^{char} = \det \begin{pmatrix} t & -1 \\ -1 & t \end{pmatrix} = t^2 - 1 = (t-1)(t+1) \in \mathbb{R}[t] \Rightarrow$ EW von $\varphi : 1, -1$
Es ist $\mu_{alg}(\varphi, 1) = 1, \mu_{alg}(\varphi, -1) = 1$
$Eig(\varphi, 1) = Eig(A, 1) = \text{Lös}(E_2 - A, 0) = \text{Lös}(\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}, 0) = Lin(\binom{1}{-1})$, also $\mu_{geo}(\varphi, 1) = \dim Eig(\varphi, 1) = 1$.
$Eig(\varphi, -1) = 1$ (analog)
(b) $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$, $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{=:A} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$.

Es ist $\chi_\varphi^{char} = \chi_A^{char} = \det \begin{pmatrix} t & 1 \\ -1 & t \end{pmatrix} = t^2 + 1$, χ_φ^{char} hat keine NS in $\mathbb{R} \Rightarrow \varphi$ hat keine Eigenwerte.
(c) $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$, $\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \underbrace{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}}_{=:A} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$.

Es ist $\chi_\varphi^{char} = \chi_A^{char} = \det \begin{pmatrix} t-1 & -1 \\ 0 & t-1 \end{pmatrix} = (t-1)^2 \Rightarrow 1$ ist einziger EW von φ, es ist $\mu_{alg}(\varphi, 1) = 2$
$Eig(\varphi, 1) = Eig(A, 1) = \text{Lös}(1 \cdot E_2 - A, 0) = \text{Lös}(\begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}, 0) = Lin(\binom{1}{0}) \Rightarrow \mu_{geo}(\varphi, 1) = 1. \Rightarrow \varphi$ ist nicht diagonalisierbar.

Satz 1.16. V endlichdimensional, $n = \dim V$
(a) Ist φ diagonalisierbar, dann ist $\chi_\varphi^{char} = (t - \lambda_1) \cdot \ldots \cdot (t - \lambda_n)$ mit $\lambda_1, \ldots, \lambda_n \in K$, nicht notwendig verschieden, d.h. χ_φ^{char} zerfällt in Linearfaktoren.
(b) Ist $\chi_\varphi^{char} = (t - \lambda_1) \cdot \ldots \cdot (t - \lambda_n)$ mit paarweise verschiedenen $\lambda_1, \ldots, \lambda_n \in K$, dann ist φ diagonalisierbar.

Bemerkung 1.17. V endlichdimensional, $n = \dim V$, λ EW von φ. Dann gilt:
$1 \leq \mu_{geo}(\varphi, \lambda) \leq \mu_{alg}(\varphi, \lambda)$

Bemerkung 1.18. $\lambda_1, \ldots, \lambda_n$ paarweise verschiedene EW von φ
Dann gilt: $Eig(\varphi, \lambda_i) \cap \sum_{j=1, j \neq i}^{r} Eig(\varphi, \lambda_j) = \{0\}$ für alle $i \in \{1, \ldots, r\}$

Satz 1.19. V endlichdimensional. Dann sind äquivalent:
(i) φ diagonalisierbar
(ii) χ_φ^{char} zerfällt in Linearfaktoren und $\mu_{alg}(\varphi, \lambda) = \mu_{geo}(\varphi, \lambda)$ für alle EW λ von φ.
(iii) Sind $\lambda_1, \ldots, \lambda_k$ die paarweise verschiedene EW von φ, dann ist $V = Eig(\varphi, \lambda_1) \oplus \ldots \oplus Eig(\varphi, \lambda_k)$
In diesem Fall erhält man eine Basis von V aus EV von φ, indem man Basen von $Eig(\varphi, \lambda_i), i = 1, \ldots, k$, zusammenfügt.

Anmerkung: In der Praxis ist es in der Regel schwierig festzustellen, ob χ_φ^{char} in Linearfaktoren zerfällt oder die NS von χ_φ^{char} zu bestimmen. Für Polynome vom Grad ≥ 5 existiert keine Lösungsformel zur Bestimmung der Nullstellen, die Nullstellen müssen numerisch bestimmt werden.

Beispiel 1.20. (a) In 1.15(c) ist $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in M(2\times 2,\mathbb{R}), \chi_A^{char} = (t-1)^2, \mu_{geo}(A,1) = 1 < \underbrace{\mu_{alg}(A;1)}_{=2}$

$\Rightarrow A$ nicht diagonalisierbar.

(b) $A = \begin{pmatrix} 2 & -1 & -1 \\ -6 & 1 & 2 \\ 3 & -1 & -2 \end{pmatrix} \in M(3\times 3,\mathbb{R}) \Rightarrow \chi_A^{char} = det\begin{pmatrix} t-2 & 1 & 1 \\ 6 & t-1 & -2 \\ -3 & 1 & t+2 \end{pmatrix} = t^3 - t^2 - 5*t - 3$

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

$Eig(A,-1) = \text{Lös}(-E_n - A, 0) = \text{Lös}(\begin{pmatrix} -3 & 1 & 1 \\ 6 & -2 & -2 \\ -3 & 1 & 1 \end{pmatrix}, 0) = Lin(\begin{pmatrix} -1 \\ 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \\ 3 \end{pmatrix}) \Rightarrow \mu_{geo}(A,-1) = 2 = \mu_{alg}(A,-1).$

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

$\Rightarrow$ A ist diagonalisierbar, $B := (\begin{pmatrix} -1 \\ 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix})$ ist eine Basis des $\mathbb{R}^3$ aus EV von A, $M_B(\tilde{A}) = \begin{pmatrix} -1 & & 0 \\ & -1 & \\ 0 & & 3 \end{pmatrix}$

Mit $S := \begin{pmatrix} -1 & 0 & 1 \\ 3 & -1 & -2 \\ 0 & 3 & 1 \end{pmatrix}^{-1}$ ist $SAS^{-1} = \begin{pmatrix} -1 & & 0 \\ & -1 & \\ 0 & & 3 \end{pmatrix}$

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

- Endomorphismen $\varphi \in End_K(V)$ einsetzen durch die Regel $f(\varphi) := a_m\varphi^m + \ldots + a_1\varphi + a_0 id_V \in End_K(V)$, wobei $\varphi^k := \underbrace{\varphi \circ \ldots \circ \varphi}_{\text{k- mal}}$
- Matrizen $A \in M(n\times n,K)$ einsetzen durch die Regel $f(A) := a_m A^m + \ldots + a_1 A + a_0 E_n \in M(n\times n,K)$

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

Satz 1.21. (Satz von Cayley-Hamilton)
V endlichdimensional, dann gilt: $\chi_\varphi^{char}(\varphi) = 0$
Insbesondere gilt für alle $A \in M(n\times n,K) : \chi_A^{char}(A) = 0$

Anmerkung: Der "Beweis" $\chi_A(A) = (\det(tE_n - A))(A) = \det(AE_n - A) = \det(A-A) = \det(0) = 0$ funktioniert nicht, denn $\underbrace{(\underbrace{\det(tE_n - A}_{\in K[t])})(A)}_{\in M(n\times n,K)}$ "$\neq$" $\underbrace{\det(\underbrace{AE_n - A}_{\in M(n\times n,K)})}_{\in K}$

Satz 1.22. V endlichdimensional, $I := \{f \in K[t] | f(\varphi) = 0\}$
Dann gilt:
(a) Es gibt ein eindeutig bestimmtes normiertes Polynom $\chi_\varphi^{min} \in K[t]$, sodass $I = \chi_\varphi^{min} K[t] := \{\chi_\varphi^{min} q | q \in K[t]\}$
χ_φ^{min} heißt das Minimalpolynom von φ. χ_φ^{min} ist das eindeutig bestimmte normierte Polynom f kleinsten Grades mit $f(\varphi) = 0$.
(b) $\chi_\varphi^{min} | \chi_\varphi^{char}$, d.h. es existiert ein $q \in K[t]$ mit $\chi_\varphi^{char} = q \cdot \chi_\varphi^{min}$
Analog konstruiert man für $A \in M(n\times n,K)$ das Minimalpolynom χ_A^{min}. Es ist $\chi_\varphi^{min} = \chi_{\tilde{A}}^{min}$

Bemerkung 1.23. V endlichdimensional, $\lambda \in K$
Dann gilt: $\chi_\varphi^{char}(\lambda) = 0 \Leftrightarrow \chi_\varphi^{min}(\lambda) = 0$
Insbesondere haben χ_φ^{char} und χ_φ^{min} dieselben Nullstellen.

Beispiel 1.24. (a) $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M(2\times 2, \mathbb{Q})$. $\chi_A^{char} = (t-1)^2$
Wegen 1.22, 1.23 gilt: χ_A^{min} normiert, $\chi_A^{min} | \chi_A^{char}$, $\chi_A^{min}(1) = 0 \Rightarrow \chi_A^{min} \in \{t-1, (t-1)^2\}$
Wegen $A - E_2 = 0$ ist $\chi_A^{min} = t-1$.
(b) $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in M(2\times 2, \mathbb{Q}) \Rightarrow \chi_A^{char} = (t-1)(t+1) \overset{1.22,\, 1.23}{\Rightarrow} \chi_A^{min} = (t-1)(t+1) = \det \begin{pmatrix} t & -1 \\ -1 & t \end{pmatrix} = t^2 - 1$
(c) $A = \begin{pmatrix} 1 & -1 & 0 \\ -8 & 1 & 4 \\ 2 & -1 & -1 \end{pmatrix} \in M(3\times 3, \mathbb{R}) \Rightarrow \chi_A^{char} = (t+1)^2(t-3) \Rightarrow \chi_A^{min} = \{(t+1)(t-3), (t+1)^2(t-3)\}$
Es ist $(A+E_n)(A-3E_n) \neq 0$, also $\chi_A^{min} = (t+1)^2(t-3)$
(d) $A = \begin{pmatrix} 2 & -1 & -1 \\ -6 & 1 & 2 \\ 3 & -1 & -2 \end{pmatrix} \in M(3\times 3, \mathbb{R}) \Rightarrow \chi_A^{char} = (t+1)^2(t-3) \Rightarrow \chi_A^{min} \in \{(t+1)(t-3), (t+1)^2(t-3)\}$
Es ist $(A+E_n)(A-3E_n) = 0 \Rightarrow \chi_A^{min} = (t+1)(t-3)$.

Satz 1.25. *V endlichdimensional. Dann sind äquivalent:*
(i) φ diagonalisierbar
(ii) Das Minimalpolynom χ_φ^{min} zerfällt in Linearfaktoren und besitzt nur einfache Nullstellen,
d.h. $\chi_\varphi^{min} = (t-\lambda_1) \cdot \ldots \cdot (t-\lambda_r)$ mit paarweise verschidenen $\lambda_1, \ldots, \lambda_r \in K$

Beispiel 1.26. (vgl. 1.24)
(a) $A = \begin{pmatrix} 1 & -1 & 0 \\ -8 & 1 & 4 \\ 2 & -1 & -1 \end{pmatrix} \in M(3\times 3, \mathbb{R})$. Es ist $\chi_A^{min} = (t+1)^2(t-3) \overset{1.25}{\Rightarrow} A$ nicht diagonalisierbar.
(b) $A = \begin{pmatrix} 2 & -1 & -1 \\ -6 & 1 & 2 \\ 3 & -1 & -2 \end{pmatrix} \in M(3\times 3, \mathbb{R})$. Es ist $\chi_A^{min} = (t+1)(t-3) \overset{1.25}{\Rightarrow} A$ diagonalisierbar.

2. Dualraum

In diesem Abschnitt sei V ein K-VR.

Definition 2.1.
$V^* := Hom_K(V,K) = \{\varphi : V \to K | \varphi \text{ linear}\}$ heißt Dualraum von V, die Elemente aus V^* heißen Linearformen auf V.

Beispiel 2.2.
(a) $K = \mathbb{R}, V = \mathbb{R}^n$; $\varphi : \mathbb{R}^n \to \mathbb{R}$, $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto x_1$ ist eine Linearform auf $\mathbb{R}^n$
(b) $K = \mathbb{R}$, $V = \rho[0,1] = \{f : [0,1] \to \mathbb{R} | f \text{ stetig}\}\varphi : \rho[0,1] \to \mathbb{R}$, $f \mapsto \int_0^1 f(t)dt$ ist eine Linearform auf $\rho[0,1]$.

Bemerkung 2.3. V endlichdimensional, $B = (v_1, \dots, v_n)$ Basis von V. Wir definieren für $i = 1, \dots, n$ die linaere Abbildung $v_i^* : V \to K$, $v_j \mapsto \delta_{ij} = \begin{cases} 1, \text{ falls } i = j \\ 0, \text{ falls } i \neq j \end{cases}$
Dann ist $B^* := (v_1^*, \dots, v_n^*)$ ist eine Basis von V^*, die duale Basis zu B.

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

Notation: Elemente des K^n schreiben wir im Folgenden als Spaltenvektoren. Ist $\varphi \in (K^n)^* = Hom_K(K^n, K)$, dann existiert nach LA 1 ein eindeutig bestimmtes $A = \begin{pmatrix} a_1 & \dots & a_n \end{pmatrix} \in M(1 \times n, K)$ mit $\varphi = \tilde{A} : K^n \to K$,
$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} a_1 & \dots & a_n \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ (es ist $A = M_{(e_1)}^{(e_1,\dots,e_n)}(\varphi)$).
Dementsprechend schreiben wir Elemente von $(K^n)^*$ als Zeilenvektoren.

Beispiel 2.4. $(a) V = K^n, B = (e_1, \dots, e_n) \Rightarrow B^* = (e_1^*, \dots, e_n^*)$ duale Basis zu B mit $e_i^* = (0, \dots, 0, \underbrace{1}_{\text{i-te Stelle}}, 0, \dots, 0)$.
Für die Abbildung aus 2.2(a) gilt: $\varphi = e_1^* = (1, 0, \dots, 0)$.
(b) $K = \mathbb{R}, V = \mathbb{R}^2, B = (v_1, v_2)$ mit $v_1 = \binom{1}{0}, v_2 = \binom{1}{1}$.
Es ist $e_1 = v_1, e_2 = v_2 - v_1$
$\Rightarrow v_1^*(e_1) = v_1^*(v_1) = 1$, $v_1^*(e_2) = v_1^*(v_2 - v_1) = \underbrace{v_1^*(v_2)}_{=0} - \underbrace{v_1^*(v_1)}_{=1} = -1 \Rightarrow v_1^* = (1, -1)$
$v_2^*(e_1) = v_2^*(v_1) = 0$, $v_2^*(e_2) = v_2^*(v_2 - v_1) = \underbrace{v_2^*(v_2)}_{=1} - \underbrace{v_2^*(v_1)}_{=0} = 1 \Rightarrow v_2^* = (0, 1)$.

Folgerung 2.5. V endlichdimensional, $v \in V$, $v \neq 0$
Dann existiert $\varphi \in V^*$ mit $\varphi(v) \neq 0$

Anmerkung: Die Aussage gilt auch ohne die Voraussetzung "V endlichdimensional"

Folgerung 2.6. V endlichdimensional $B = (v_1, \dots, v_n)$ Basis von V, $B^* = (v_1^*, \dots, v_n^*)$ duale Basis zu B
Dann gibt es einen Isomorphismus $\psi_B : V \to V^*$, $v_i \mapsto v_i^*$ $(i = 1, \dots, n)$. Insbesondere ist $\dim V = \dim V^*$

Bemerkung 2.7. $U \subseteq V$ UVR
$U^0 = \{\varphi \in V^* | \varphi(u) = 0 \text{ für alle } u \in U\} \subseteq V^*$ heißt der Annulator von U. U^0 ist ein UVR von V^*.

Satz 2.8. V endlichdimensional $U \subseteq V$ UVR, $(u_1, \dots, u_k)$ von U. $B = (u_1, \dots, u_k, v_1, \dots, v_r)$ Basis von V
Dann ist die Teilfamilie $(v_1^*, \dots, v_r^*)$ von V^* eine Basis von U^0. Insbesondere ist $\dim U^0 = \dim V - \dim U$.

Bemerkung 2.9. V,W, K-VR $f : V \to W$ lineare Abbildung
Wir definieren $f^* : W^* \to V^*$, $\psi \mapsto f^*(\psi) = \psi \circ f$
f^* heißt die zu f duale Abbildung. Es gilt f^* ist linear.

Bemerkung 2.10. V,W endlichdimensional K-VRe
Dann ist die Abbildung $* : Hom_K(V,W) \to Hom_K(W^*,V^*)$, $f \mapsto f^*$ ist ein Isomorphismus von K-VR.

Satz 2.11. V,W endlichdimensionaler K-VR, A,B Basen von V bzw. W, $f : V \to W$ lineare Abbildung.
Dann gilt: $M^{B^*}_{A^*}(f^*) = (M^A_B(f))^t$

Satz 2.12. V,W endlichdimensional K-VR, $f : V \to W$ lineare Abbildung. Dann gilt:
(a) $im(f^*) = ker(f)^0$
(b) $\ker(f^*) = im(f)^0$

Folgerung 2.13. V,W endlichdimesnional K-VR, $f : V \to W$ lineare Abbildung. Dann gilt:
Rang(f^*) = Rang(f)

Folgerung 2.14. $A \in M(m \times n, K)$. Dann gilt:
Zeilenrang(A) = Spaltenrang(A)

Definition 2.15. $V^{**} := (V^*)^* = Hom_K(V^*,K)$ heißt der Bidualraum von V.

Satz 2.16. V endlichdimensional
Dann gibt es einen kanonischen (d.h. basisunabhängigen) Isomorphismus $i : V \to V^{**}$, $v \mapsto i_v$ mit $i_v : V^* \to K$, $\varphi \mapsto \varphi(v)$

Anmerkung:

- Im Gegensatz zu $\psi_B : V \to V^*$ ist der Isomorphismus $i : V \to V^{**}$ unabhängig von der Wahl einer Basis, d.h. V und V^* sind unkanonisch ismorph, 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 nie surjektiv.

Kapitel IV Bilinearformen und Skalarprodukte

In diesem Kapitel sei K stets ein Körper

3. Bilinearformen

In diesem Abschnitt sei V ein K-VR

Definition 3.1. $\gamma : V \times V \to K$ heißt eine Bilinearform auf V
$\Leftrightarrow$ Die folgenden Bedingungen sind erfüllt:
(B1) $\gamma(v_1 + v_2, w) = \gamma(v_1, w) + \gamma(v_2, w)$, $\gamma(\lambda v, w) = \lambda \gamma(v, w)$
(B2) $\gamma(v, w_1 + w_2) = \gamma(v, w_1) + \gamma(v, w_2)$, $\gamma(v, \lambda w) = \lambda \gamma(v, w)$
für alle $v, w, v_1, v_2, w_1, w_2 \in V$, $\lambda \in K$.

Beispiel 3.2.
(a) $K = \mathbb{R}$, $V = \mathbb{R}^n$, $\gamma : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$, $\gamma(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}) = x_1 y_1 + \ldots + x_n y_n$ ist eine Bilinearform auf $\mathbb{R}^n$.
(b) $K = \mathbb{R}$, $V = \rho[0,1]$, $\gamma : \rho[0,1] \times \rho[0,1] \to \mathbb{R}$, $\gamma(f, g) := \int_0^1 f(t)g(t)dt$ ist eine Bilinearform auf $\rho[0,1]$ (c) $K = \mathbb{R}$, $V = \mathbb{R}^2$, $\gamma : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$, $\gamma(\binom{x_1}{x_2}), \binom{y_1}{y_2})) = x_1 y_1 + 2x_1 y_2 - x_2 y_2$ ist eine Bilinearform auf $\mathbb{R}^2$.

Definition 3.3. V endlichdimensional, $B = (v_1, \ldots, v_n)$ Basis von V, γ Bilinearform auf V:
$M_B(\gamma) = (\gamma(v_i, v_j))_{1 \leq i \leq n, 1 \leq j \leq n} \in M(n \times n, K)$ heißt die Darstellungsmatrix (Fundamentalmatrix) von γ bzgl. B.

Beispiel 3.4.
(a) In 3.2a ist für $B = (e_1, \ldots, e_n) : M_B(\gamma) = E_n$
(b) In 3.2c ist für $B = (e_1, e_2) : M_B(\gamma) = \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix}$

Bemerkung 3.5. V endlichdimensional, $B = (v_1, \ldots, v_n)$ Basis von V, γ Bilinearform auf V, $A = M_B(\gamma)$, $\overline{\underline{\phi}}_B : K^n \to V$ Koordinatensystem zu B, $v, w \in V$, $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \overline{\underline{\phi}}_B^{-1}(v)$, d.h. $v = x_1 v_1 + \ldots + x_n v_n$, $y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \overline{\underline{\phi}}_B^{-1}(w)$, d.h. $w = y_1 v_1 + \ldots + y_n v_n$.

Dann gilt: $\gamma(v, w) = \overline{\underline{\phi}}_B^{-1}(v)^t A \overline{\underline{\phi}}_B^{-1}(w) = x^t A y = (x_1 \cdots x_n) A \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$

Bemerkung 3.6. V endlichdimensional, $B = (v_1, \ldots, v_n)$ Basis von V, $A \in M(n \times n, K)$
Dann gilt: Durch $\Delta_A^B : V \times V \to K$, $(v, w) \mapsto \overline{\underline{\phi}}_B^{-1}(v)^t A \overline{\underline{\phi}}_B^{-1}(w)$ ist eine Bilinearform auf V gegeben.

Beispiel 3.7. (wichtiger Spezialfall von 3.6)
$V = K^n, B = (e_1, \ldots, e_n), A \in M(n \times n, K) \Rightarrow \overline{\underline{\phi}}_B = id_{K^n} \Rightarrow$ Durch $\Delta_A^{(e_1, \ldots, e_n)} : K^n \times K^n \to K$, $(v, w) \mapsto v^t A w$ ist eine Bilinearform auf K^n gegeben. Wir setzen kurz $\Delta(A) := \Delta_A := \Delta_A^{(e_1, \ldots, e_n)}$

Bemerkung 3.8.
$Bil(V) := \{\gamma : V \times V \to K | \gamma \text{ ist Bilinearform}\}$ ist ein K-VR (ist ein UVR vom K-VR $Abb(V \times V, K)$)

Bemerkung 3.9. V endlichdimensional, $B = (v_1, \ldots, v_n)$ Basis von V, $A \in M(n \times n, K)$
Dann gilt: Die Abb. $M_B : Bil(V) \to M(n \times n, K)$ ist ein Isomorphismus von K-VR mit Umkehrabbildung $\Delta^B : M(n \times n, K) \to Bil(V), A \mapsto \Delta_A^B$

Satz 3.10. V endlichdimensional, A, B Basen von V, γ Bilinearformen auf V
Dann gilt: $M_B(\gamma) = (T_A^B)^t M_A(\gamma) T_A^B$.

Definition 3.11.
V endlichdimensional, γ Bilinearform auf V. Wir setzen $Rang(\gamma) := Rang(M_B(\gamma))$, wobei B eine Basis von V ist.

Anmerkung: Dies ist wohldefiniert (folgt aus 3.10, da die Matrizen T_A^B invertierbar sind)

Bemerkung 3.12. Es gilt:
(a) Ist $\gamma : V \times V \to K$ eine Bilinearform, dann induziert γ die linearen Abbildungen
$\Gamma_l : V \to V^*$, $w \mapsto \gamma(\cdot, w)$, wobei $\gamma(\cdot, w) : V \to K$, $v \mapsto \gamma(v, w)$
$\Gamma_r : V \to V^*$, $v \mapsto \gamma(v, \cdot)$, wobei $\gamma(v, \cdot) : V \to K$, $w \mapsto \gamma(v, w)$
(b) Jede lineare Abbildung $\Gamma : V \to V^*$ induziert Bilinearformen
$\gamma_l : V \times V \to K$, $\gamma_l(v, w) := \Gamma(w)(v)$
$\gamma_r : V \times V \to K$, $\gamma_r(v, w) := \Gamma(v)(w)$
Die Zuordnungen aus (a),(b) induzieren einen Isomorphismus $Bil(V) \cong Hom_K(V, V^*)$

Definition 3.13. γ Bilinearform auf V
γ heißt nicht-ausgeartet $\Leftrightarrow$ Γ_l und Γ_r sind injektiv $\Leftrightarrow$ ($\gamma(v, w) = 0$ für alle $v \in V \Rightarrow w = 0$ (Injektivität von Γ_l) und $\gamma(v, w) = 0$ für alle $w \in V \Rightarrow v = 0$ (Injektivität von Γ_r))
γ heißt perfekt $\Leftrightarrow$ Γ_l und Γ_r sind Isomorphismen.

Bemerkung 3.14. V endlichdimensional, γ Bilinearform auf V, $B = (v_1, \ldots, v_n)$ Basis von V, B^* duale Basis zu B
Dann gilt: $M_{B^*}^B(\Gamma_l) = M_B(\gamma) = (M_{B^*}^B(\Gamma_r))^t$

Folgerung 3.15. V endlichdimensional, γ Bilinearform auf V, B Basis von V. Dann sind äquivalent:
(i) γ nicht-ausgeartet
(ii) γ perfekt
(iii) $M_B(\gamma)$ invertierbar
(iv) Γ_l injektiv
(v) Γ_r injektiv

Definition 3.16. γ Bilinearform auf V
γ heißt symmetrisch $\Leftrightarrow$ $\gamma(v, w) = \gamma(w, v)$ für alle $v, w \in V$
γ heißt antisymmetrisch $\Leftrightarrow$ $\gamma(v, w) = -\gamma(w, v)$ für alle $v, w \in V$
γ heißt alternierend $\Leftrightarrow$ $\gamma(v, v) = 0$ für alle $v \in V$

Anmerkung:

- γ symmetrisch $\Rightarrow \Gamma_l = \Gamma_r$
- Für $char(K) \neq 2$ gilt: γ alternierend $\Leftrightarrow$ γ antisymmetrisch
- Für $char(K) = 2$ gilt immer noch γ alternierend $\Rightarrow$ γ (anti)symmetrisch
- Die Umkehrung ist falsch: $\gamma : \mathbb{F}_2^3 \times \mathbb{F}_2^3 \to \mathbb{F}_2$, $\gamma(x, y) = x_1y_1 + x_2y_2 + x_3y_3$ ist (anti)symmetrisch, aber nicht alternierend ($\gamma(\begin{pmatrix} \overline{1} \\ \overline{0} \\ \overline{0} \end{pmatrix}, \begin{pmatrix} \overline{1} \\ \overline{0} \\ \overline{0} \end{pmatrix}) = \overline{1} \neq \overline{0}$)

Bemerkung 3.17. V endlichdimensional, B Basis von V, γ Bilinearform auf V
Dann gilt:
(a) γ symmetrisch $\Leftrightarrow$ $M_B(\gamma)$ ist symmetrisch, d.h. $M_B(\gamma)^t = M_B(\gamma)$
(b) γ antisymmetrisch $\Leftrightarrow$ $M_B(\gamma)$ ist antisymmetrisch, d.h. $M_B(\gamma)^t = -M_B(\gamma)$

4. Quadratische Räume

Definition 4.1. V K-VR. Eine Abb. $q : V \to K$ heißt eine quadratische Form auf $V \Leftrightarrow$ Die folgenden Bedingungen sind erfüllt:
(Q1) $q(\lambda v) = \lambda^2 q(v)$ für alle $\lambda \in K$, $v \in V$
(Q2) Die Abbildung $\varepsilon_q : V \times V \to K$, $(v,w) \mapsto q(v+w) - q(v) - q(w)$ ist eine (automatisch symmetrische) Bilinearform.

Beispiel 4.2. $K = \mathbb{R}$, $V = \mathbb{R}^2$, $q(\binom{x_1}{x_2}) = x_1^2 + x_1x_2 + x_2^2$ ist eine quadratische Form auf $\mathbb{R}^2$:
(Q1) ist erfüllt, (Q2) ist ebenfalls erfüllt, denn:
$\varepsilon_q(\binom{x_1}{x_2}, \binom{y_1}{y_2}) = q(\binom{x_1+y_1}{x_2+y_2}) - q(\binom{x_1}{x_2}) - q(\binom{y_1}{y_2}) = (x_1+y_1)^2 + (x_1+y_1)(x_2+y_2) + (x_2+y_2)^2 - x_1^2 - x_1x_2 - x_2^2 - y_1^2 - y_1y_2 - y_2^2 = 2x_1y_1 + x_1y_2 + x_2y_1 + 2x_2y_2$, d.h. ε_q ist eine symmetrische Bilinearform.

Bemerkung 4.3. $charK \neq 2$, V K-VR, $SymBil(V) := \{\gamma : V \times V \to |\gamma \text{ ist symmetrische Bilinearform}\}$,
$Quad(V) := \{q : V \to K | q \text{ ist quadratische Form}\}$ Dann sind die Abbildungen:
$\underline{\overline{\phi}} : SymBil(V) \to Quad(V)$, $\gamma \mapsto q_\gamma$ mit $q_\gamma : V \to K$, $v \mapsto \gamma(v,v)$
$\underline{\psi} : Quad(V) \to SymBil(V)$, $q \mapsto \gamma_q := 1/2\varepsilon_q$, d.h. $\gamma_q : V \times V \to K$, $(v,w) \mapsto 1/2(q(v+w) - q(v) - q(w))$
zueinander inverse Bijektionen.

Anmerkung:

1. Philosophie dahinter: symmetrische Bilinearformen/quadratische Formen auf V sind für $char(K) \neq 2$ fast dasselbe.

2. Für $char(K) = 2$ kann man die Abbildung $\underline{\overline{\phi}}$ immer noch definieren, $\underline{\overline{\phi}}$ ist im allgemeinen weder injektiv noch surjetiv (exemplarisch: Für $K = \mathbb{F}_2$, $V = \mathbb{F}_2^2$ liegt die quadratische Form $q : \mathbb{F}_2^2 \to \mathbb{F}_2$, $\binom{x_1}{x_2}) \mapsto X_1^2 + x_1x_2 + x_2^2$ liegt nicht im Bild von $\underline{\overline{\phi}}$)

Für den Rest dieses Abschnittes sei K stets ein Körper mit $char(K) \neq 2$

Definition 4.4. Ein quadratischer Raum ist ein Paar (V,γ), bestehend aus einem endlichdimensionalen K-VR V und einer symmetrischen Bilinearform γ auf V.
$v,w \in V$ heißen orthogonal bzgl. $\gamma \Leftrightarrow \gamma(v,w) = 0$.
$(v_i)_{i\in I}$ Familie von Vektoren aus V heißt orthogonal bzgl. $\gamma \Leftrightarrow \gamma(v_i,v_j) = 0$ für alle $i,j \in I$, $i \neq j$.
Eine Familie $(v_1,\dots,v_n)$ von Vektoren aus V heißt eine Orthogonalbasis (OB) von $(V,\gamma) \Leftrightarrow (v_1,\dots,v_n)$ ist eine Basis von V und ist orthogonal bzgl. γ.

Anmerkung:

- Ist γ aus dem Kontext klar, wird es häufig weggelassen

- Ist B eine Basis von V, dann gilt: B OB von $(V,\gamma) \Leftrightarrow M_B(\gamma)$ ist eine Diagonalmatrix

Definition 4.5. (V,γ_V), (W,γ_W) quadratische Räume, $f : V \to W$ lineare Abbildung
f heißt Homomorphismus quadratischer Räume $\Leftrightarrow \gamma_W(f(v_1),f(v_2)) = \gamma_V(v_1,v_2)$ für alle $v_1,v_2 \in V$
f heißt Isomorphismus quadratischer Räume $\Leftrightarrow f$ ist ein Isomorphismus von K-VR und ein Homomorphismus quadratischer Räume.
Notation: Wir schreiben häufig $f : (V,\gamma_V) \to (W,\gamma_W)$ für eine Abb./Hom. quadratischer Räume

Anmerkung:

- Ist $f : (V,\gamma_V) \to (W,\gamma_W)$ ein Isomorphismus quadratischer Räume, dann ist $f^{-1} : (W,\gamma_W) \to (V,\gamma_V)$ ebenfalls ein Isomorphismus quadratischer Räume, und es ist $Rang(\gamma_V) = Rang(\gamma_W)$

Ziel: Klassifiziere quadratische Räume bis auf Isomorphie quadratischer Räume

Satz 4.6. (V,γ) quadratischer Raum. Dann besitzt (V,γ) eine OB.

Folgerung 4.7. $A \in M(n\times n, K)$ symmetrisch
Dann existiert ein $T \in GL(n,K)$, sodass T^tAT eine Diagonalmatrix ist

Folgerung 4.8. (V,γ) quadratischer Raum, $n = \dim V$, $r = Rang(\gamma)$
Dann existieren $\lambda_1,\ldots,\lambda_r \in K\backslash\{0\}$ un ein Isomorphismus von quadratischen Räumen

$$\underline{\overline{\phi}} : (K^n, \Delta(\begin{pmatrix} \lambda_1 & & & & & 0 \\ & \ddots & & & & \\ & & \lambda_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ 0 & & & & & 0 \end{pmatrix})) \to (V,\gamma)$$

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

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

Satz 4.9. (V,γ) quadratischer Raum über $\mathbb{C}$, $n = \dim V$, $r = Rang(\gamma)$
Dann existiert eine OB B von (V,γ) mit
$M_B(\gamma) = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$

Insbesondere existiert ein Isomorphismus quadratischer Räume $\underline{\overline{\phi}} : (\mathbb{C}^n, \Delta(\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix})) \to (V,\gamma)$

Folgerung 4.10. $A \in M(n\times n, \mathbb{C})$ symmetrisch, $r = Rang(A)$
Dann existiert ein $T \in GL(n,\mathbb{C})$, sodass $T^tAT = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$

Folgerung 4.11. (V,γ_V), (W,γ_W) quadratische Räume über $\mathbb{C}$. Dann sind äquivalent:
(i) Es gibt einen Isomorphismus quadratischer Räume $(V,\gamma_V) \to (W,\gamma_W)$
(ii) $\dim V = \dim W$ und $Rang(\gamma_V) = Rang(\gamma_W)$

Definition 4.12. (V,γ) quadratischer Raum, $U_1,\ldots,U_m \subseteq V$ UVR mit $V = U_1 \oplus \ldots \oplus U_m$.
Die direkte Summe heißt orthogonale direkte Summe $(V = U_1 \hat{\oplus} \ldots \hat{\oplus} U_m) \Leftrightarrow \gamma(u_i,u_j) = 0$ für alle $u_i \in U_i$, $u_j \in U_j$, $i \neq j$. (alternativ: $\perp$)

Satz 4.13. (V,γ) quadratischer Raum über $\mathbb{R}$, $n = \dim V$. Dann existiert eine OB B von (V,γ) sowie $r_+, r_- \in \{0,\ldots,\dim V\}$ mit

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

Insbesondere existiert ein Isomorphismus quadratischer Räume $(\mathbb{R}^n, \Delta(\begin{pmatrix} E_{r_+} & & 0 \\ & -E_{r_-} & \\ 0 & & 0 \end{pmatrix})) \to (V,\gamma)$. Die Zahlen r_+, r_- sind unabhängig von der Wahl einer solchen Basis . Wir nennen die Signatur$(\gamma) := (r_+, r_-)$ heißt die Signatur von γ

Folgerung 4.14. (Sylvesterscher Trägheitssatz)
$A \in M(n \times n, \mathbb{R})$ symmetrisch. Dann exisitert ein $T \in GL(n, \mathbb{R}), r_+, r_- \in \{0, \dots, n\}$ 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.
Signatur$(A) := (r_+, r_-)$ heißt die Signatur von A

Folgerung 4.15. $(V, \gamma_V), (W, \gamma_W)$ quadratische Räume über $\mathbb{R}$. Dann sind äquivalent:
(i) Es gibt einen Isomorphismus quadratischer Räume $(V, \gamma_V) \to (W, \gamma_W)$
(ii) $\dim V = \dim W$ und Signatur$(\gamma_V) =$ Signatur(γ_W)

5. Euklidische Räume

Definition 5.1. V $\mathbb{R}$-VR, $\gamma : V \times V \to \mathbb{R}$ symmetrische Bilinearform
γ heißt:
positiv definit $\Leftrightarrow \gamma(v, v) > 0$ für alle $v \in V \setminus \{0\}$
positiv semidefinit $\Leftrightarrow \gamma(v, v) \geq 0$ für alle $v \in V \setminus \{0\}$
negativ definit $\Leftrightarrow \gamma(v, v) < 0$ für alle $v \in V \setminus \{0\}$
negativ semidefinit $\Leftrightarrow \gamma(v, v) \leq 0$ für alle $v \in V \setminus \{0\}$
indefinit $\Leftrightarrow \gamma$ weder positiv noch negativ semidefinit.
Eine positiv definite symmetrische Bilinearform nennt man auch ein Skalarprodukt

Beispiel 5.2. (a) $V = \mathbb{R}^n$, $< .,. >: \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$, $< \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} > := x_1 y_1 + \ldots + x_n y_n$ ist ein Skalarprodukt auf dem $\mathbb{R}^n$

positiv Definitheit: $< \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} > = x_1^2 + \ldots + x_n^2 > 0$, falls $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \neq 0$

$< .,. >$ heißt das Standardskalarprodukt auf dem $\mathbb{R}^n$.
(b) $V = \rho[0, 1]$
$\gamma : \rho[0, 1] \times \rho[0, 1] \to \mathbb{R}$, $(f, g) \mapsto \int_0^1 f(t) g(t) dt$ ist ein Skalarprodukt.

Anmerkung: Um die Definitheit eine symmetrischen Bilinearform nachzuweisen, genügt es nicht, das Verhalten auf den Basisvektoren zu untersuchen:
Sei $\gamma : \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}$ gegeben durch $\gamma = \Delta(\begin{pmatrix} 1 & -2 \\ -2 & 1 \end{pmatrix})$, d.h. $M_{(e_1, e_2)}(\gamma) = \begin{pmatrix} 1 & -2 \\ -2 & 1 \end{pmatrix}$ Dann ist $\Gamma(e_1, e_2) = 1$, $\gamma(e_2, e_2) = 1$, aber
$\gamma(\binom{1}{1}, \binom{1}{1}) = (1\ 1) \begin{pmatrix} 1 & -2 \\ -2 & 1 \end{pmatrix} \binom{1}{1} = (1\ 1) \binom{-1}{-1} = -2 < 0$, d.h. γ ist indefinit.

Definition 5.3. 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 5.4. $v \in V$
$||v|| := \sqrt{\gamma(v, v)}$ heißt die Norm von V.
$(v_i)_{i \in I}$ Familie von Vektoren aus V heißt orthonormal $\Leftrightarrow (v_i)_{i \in I}$ ist orthogonal und $||v_i|| = 1$ für alle $i \in I$
$B = (v_1, \ldots v_n)$ heißt Orthonormalbasis von (V, γ) (ONB) $\Leftrightarrow B$ ist Basis von V und B ist orthonormal.

Bemerkung 5.5. $(v_1, \ldots, v_n)$ orthogonale Familie von Vektoren aus $V \setminus \{0\}$
Dann gilt:
(a) $(\frac{v_1}{||v_1||}, \ldots \frac{v_n}{||v_n||})$ ist eine orthonormale Familie
(b) $(v_1, \ldots, v_n)$ ist linear unabhängig

Bemerkung 5.6. Es gilt:
(a) (V, γ) besitzt eine ONB
(b) γ ist nicht-ausgeartet
(c) Es gibt eine Basis B von V mit $M_B(\gamma) = E_n$, wobei $n = \dim(V)$

Bemerkung 5.7. $B = (v_1, \ldots, v_n)$ ONB von (V, γ), $v \in V$
Dann gilt: Ist $v = \lambda_1 v_1 + \ldots + \lambda_n v_n$, dann ist $\lambda_i = \gamma(v, v_i)$ für $i = 1, \ldots, n$

Bemerkung 5.8. $U \subseteq V$ UVR
$U^\perp := \{v \in V | \gamma(v, u) = 0$ für alle $u \in U\}$ heißt das orthogonale Komplement zu U.
$U^\perp$ ist ein UVR von V.

Satz 5.9. $U \subseteq V$ UVR. Dann gilt:
(a) $V = U \oplus U^\perp$
(b) $\dim(U^\perp) = \dim(V) - \dim(U)$
(c) $(U^\perp)^\perp = U$
(d) Ist $(u_1, \ldots, u_m)$ eine ONB von $(U, \gamma|_{UxU})$, und ist $v \in V$ mit $v = u + v'$, $u \in U$, $v' \in U^\perp$, dann ist $u = \sum_{j=1}^{m} \gamma(v, u_j) u_j$.

Die lineare Abbildung $\pi_u : V \to U$, $v \mapsto \sum_{j=1}^{m} \gamma(v, u_j) u_j$ heißt die Orthogonalprojektion von V auf U.

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

Beispiel 5.10. $(V, \gamma) = (\mathbb{R}^2, <.,.>)$, $U = Lin(\binom{1}{1})$
$\Rightarrow U^\perp = Lin(\binom{-1}{1})$, denn $\binom{-1}{1} \in U^\perp$, wegen $< \binom{-1}{1}, \binom{1}{1} >= 0$, und es ist $\dim(U^\perp) = 2 - \dim(U) = 2 - 1 = 1$
Jedes Element aus V lässt sich eindeutig schreiben als $v = \lambda \binom{1}{1} + \mu \binom{-1}{1}$, d.h.
$$\pi_u : v = \underbrace{\lambda \begin{pmatrix} 1 \\ 1 \end{pmatrix}}_{\in U} + \underbrace{\mu \begin{pmatrix} -1 \\ 1 \end{pmatrix}}_{\in U^\perp} \mapsto \lambda \binom{1}{1} = \tfrac{1}{2}\gamma(v, \binom{1}{1})\binom{1}{1} = \gamma(v, 1/\sqrt{2}\binom{1}{1}) 1/\sqrt{2}\binom{1}{1}.$$

Frage: Wie bestimmt man explizit eine ONB eines euklidischen Raumes?

Satz 5.11. Algorithmus: Gram-Schmidt-Verfahren:
Eingabe: $(v_1, \ldots, v_n)$ Basis von V
Ausgabe: ONB $(w_1, \ldots, w_n)$ von (V, γ)
Durchführung:
1. Setze $w_1 := \frac{v_1}{||v_1||}$
2. Setze für $k = 2, \ldots, n$
$\tilde{w_k} := v_k - \sum_{i=1}^{k-1} \gamma(v_k, w_i) w_i$, $w_k := \frac{\tilde{w_k}}{||\tilde{w_k}||}$
3. $(w_1, \ldots, w_n)$ ist eine ONB von (V, γ).

Beispiel 5.12. Wir betrachten $(\mathbb{R}^3, <.,.>)$, $U = Lin((v_1, v_2))$ mit $v_1 := \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}$, $v_2 := \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}$

Gesucht ist eine ONB von U bzgl $<.,.>$.

Setze $w_1 := \frac{v_1}{||v_1||} = \frac{1}{\sqrt{5}} \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}$

$\tilde{w}_2 = v_2 - <v_2, w_1> w_1 = \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} - < \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}, \frac{1}{\sqrt{5}} \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} > \frac{1}{\sqrt{5}} \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} - \frac{1}{5} < \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} > \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} =$

$\begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} + \frac{2}{5} \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -\frac{1}{5} \\ 1 \\ \frac{2}{5} \end{pmatrix} = \frac{1}{5} \begin{pmatrix} -1 \\ 5 \\ 2 \end{pmatrix}$

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

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

Definition 5.13. $A \in M(n \times n, \mathbb{R})$ symmetrisch.
A heißt positiv definit (Notation: $A > 0$) $\Leftrightarrow$ Die symmetrische Bilinearform $\Delta(A) : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$, $(x, y) \mapsto x^t A y$ ist positiv definit.

Bemerkung 5.14. $A \in M(n \times n, \mathbb{R})$ symmetrisch. Dann sind äquivalent:
(i) $A > 0$
(ii) Es existiert ein $T \in Gl(n, \mathbb{R})$ mit $A = T^t T$

Anmerkung: (i), (ii) sind äquivalent zu: (iii): Es existiert eine obere Dreiecksmatrix P mit positiven Diagonaleinträgen, sodass $A = P^t P$ (siehe Übungen). Obiges P ist sogar eindeutig bestimmt, eine solche Zerlegung heißt Cholesky-Zerlegung.

Satz 5.15. (Cauchy-Schwarz-Ungleichung)
$v, w \in V$. Dann gilt:
$|\gamma(v, w)| \leq ||v|| \cdot ||w||$
Gleichheit gilt hierbei genau dann, wenn (v, w) linear abhängig.

Bemerkung 5.16. (Eigenschaften der Norm)
$v, w \in V, \lambda \in \mathbb{R}$. Dann gilt:
(a) $||v|| = 0 \Leftrightarrow v = 0$
(b) $||\lambda v|| = |\lambda| ||v||$
(c) $||v + w|| \leq ||v|| + ||w||$ (Dreiecksungleichung)

Bemerkung 5.17. $v, w \in V$. Dann gilt:
(a) $||v + w||^2 = ||v||^2 + ||w||^2 \Leftrightarrow \gamma(v, w) = 0$ (Satz des Pythagoras)
(b) $||v + w||^2 + ||v - w||^2 = 2||v||^2 + 2||w||^2$ (Parallelogrammgleichung)

Anmerkung: V $\mathbb{R}$-VR. Eine Abb $||.|| : V \to \mathbb{R}_{\geq 0}$ mit den Eigenschaften (a)-(c) aus 5.16 heißt eine Norm auf V, $(V, ||.||)$ ein normierter VR.
Man kann zeigen: Ist $(V, ||.||)$ ein normierter VR, 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 $||v|| = \sqrt{\gamma(v,v)}$ gegeben, d.h. in diesen Fällen ist (V,γ) ein euklidischer VR, dessen Norm mit der gegebenen übereinstimmt.

6. Die orthogonale Gruppe

Definition 6.1. (V, γ_V), (W, γ_W) euklidische Räume, $\varphi : V \to W$ lineare Abbildung
φ heißt orthogonal $\Leftrightarrow$ φ ist ein Homomorphismus quadratischer Räume, d.h. $\gamma_W(\varphi(v_1), \varphi(v_2)) = \gamma_V(v_1, v_2)$ für alle $v_1, v_2 \in V$.

Bemerkung 6.2. (V, γ_V), (W, γ_W) euklidische Räume, $\varphi : V \to W$ orthogonale Abbildung. Dann gilt:
(a) $||\varphi(v)||_W = ||v||_V$ für alle $v \in V$.
(b) $v_1 \perp v_2 \Leftrightarrow \varphi(v_1) \perp \varphi(v_2)$ für $v_1, v_2 \in V$
(c) φ ist injektiv

Bemerkung 6.3. (V,γ) euklidischer Raum, $n = \dim(V)$, B ONB von (V,γ).
Dann ist das Koordinatensystem $\underline{\overline{\phi}}_B : (\mathbb{R}^n, <.,.>) \to (V,\gamma)$ ist ein orthogonaler Isomorphismus

Bemerkung 6.4. (V,γ) euklidischer Raum. $\varphi \in End(V)$ orthogonal. Dann gilt:
(a) φ ist ein Isomorphismus
(b) φ^{-1} ist orthogonal
(c) $\lambda \in \mathbb{R}$ EW von $\varphi \Rightarrow |\lambda| = 1$, d.h. $\lambda \in \{\pm 1\}$

Bemerkung 6.5. (V,γ) euklidischer Raum, $n = \dim V$, B ONB von V, $\varphi \in End(V)$, $A = M_B(\varphi)$
Dann sind äquivalent:
(i) φ ist orthogonal
(ii) $A^t A = E_n$

Definition 6.6. $A \in M(n \times n, \mathbb{R})$
A heißt orthogonal $\Leftrightarrow A^t A = E_n$
$O(n) := \{A \in M(n \times n, \mathbb{R}) | A \text{ ist orthogonal}\}$
$O(n)$ ist bzgl. der Matrixmultiplikation eine Gruppe, die orthogonale Gruppe vom Rang n.

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

Bemerkung 6.7. $A \in M(n \times n, \mathbb{R})$. Dann sind äquivalent:
(i) $A \in O(n)$
(ii) $AA^t = E_n$
(iii) $A^t A = E_n$
(iv) Die Transponierten der Zeilen von A bilden eine ONB von $(\mathbb{R}^n, <.,.>)$
(v) Die Spalten von A bilden eine ONB von $(\mathbb{R}^n, <.,.>)$
(vi) Die Abb. $\tilde{A} : (\mathbb{R}^n, <.,.>) \to (\mathbb{R}^n, <.,.>)$ ist orthogonal

Satz 6.8. $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ (nicht notwendig linear) abstandstreu, d.h.
$||\varphi(x) - \varphi(y)|| = ||x - y||$ für alle $x, y \in \mathbb{R}^n$, wobei $||.||$ die Norm auf $(\mathbb{R}^n, <.,.>)$ bezeichne.
Dann existieren eindeutig bestimmte $A \in O(n)$, $b \in \mathbb{R}^n$, sodass $\varphi(x) = Ax + b$ für alle $x \in \mathbb{R}^n$ gilt.

Bemerkung 6.9. $SO(n) := \{A \in O(n) | \det(A) = 1\}$ ist eine Untergruppe von $O(n)$ (d.h. $SO(n) \subseteq O(n)$ und ist eine Gruppe bzgl. der eingeschränkten Verknüpfung), dei spezielle orthogonale Gruppe vom Rang n.

Beispiel 6.10. $n = 1 : O(1) = \{\pm 1\}, SO(1) = \{1\}$

Bemerkung 6.11. $A \in O(2)$. Dann gilt:
(a) $A \in SO(2) \Leftrightarrow$ Es existiert genau ein $\alpha \in [0, 2\pi)$ 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 $\alpha = 0 : A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, einziger EW: $+1$
Falls $\alpha = \pi : A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, einziger EW: -1
(b) $A \in O(2) \backslash SO(2) \Leftrightarrow$ Es existiert genau ein $\alpha \in [0, 2\pi)$ mit
$A = \begin{pmatrix} \cos(\alpha) & \sin(\alpha) \\ \sin(\alpha) & -\cos(\alpha) \end{pmatrix}$
In diesem Fall beschreibt A eine Spiegelung an der Geraden $Lin(\binom{\cos(\frac{\alpha}{2})}{\sin(\frac{\alpha}{2})})$, A besitzt die EW ± 1, und es existiert eine ONB B von $(\mathbb{R}^2, <.,.>)$ mit $M_B(\tilde{A}) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Folgerung 6.12. $\varphi : (\mathbb{R}^2, <.,.>) \to (\mathbb{R}^2, <.,.>)$, sodass $M_B(\varphi) = \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix}$ oder $M_B(\varphi) = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$ für ein $\alpha \in (0, \pi)$
Die Anzahl der ± 1 sowie α sind unabhängig von der Wahl einer solchen ONB B (d.h. sind Invarianten von φ)

Ab hier nicht klausurrelevant

Ziel: Verallgemeinerung von 6.12 auf $(\mathbb{R}^n, <.,.>)$

Bemerkung 6.13. $f \in \mathbb{R}[t] \backslash \{0\}$, $n = \deg(f)$
Dann existieren $r, m \in \mathbb{N}_0$ mit $r + 2m = n$, $a \in \mathbb{R}^*$, $\lambda_1, \ldots, \lambda_r \in \mathbb{R}$, $b_1, \ldots, b_m \in \mathbb{R}$, $c_1, \ldots, c_m \in \mathbb{R}$, sodass $f = a(t - \lambda_1) \cdot \ldots \cdot (t - \lambda_r)(t^2 + b_1 t + c_1) \cdot \ldots \cdot (t^2 + b_m t + c_m)$ und die Polynome $t^2 + b_i t + c_i$ haben keine reellen Nullstellen.

Satz 6.14. V endlichdimensionaler $\mathbb{R}$-VR, $\dim(V) \geq 1$, $\varphi \in End(V)$
Dann existiert ein UVR $W \subseteq V$ mit $\varphi(W) \subseteq W$ und $1 \leq \dim(W) \leq 2$

Satz 6.15. (V,γ) euklidischer VR, $\varphi \in End(V)$ orthogonal
Dann existiert eine ONB B von V, sodass

$$M_B(\varphi) = \begin{pmatrix} +1 &&&&&&&& \\ & \ddots &&&&&&& \\ && +1 &&&&&& \\ &&& -1 &&&&& \\ &&&& \ddots &&&& \\ &&&&& -1 &&& \\ &&&&&& A_1 && \\ &&&&&&& \ddots & \\ &&&&&&&& A_k \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}1\\1\\1\end{matrix}}\right\}\text{r} \\ \left.\vphantom{\begin{matrix}1\\1\\1\end{matrix}}\right\}\text{s} \\ \vphantom{\begin{matrix}1\\1\\1\end{matrix}} \end{matrix}$$

wobei $A_j = \begin{pmatrix} \cos(\alpha_j) & -\sin(\alpha_j) \\ \sin(\alpha_j) & \cos(\alpha_j \end{pmatrix} \in SO(2)$, $\alpha_j \in (0,\pi)$
r,s und $\alpha_1,\dots,\alpha_k$ (bis auf Reihenfolge) sind unabhängig von der Wahl einer solchen ONB.
Insbesondere gilt: $r =$ Vielfachheit des EW $+1$ von φ
$s =$ Vielfachheit des EW -1 von φ

Folgerung 6.16. Jede orthogonale Selbstabbildung des $(\mathbb{R}^3, <.,.>)$ kann man bzgl. einer geeigneten ONB wie folgt darstellen:

(I) $\begin{pmatrix} 1 && \\ & 1 & \\ && 1 \end{pmatrix}$ id. Abbildung

(IV) $\begin{pmatrix} -1 && \\ & -1 & \\ && -1 \end{pmatrix}$ Punktspiegelung an 0.

(II) $\begin{pmatrix} 1 && \\ & 1 & \\ && -1 \end{pmatrix}$ Spiegelung an Ebene

(V) $\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\alpha) & -\sin(\alpha) \\ 0 & \sin(\alpha) & \cos(\alpha) \end{pmatrix}$ Drehung mit fester Drehachse um den Winkel $\alpha \in (0,\pi)$

(III) $\begin{pmatrix} 1 && \\ & -1 & \\ && -1 \end{pmatrix}$ Drehung mit fester Drehachse um den Winkel π

(VI) $\begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos(\alpha) & -\sin(\alpha) \\ 0 & \sin(\alpha) & \cos(\alpha) \end{pmatrix}$ "Drehspiegelung": Drehung mit fester Drehachse um den Winkel $\alpha \in (0,\pi)$ mit nachfolgender Spiegelung an der zur Drehachse orthogonalen Ursprungsebene

Ende der nicht Klausurrelevanz

7. Der Spektralsatz

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

Bemerkung 7.1. Die Abb. $\Gamma : V \to V^*$, $w \mapsto \gamma(.,w)$ ist ein Isomorphismus.

Anmerkung: Insbesondere sind für einen euklidischen VR (V,γ) die VRe V und V^* kanonisch isomporph

Bemerkung 7.2. $B = (v_1,\dots,v_n)$ ONB von (V,γ), $B^* = (v_1^*,\dots,v_n^*)$ duale Basis zu B, $U \subseteq V$ UVR, $\Gamma : V \to V^*$ kanonische Abbildung aus 7.1. Dann gilt:
(a) $\Gamma(U^\perp) = U^0$
(b) $\Gamma(v_i) = v_i^*$ für $i = 1,\dots,n$

Bemerkung 7.3. (V,γ_V), (W,γ_W) euklidische Räume, $\varphi : V \to W$
Dann existiert genau eine lineare Abbildung $\varphi^{ad} : W \to V$ mit $\gamma_W(\varphi(v),w) = \gamma_V(v,\varphi^{ad}(w))$ für alle $v \in V, w \in W$.
φ^{ad} heißt die zu φ adjungierte Abbildung

Anmerkung: Ist $\varphi : V \to V$ orthogonal, dann ist $\varphi^{ad} = \varphi^{-1}$, denn für $v,w \in V$:
$\gamma(\varphi(v),w) = \gamma(\varphi(v),\varphi(\varphi^{-1}(w))) = \gamma(v,\varphi^{-1}(w))$.

Bemerkung 7.4. $(V,\gamma_V),(W,\gamma_W)$ eukldische Räume, A ONB von (V,γ_V), B ONB von (W,γ_W), $\varphi : V \to W$ lineare Abbildung. Dann gilt:
$M_A^B(\varphi^{ad}) = (M_B^A(\varphi))^t$
Insbesondere ist $(\varphi^{ad})^{ad} = \varphi$.

Satz 7.5. (V,γ_V), (W,γ_W) euklidische Räume, $\varphi : V \to W$ lineare Abbildung. Dann gilt:
(a) $\ker(\varphi^{ad}) = (im(\varphi))^\perp$
(b) $im(\varphi^{ad}) = (\ker(\varphi))^\perp$

Folgerung 7.6. $\varphi \in End(V)$
Dann gilt:
$V = \ker(\varphi)\hat{\oplus} im(\varphi^{ad})$ sowie $V = \ker(\varphi^{ad})\hat{\oplus} im(\varphi)$

Definition 7.7. $\varphi \in End(V)$
φ heißt selbstadjungiert $\Leftrightarrow \varphi = \varphi^{ad}$

Bemerkung 7.8. B ONB von (V,γ). Dann sind äquivalent:
(i) φ selbstadjungiert
(ii) $M_B(\varphi)$ symmetrsich.
In diesem Fall ist $V = \ker(\varphi)\hat{\oplus} im(\varphi)$.

Satz 7.9. Es gilt:
(a) $\varphi \in End(V)$ selbstadjungiert: $\Rightarrow \gamma' : V \times V \to \mathbb{R}$, $\gamma'(x,y) = \gamma(\varphi(x),y)$ ist eine symmetrische Bilinearform
(b) Ist $\gamma' : V \times V \to \mathbb{R}$ eine symmetrische Bilinearform, dann existiert genau ein selbstadjungierter Endomorphismus $\varphi \in End(V)$ mit $\gamma'(x,y) = \gamma(\varphi(x),y)$ für alle $x,y \in V$.
In diesen Fällen gilt bzgl. jeder ONB B von (V,γ): $M_B(\gamma') = M_B(\varphi)$.

Anmerkung: Interpretation für $(\mathbb{R}^n, <.,.>)$:
Ist $A \in M(n \times n,\mathbb{R})$ symmetrisch, dann ist A:

- Darstellungsmatrix bzgl. $(e_1,\dots,e_n)$ des selbstadjungierten Endomorphismus $\tilde{A}$ von $\mathbb{R}^n$
- Darstellungsmatrix bzgl $(e_1,\dots,e_n)$ der symmetrischen Bilinearform $\gamma' = \Delta(A) : (x,y) \mapsto x^tAy$

Es ist $\gamma'(x,y) = x^tAy = x^tA^ty = (Ax)^ty = < Ax, y > = < \tilde{A}(x), y >$ für alle $x, y \in \mathbb{R}^n$.
Bzgl. jeder ONB von $(\mathbb{R}^n, < ., . >)$ gilt $M_B(\tilde{A}) = M_B(\gamma')$.

Bemerkung 7.10. $\varphi \in End(V)$ selbstadjungiert, $U \subseteq V$ UVR mit $\varphi(U) \subseteq U$
Dann gilt: $\varphi(U^\perp) \subseteq U^\perp$

Bemerkung 7.11. $\varphi \in End(V)$ selbstadjungiert:
Dann zerfällt χ_φ^{char} über $\mathbb{R}$ in Linearfaktoren.

Satz 7.12. (Spektralsatz für selbstadjungierte Endomorphismen)
$\varphi \in End(V)$ selbstadjungierter Endomorphismus. Dann existiert eine ONB von (V, γ) aus EV von φ.
Sind $\lambda_1, \ldots, \lambda_r$ die verschiedenen EW von φ, so ist $V = Eig(\varphi, \lambda_1) \hat{\oplus} \ldots \hat{\oplus} Eig(\varphi, \lambda_r)$

Folgerung 7.13. $\gamma' : V \times V \to \mathbb{R}$ symmetrische Bilinearform, $n = \dim V$.
Dann existiert eine ONB B von (V, γ), bzgl. derer die Darstellungsmatrix von γ' Diagonalgestalt hat:
$M_B(\gamma') = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$ Hierbei sind $\lambda_1, \ldots, \lambda_n$ die EWe (mit Vielf.) des zu γ' gehörenden eindeutig bestimmten selbstadjungierten Endomorphismus $\varphi \in End(V)$mit $\gamma'(x,y) = \gamma(\varphi(x), y)$ (vgl. 7.9)

Folgerung 7.14. $A \in M(n \times n, \mathbb{R})$ 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 $\lambda_1, \ldots, \lambda_n$ die EWe (mit Vielf.) von A. Die Spalten von T bilden eine ONB von $(\mathbb{R}^n, < ., . >)$ aus EV von A.

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

Satz 7.15. (Algorithmus Hauptachsentranformation)
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 $\chi_A^{char} = (t - \lambda_1)^{r_1} \cdot \ldots \cdot (t - \lambda_k)^{r_k}$ mit $\lambda_1, \ldots, \lambda_k$ paarweise verschieden
2. Bestimme für $i = 1, \ldots k$ jeweils eine Basis von $Eig(A, \lambda_i)$
3. Bestimme mit dem Gram-Schmidt-Verfahren für $i = 1, \ldots, k$ eine ONB $B_i = (v_{i_1}, \ldots, v_{i,r_i})$ von $Eig(A, \lambda_i)$
4. Die ONB B_i, $i = 1, \ldots, k$ bilden zusammen eine ONB $B = (v_{1,1}, \ldots, v_{1,r_1}, \ldots, v_{k,1}, \ldots, v_{k,r_k})$ des $(\mathbb{R}^n, < ., . >)$ aus EV von A.
5. Schreibe die Basisvektoren aus B in Spalten von T

Es ist dann $T^{-1}AT = \begin{pmatrix} \lambda_1 & & & & & & \\ & \ddots & & & & & \\ & & \lambda_1 & & & & \\ & & & \ddots & & & \\ & & & & \lambda_k & & \\ & & & & & \ddots & \\ & & & & & & \lambda_k \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}1\\1\\1\end{matrix}}\right\} r_1 \\ \\ \left.\vphantom{\begin{matrix}1\\1\\1\end{matrix}}\right\} r_k \end{matrix}$

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

Beispiel 7.16.
$A = \begin{pmatrix} 2 & -1 & 2 \\ -1 & 2 & 2 \\ 2 & 2 & -1 \end{pmatrix} \in M(3\times 3, \mathbb{R})$
Es ist $\chi_A^{char} = t^3 - 3*t^2 - 9*t + 27 = (t-3)^2(t+3)$
Es ist $Eig(A,3) = \ldots = Lin(\begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix})$

Nach Bsp 5.12 ist $(\frac{1}{\sqrt{5}}\begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{30}}\begin{pmatrix} -1 \\ 5 \\ 2 \end{pmatrix})$ eine ONB von $Eig(A,3)$

$Eig(A,-3) = Lin(\begin{pmatrix} 1 \\ 1 \\ -2 \end{pmatrix}) \Rightarrow (\frac{1}{\sqrt{6}}\begin{pmatrix} 1 \\ 1 \\ -2 \end{pmatrix})$ ist eine ONB von $Eig(A,-3)$

$\Rightarrow (\frac{1}{\sqrt{5}}\begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{30}}\begin{pmatrix} -1 \\ 5 \\ 2 \end{pmatrix}, \frac{1}{\sqrt{6}}\begin{pmatrix} 1 \\ 1 \\ -2 \end{pmatrix})$ ist ONB von $(\mathbb{R}^3, <.,.>)$ aus EVen von A.

Mit $T = \begin{pmatrix} \frac{2}{\sqrt{5}} & -\frac{1}{\sqrt{30}} & \frac{1}{\sqrt{6}} \\ 0 & \frac{5}{\sqrt{30}} & \frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{5}} & \frac{2}{\sqrt{30}} & -\frac{2}{\sqrt{6}} \end{pmatrix}$ ist $T^{-1}AT = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & -3 \end{pmatrix}$
Es ist $\det(T) = -1$, also $T \in O(3)\backslash SO(3)$.
Setzt man $T' := \begin{pmatrix} -\frac{2}{\sqrt{5}} & -\frac{1}{\sqrt{30}} & \frac{1}{\sqrt{6}} \\ 0 & \frac{5}{\sqrt{30}} & \frac{1}{\sqrt{6}} \\ -\frac{1}{\sqrt{5}} & \frac{2}{\sqrt{30}} & -\frac{2}{\sqrt{6}} \end{pmatrix}$ ist $(T')^{-1}AT' = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & -3 \end{pmatrix}$ und es ist $T' \in SO(3)$

Ab hier nicht klausurrelevant

Bemerkung 7.17. $\gamma' \colon V \times V \to \mathbb{R}$ symmetrische Bilinearform
Dann existiert eine Orthogonalbasis B von (V, γ) mit

$$M_B(\gamma') = \begin{pmatrix} 1 &&&&&&&& \\ & \ddots &&&&&&& \\ && 1 &&&&&& \\ &&& -1 &&&&& \\ &&&& \ddots &&&& \\ &&&&& -1 &&& \\ &&&&&& 0 && \\ &&&&&&& \ddots & \\ &&&&&&&& 0 \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}1\\ \ddots\\ 1\end{matrix}}\right\} s_+ \\ \left.\vphantom{\begin{matrix}1\\ \ddots\\ 1\end{matrix}}\right\} s_- \\ \left.\vphantom{\begin{matrix}1\\ \ddots\\ 1\end{matrix}}\right\} s_0 \end{matrix}$$

Ist $\varphi \in End(V)$ der gemäß 7.9 zu γ' gehörige selbstadjungierte Endomorphismus von V, dann:
$s_+ =$ Anzahl der positiven Eigenwerte von φ (mit Vielf.)
$s_- =$ Anzahl der negativen Eigenwerte von φ (mit Vielf.)
$s_0 =$ Vielfachheit des Eigenwerts 0 von φ
Die Invarianten s_+, s_-, s_0 stimmen mit den Invarianten $r_+, r_-, n-(r_+ + r_-)$ aus dem Sylvesterschen Trägheitssatz für (V, γ') überein.

Folgerung 7.18. $A \in M(n \times n, \mathbb{R})$ symmetrisch
Dann existiert ein $T \in Gl(n, \mathbb{R})$ (deren Spalten eine Orthogonalbasis von $(\mathbb{R}^n, <.,.>)$ bilden) mit

$$T^tAT = \begin{pmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 1 & & & & & & \\ & & & -1 & & & & & \\ & & & & \ddots & & & & \\ & & & & & -1 & & & \\ & & & & & & 0 & & \\ & & & & & & & \ddots & \\ & & & & & & & & 0 \end{pmatrix} \begin{array}{l} \left.\begin{array}{l} \\ \\ \\ \end{array}\right\} s_+ \\ \left.\begin{array}{l} \\ \\ \\ \end{array}\right\} s_- \\ \left.\begin{array}{l} \\ \\ \\ \end{array}\right\} s_0 \end{array}$$

Hierbei ist $s_+ =$ Anzahl der positiven Eigenwerte von A, $s_- =$ Anzahl der negativen Eigenwerte von A (jeweils mit Vielfachheit). $s_0 =$ Vielfachheit des Eigenwerts 0 von A.
Die Invarianten s_+, s_-, s_0 stimmen mit $r_+, r_-, n-(r_+ + r_-)$ aus dem Sylvesterschen Trägheitssatz überein.

Folgerung 7.19. $A \in M(n \times n, \mathbb{R})$ symmetrisch, $S \in Gl(n, \mathbb{R})$
Dann gilt: A und S^tAS haben mit Vielfachheit gezählt die gleiche Anzahl positiv und negativer Eigenwerte.

Ende der nicht Klausurrelevanz

8. Unitäre Räume

Definition 8.1. V $\mathbb{C}$-VR, $h : V \times V \to \mathbb{C}$, $(v,w) \mapsto h(v,w)$ heißt Sesquilinearform auf V $\Leftrightarrow$ Die folgenden Bedingungen sind erfüllt:
(S1) $h(v_1+v_2,w) = h(v_1,w)+h(v_2,w)$, $h(\lambda v,w) = \lambda h(v,w)$
(S2) $h(v,w_1+w_2) = h(v,w_1)+h(v,w_2)$, $h(v,\lambda w) = \overline{\lambda}h(v,w)$
für alle $v_1,v_2,w_1,w_2,v,w \in V, \lambda \in \mathbb{C}$

Beispiel 8.2. $h : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$, $h(x,y) := x^t\overline{y}$ ist eine Sesquilinearform auf $\mathbb{C}^n$
(beachte: $h(x,\lambda y) = x^t\overline{\lambda y} = \overline{\lambda}x^ty$), aber keine Bilinearform auf $\mathbb{C}^n$

Bemerkung 8.3. V $\mathbb{C}$-VR, $h : V \times V \to \mathbb{C}$ Sesquilinearform auf V.
Dann induziert h eine "semilineare" Abbildung
$\Gamma : V \to V^*$, $w \mapsto h(\cdot,w)$
(d.h. $\Gamma(w_1+w_2) = \Gamma(w_1)+\Gamma(w_2)$, $\Gamma(\lambda(w)) = \overline{\lambda}\Gamma(w)$ für alle $w_1,w_2 \in V, w \in V, \lambda \in \mathbb{C}$)

Definition 8.4. V endlichdimensional $\mathbb{C}-VR$, h Sesquilinearform auf V, $B = (v_1,\dots,v_n)$ Basis von V
$M_B(h) = (h(v_i,v_j))_{1\leq i\leq n, 1\leq j\leq n}$ heißt die Darstellungsmatrix (Fundamentalmatrix) von h bzgl. B.

Bemerkung 8.5. V endlichdimensional $\mathbb{C}$-VR, $B = (v_1,\dots v_n)$ Basis von V.
$Sesq(V) := \{h : V \times V \to \mathbb{C} | h \text{ ist eine Sesquilinearform}\}$ ist eine $\mathbb{C}$-VR/UVR von $Abb(V \times V, \mathbb{C})$
Dann gilt: Die Abb. $M_B : Sesq(V) \to M(n \times n, \mathbb{C})$, $h \mapsto M_B(h)$ ist ein Isomorphismus von $\mathbb{C}$-VR mit Umkehrabbildung $\Delta^B : M(n \times n, \mathbb{C}) \to Sesq(V)$ mit $\Delta^B(A)(v,w) = \underline{\phi}_B^{-1}(v)^tA\overline{\underline{\phi}_B^{-1}(w)}$

Satz 8.6. V endlichdimensional $\mathbb{C}$-VR, A,B Basen von V, h Sesquilinearform auf V
Dann gilt: $M_B(h) = (T_A^B)^t \cdot M_A(h) \cdot \overline{T_A^B}$

Definition 8.7. V $\mathbb{C}$-VR, h Sesquilinearform auf V
h heißt hermitesch $\Leftrightarrow h(w,v) = \overline{h(v,w)}$ für alle $v,w \in V$

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

Bemerkung 8.8. V endlichdimensionaler $\mathbb{C}$-VR, h Sesquilinearform auf V, B Basis von V, $A = M_B(h)$
Dann sind äquivalent:
(i) h ist hermitesch
(ii) $\overline{A}^t = A$

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

Definition 8.9. V $\mathbb{C}$-VR, h hermitesche Form auf V
h heißt positiv definit $\Leftrightarrow h(v,v) > 0$ für alle $v \in V$, $v \neq 0$
Eine positiv definite hermitesche Form nennt man auch ein Skalarprodukt

Beispiel 8.10. $V = \mathbb{C}^n$, $< .,. >: \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$, $< x,y >:= x^t\overline{y}$ ist ein Skalarprodukt auf $\mathbb{C}^n$ (das Standardskalarprodukt auf $\mathbb{C}^n$):

- $< .,. >$ ist sesquilinear (vgl. 8.2)
- $< .,. >$ ist hermitesch: $< y,x >= y^t\overline{x} = (y^t\overline{x})^t = \overline{x}^t y = \overline{x^t\overline{y}} = \overline{< x,y >}$

$< .,. >$ ist postiv definit: $< x,x >= x^t\overline{x} = (x_1 \cdots x_n) \begin{pmatrix} \overline{x_1} \\ \vdots \\ \overline{x_n} \end{pmatrix} = X_1\overline{x_1} + \ldots + x_n\overline{x_n} = |x_1|^2 + \ldots + |x_n|^2 > 0$ für $x \neq 0$

Definition 8.11. Ein unitärer Raum ist ein Paar (V,h), betstehend aus einem endlichdimensionalen $\mathbb{C}$-VR 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 und orthogonales Komplement.
Es gilt dabei:

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

Definition 8.12. (V,h_V), (W,h_W) unitäre Räume, $\varphi : V \to W$ lineare Abbildung
φ heißt unitär $\Leftrightarrow h_W(\varphi(v_1), \varphi(v_2)) = h_V(v_1,v_2)$ für alle $v_1,v_2 \in V$

Bemerkung 8.13. $n = \dim(V)$, B ONB von (V,h)
Dann ist das Koordinatensystem $\underline{\overline{\phi}}_B : (\mathbb{C}^n, < .,. >) \to (V,h)$ ist ein unitärer Isomorphismus

Bemerkung 8.14. B ONB von (V,h), $\varphi \in End(V)$, $A = M_B(\varphi)$. Dann sind äquivalent:
(i) φ ist unitär
(ii) $\overline{A}^t A = E_n$

Bemerkung 8.15. $A \in M(n\times, \mathbb{C})$
A heißt unitär $\Leftrightarrow \overline{A}^t A = E_n$
$U(n) := \{A \in M(n \times n, \mathbb{C}) | A \text{ ist unitär}\}$
$U(n)$ ist eine Gruppe bzgl. "$\cdot$", die unitäre Gruppe vom Rang n
$SU(n) := \{A \in U(n) | \det(A) = 1\}$ ist eine Untergruppe von $U(n)$, die spezielle unitäre Gruppe vom Rang n

Bemerkung 8.16. $B = (v_1, \ldots, v_n)$ ONB von (V,h), $B^* = (v_1^*, \ldots, v_n^*)$ duale Basis.
Dann ist die Abb. $\Gamma : V \to V^*$, $w \mapsto h(\cdot, w)$ ist ein Semiisomorphismus mit $\Gamma(v_i) = v_i^*$ für $i = 1, \ldots, n$.

Satz 8.17. (V, h_V),(W, h_W) unitäre Räume, $\varphi : V \to W$ lineare Abbildung, A ONB von (V, h_V) B ONB von (W, h_W).
Dann gilt:
(a) Es gibt genau eine lineare Abbildung $\varphi^{ad} : W \to V$ mit $h_W(\varphi(v), w) = h_V(v, \varphi^{ad}(w))$ für alle $v \in V, w \in W$.
φ^{ad} heißt die zu φ adjungierte Abbildung.
(b) $M_A^B(\varphi^{ad}) = \overline{M_B^A(\varphi)}^t$

Bemerkung 8.18. $\varphi \in End(V)$. Dann gilt:
(a) $\ker(\varphi^{ad}) = (im(\varphi))^\perp$
(b) $im(\varphi^{ad}) = (\ker(\varphi))^\perp$

Definition 8.19. $\varphi \in End(V)$. φ heißt selbstadjungiert $\Leftrightarrow \varphi = \varphi^{ad}$

Bemerkung 8.20. $\varphi \in End(V)$, B ONB von (V,h), $A = M_B(\varphi)$. Dann sind äquivalent:
(i) φ selbstadjungiert
(ii) $\overline{A}^t = A$, d.h. A ist hermitesch

Bemerkung 8.21. $\varphi \in End(V)$ selbstadjungiert. Dann sind alle Eigenwerte von φ reell.

Definition 8.22. $\varphi \in End(V)$
φ heißt normal $\Leftrightarrow \varphi^{ad} \circ \varphi = \varphi \circ \varphi^{ad}$
$A \in M(n \times n, \mathbb{C})$ heißt normal $\Leftrightarrow \overline{A}^t A = A\overline{A}^t$

Anmerkung: Ist B eine ONB von (V,h), dann: φ normal $\Leftrightarrow M_B(\varphi)$ normal.

Bemerkung 8.23. $\varphi \in End(V)$. Dann gilt:
(a) φ unitär $\Rightarrow$ normal
(b) φ selbstadjungiert $\Rightarrow$ normal
Für $A \in M(n \times n, \mathbb{C})$ gilt: A unitär $\Rightarrow A$ normal, A hermitesch $\Rightarrow A$ normal.

Satz 8.24. $\varphi \in End(V)$ normal
Dann gilt:
(a) $\ker(\varphi^{ad}) = \ker(\varphi)$
(b) $im(\varphi^{ad}) = im(\varphi)$
Insbesondere gilt $V = \ker(\varphi) \hat{\oplus} im(\varphi)$

Bemerkung 8.25. $\varphi \in End(V)$ normal, $\lambda \in \mathbb{C}$
Dann gilt:
(a) $\varphi - \lambda id_V$ ist normal
(b) $Eig(\varphi, \lambda) = Eig(\varphi^{ad}, \overline{\lambda})$

Satz 8.26. (Spektralsatz für normale Endomorphismen)
$\varphi \in End(V)$. Dann sind äquivalent:
(i) Es gibt eine ONB von (V,h) aus EVen von φ
(ii) φ ist normal

Anmerkung: Insbesondere gilt:

- Für jeden selbstadjungierten/unitären Endomorphismus existiert eine ONB aus EVen
- 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 (z.B. $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ (Drehungen um$\frac{\pi}{2}$))

Folgerung 8.27. $A \in M(n \times n, \mathbb{C})$. Dann sind äquivalent:
(i) A ist normal
(ii) Es gibt ein $T \in U(n)$, sodass $T^{-1}AT = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$ $, \lambda_1, \dots, \lambda_n$ EW von A

Kapitel V Ringe und Moduln

9. Ringe, Ideale, Teilbarkeit

In diesem Abschnitt seien R, S stets kommutative Ringe (bei uns immer mit Eins)

Definition 9.1. $\varphi : R \to S$ Abbildung. φ heißt Ringhomomorphismus $\Leftrightarrow$ Die folgenden Bedingungen sind erfüllt:
(RH1) $\varphi(a+b) = \varphi(a) + \varphi(b)$
(RH2) $\varphi(ab) = \varphi(a)\varphi(b)$ für alle $a, b \in \mathbb{R}$
(RH3) $\varphi(1_R) = 1_S$

Definition 9.2. $I \subseteq R$
I heißt Ideal in $R \Leftrightarrow$ Die folgenden Bedingungen sind erfüllt:
(I1) $0 \in I$
(I2) $a, b \in I \Rightarrow a + b \in I$
(I3) $r \in R, a \in I \Rightarrow ra \in I$

Beispiel 9.3.
(a) $\{0\}, R$ sind Ideale in R
(b) Für $n \in \mathbb{Z}$ ist $n\mathbb{Z} := \{na | a \in \mathbb{Z}\}$ ist ein Ideal in $\mathbb{Z}$

Bemerkung 9.4. $\varphi : R \to S$ Ringhomomorphismus. Dann gilt:
(a) $J \subseteq S$ Ideal $\Rightarrow \varphi^{-1}(J) \subseteq R$ Ideal
(b) $\ker(\varphi) := \{a \in R | \varphi(a) = 0\} \subseteq R$ Ideal
(c) φ injektiv $\Leftrightarrow \ker(\varphi) = \{0\}$
(d) $I \subseteq R$ Ideal und φ surjektiv $\Rightarrow \varphi(I) \subseteq S$ Ideal
(e) $im(\varphi) := \varphi(R)$ ist ein Unterring von S (d.h. ein Ring bzgl. der eingeschränkten Verknüpfung)

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

Bemerkung 9.5. $I \subseteq R$ Ideal
Dann ist durch $r_1 \sim r_2 \Leftrightarrow r_1 - r_2 \in I$ eine Äquivalenzrelation auf R gegeben, welche die zusätzliche Eigenschaft
$r_1 \sim r_2, s_1 \sim s_2 \rightarrow r_1 + s_1 \sim r_2 + s_2, r_1 s_1 \sim r_2 s_2$
hat ("Kongruenzrelation"). Die Äquivalenzklasse von $r \in R$ ist durch $\overline{r} := r + I := \{r + a | a \in I\}$ gegeben und heißt die Restklasse von r modulo I. Die Menge der Restklassen bezeichnen wir mit R/I

Bemerkung 9.6. $I \subseteq R$ Ideal. Dann wird R/I mit der Addition
$+ : R/I \times R/I \rightarrow R/I, \overline{r} + \overline{s} := \overline{r+s}$,
und der Multiplikation
$\cdot : R/I \times R/I \rightarrow R/I, \overline{r} \cdot \overline{s} := \overline{r \cdot s}$
zu einem kommutativen Ring, dem Faktorring (Restklassenring) R/I
Die Abbildung: $\pi : R \rightarrow R/I$, $r \mapsto \overline{r}$ ist ein surjektiver Ringhomomorphismus mit $\ker \pi = I$

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

Beispiel 9.7.
Ist $R = \mathbb{Z}$, $I = n\mathbb{Z}$ mit $n \in \mathbb{N}$, dann erhält man die aus LA1 bekannten Restklassenringe $\mathbb{Z}/n\mathbb{Z}$ (vgl. 6.4)

Satz 9.8. (Homomorphiesatz für Ringe)
$\varphi : R \rightarrow S$ Ringhomomorphismus.
Dann gibt es einen Ringisomorphismus $\underline{\overline{\phi}} : R/\ker(\varphi) \rightarrow im(\varphi)$, $\overline{r} = r + \ker(\varphi) \mapsto \varphi(r)$

Beispiel 9.9. K Körper, $R = K[t]$, $\varphi : K[t] \rightarrow K$, $f \mapsto f(0)$
φ ist Ringhomomorphismus (nachrechnen), $im(\varphi) = K$, $\ker(\varphi) = \{f \in K[t] | f(0) = 0\} = \{tg | g \in K[t]\} = tK[t]$
Wir erhalten einen Ringisomorphismus $\underline{\overline{\phi}} : K[t]/tK[t] \rightarrow K$, $f + tK[t] \mapsto f(0)$

Definition 9.10. $x \in R$ heißt Nullteiler $\Leftrightarrow$ Es existiert ein $y \in R, y \neq 0$ mit $xy = 0$
R heißt nullteilerfrei (Integritätsbereich) $\Leftrightarrow R \neq 0$ und $0 \in R$ ist der einzige Nullteiler in R.

Anmerkung:

- $R \neq 0 \Rightarrow 0$ ist ein Nullteiler in R (wg. $0 \cdot 1 = 0, 0 \neq 1$) (Achtung: unterschiedliche Notation in Literatur)
- Im Nullring ist 0 kein Nullteiler, aber Nullring ist nicht nullteilerfrei

Beispiel 9.11. (a) $\mathbb{Z}$ ist nullteilerfrei
(b) $\overline{2} \in \mathbb{Z}/6\mathbb{Z}$ ist Nullteiler wg $\overline{2} \cdot \overline{3} = \overline{0}$ in $\mathbb{Z}/6\mathbb{Z}$
(c) Analog zu $K[t]$ kann man den Polynomring $R[t]$ erklären. Es gilt dann: R nullteilerfrei $\Rightarrow R[t]$ nullteilerfrei

Bemerkung 9.12. $x \in R$ heißt Einheit $\Leftrightarrow$ Es existiert ein $y \in R$ mit $xy = 1$
$R^* := \{x \in R | x$ ist Einheit$\}$ bildet eine abelsche Gruppe bzgl "$\cdot$"

Beispiel 9.13.
(a) $\mathbb{Z}^* = \{1, -1\}$ denn $1 \cdot 1 = 1, (-1)(-1) = 1$, $ab = 1 \Rightarrow |a||b| = 1 \Rightarrow |a| = |b| = 1$
(b) K Körper $\Rightarrow K^* = K \backslash \{0\}$
(c) $R[t]^* = R^*$ falls R nullteilerfrei (im Allgemeinen nur $R^* \subseteq R[t]^*$)

Definition 9.14. $a_1, \ldots, a_n \in R$, $I \subseteq R$ Ideal
$(a_1, \ldots, a_n) := \{\sum_{i=1}^{n} a_i r_i | r_1, \ldots, r_n \in R\} \subseteq R$ heißt das von $a_1, \ldots, a_n$ erzeugte Ideal.
I heißt Hauptideal $\Leftrightarrow$ Es existiert ein $a \in R$ mit $I = (a) = \{ra | r \in R\} =: Ra$
R heißt Hauptidealring (HIR) $\Leftrightarrow R$ ist nullteilerfrei und jedes Ideal in R ist ein Hauptideal

Anmerkung: $(a_1, \ldots, a_n)$ ist ein Ideal in R (leicht nachzurechnen)

Bemerkung 9.15.
$\mathbb{Z}$ ist ein HIR. Ist $I \subseteq \mathbb{Z}$ ein Ideal, dann existiert ein eindeutig bestimmtes $n \in \mathbb{N}_0$ mit $I = (n) = n\mathbb{Z}$.

Beispiel 9.16. $\mathbb{Z}[t]$ ist kein HIR: Es gibt $f \in \mathbb{Z}[t]$ mit $(2,t) = (f)$, denn:
Angenommen es ex. $f \in \mathbb{Z}[t]$ mit $(f) = (2,t)$, dann existiert $h \in \mathbb{Z}[t]$ mit $2 = hf \Rightarrow \deg(h) = \deg(f) = 0$, d.h. f ist ein konstantes Polynom, etwa $f = a$ für ein $a \in \mathbb{Z}$
Außerdem ex. $\tilde{h} \in \mathbb{Z}[t]$ mit $t = \tilde{h}f = ha \underset{t \text{ normiert}}{\Rightarrow} a = \pm 1 \Rightarrow f = \pm 1$
Aber: $\pm 1 \notin (2,t)$, denn andernfalls ex. $u, v \in \mathbb{Z}[t]$ mit $\pm 1 = 2u + tv \Rightarrow \pm 1 = 2u(0) + 0 \cdot v(0) = 2u(0)$ ↯

Definition 9.17. R nullteilerfrei, $a, b \in R$
b heißt Teiler von a (Notation: $b|a$) $\Leftrightarrow$ Es exisitert ein $c \in R$ mit $a = bc$
a, b heißen assoziiert (Notation $a \widehat{=} b$) $\Leftrightarrow$ $a|b$ und $b|a$

Beispiel 9.18. $R = \mathbb{Z}$, $a \in \mathbb{Z} \Rightarrow a \widehat{=} -a$

Bemerkung 9.19. R nullteilerfrei, $a, b \in R$. Dann sind äquivalent:
(i) $a \widehat{=} b$
(ii) Es existiert ein $e \in R^*$ mit $a = be$
(iii) $(a) = (b)$

Definition 9.20. R nullteilerfrei, $a_1, \ldots, a_n \in R$
$d \in R$ heißt größter gemeinsamer Teiler von $a_1, \ldots, a_n$ $\Leftrightarrow$ Die folgenden Bedingungen sind erfüllt:
(GGT1) $d|a_1, \ldots, d|a_n$
(GGT2) $c|a_1, \ldots, c|a_n \Rightarrow c|d$
Wir bezeichnen die Meinge aller größten gemeinsamen Teiler von $a_1, \ldots, a_n$ mit $GGT(a_1, \ldots, a_n)$

Anmerkung:

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

Bemerkung 9.21. R HIR, $a_1, \ldots, a_n \in R$. Dann gilt:
(a) $GGT(a_1, \ldots, a_n) \neq \emptyset$
(b) $d \in GGT(a_1, \ldots, a_n) \Leftrightarrow (d) = (a_1, \ldots, a_n)$

Anmerkung:

- Im Fall $R = \mathbb{Z}$, $a_1, \ldots, a_n \in \mathbb{Z}$ ist $GGT(a_1, \ldots, a_n) \cap \mathbb{N}_0 = \{d\}$ für ein $d \in \mathbb{N}_0$ (beachte: $\mathbb{Z}^* = \{\pm 1\}$). Man nennt dann d den größten gemeinsamen Teiler von $a_1, \ldots, a_n$: $d =: ggT(a_1, \ldots, a_n)$
- Im Fall $R = K[t]$ (wobei K Körper in Section 10: dies ist ein HIR), $f_1, \ldots, f_n \in K[t]$, nicht alle $f_i = 0$, existiert ein eindeutig bestimmtes normiertes Polynom $d \in K[t]$ mit $d \in GGT(f_1, \ldots, f_n)$ (beachte: $K[t]^* = K^*$). Man nennt $d =: ggT(f_1, \ldots, f_n)$ den größten gemeinsament Teiler von $f_1, \ldots, f_n$ und setzt $ggT(0, \ldots, 0) := 0$

Folgerung 9.22. *R HIR, $a, b \in R$, $d \in GGT(a, b)$*
Dann existieren $u, v \in R$ mit $d = ua + vb$

Definition 9.23. R nullteilerfrei, $p \in R \backslash (R^* \cup \{0\})$
p heißt irreduzibel $\Leftrightarrow$ Aus $p = ab$ mit $a, b \in R$ folgt stets $a \in R^*$ oder $b \in R^*$
p heißt Primelement $\Leftrightarrow$ Aus $p|ab$ folgt stets $p|a$ oder $p|b$

Anmerkung: p irreduzibel/Primelement, $p' \hat{=} p \Rightarrow p'$ irreduzibel/Primelement

Beispiel 9.24. irreduzible Elemente in $\mathbb{Z}$ = Primzahlen p aus $\mathbb{N}$ sowie deren Negative $-p$.
Primelemente in $\mathbb{Z}$?

Frage: Zusammenhang zwischen irreduziblen Elementen und Primelementen?

Bemerkung 9.25. R nullteilerfrei, $p \in R \backslash (R^* \cup \{0\})$ Primelement
Dann ist p irreduzibel

Anmerkung: Es gibt Beispiele für irreduzible Elemente, die keine Primelemente sind

Satz 9.26. R HIR, $p \in R \backslash (R^* \cup \{0\})$. Dann sind äquivalent:
(i) p ist irreduzibel
(ii) p ist Primelement

Anmerkung:

- Beweis hat gezeigt: R HIR, 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 eindeutig bestimmte Primfaktorzerlegung aus $\mathbb{Z}$?

Definition 9.27. R nullteilerfrei
R heißt faktoriell $\Leftrightarrow$ Jedes $a \in R \backslash (R^* \cup \{0\})$ lässt sich eindeutig bis auf Reihenfolge und Assoziiertheit als Produkt irreduzibler Elemente aus R schreiben, d.h. es exisiteren irreduzible Elemente $p_1, \dots, p_r \in R$ mit $a = p_1 \cdot \ldots \cdot p_r$ und sind $q_1, \dots, q_s \in R$ irreduzible Elemente mit $a = q_1 \cdot \ldots \cdot q_s$, so ist $r = s$ und nach Umnummerierung ist $p_i \hat{=} q_i$ für $i = 1, \dots, r$

Ziel: HIR sind faktoriell

Definition 9.28. R heißt noethersch $\Leftrightarrow$ Für jede aufsteigende Kette $I_1 \subseteq I_2 \subseteq \ldots$ von Idealen in R existiert ein $n \in \mathbb{N}$ mit $I_k = I_n$ für alle $k \geq n$

Bemerkung 9.29. R HIR. Dann ist R noethersch

Satz 9.30. R HIR. Dann ist R faktoriell

Anmerkung:

- Fasst man in einer Zerlegung eines Elementes zueinander assoziierte Faktoren zusammen und erlaubt einen Vorfaktor $c \in R^*$, so erhält man eine Darstellung für Elemente $a \in R \backslash (R^* \cup \{0\})$ der Form $a = c p_1^{e_1} \cdot \ldots p_r^{e_r}$ mit $c \in R^*$, $p_1, \dots, p_r$ irreduzibel, $p_i \hat{\neq} p_j$ für $i \neq j$, $e_1, \dots, e_r \in \mathbb{N}$.
  Ist dann $a = d q_1^{f_1} \cdot \ldots \cdot q_s^{f_s}$ mit $d \in R^*$, $q_1, \dots, q_s$ irreduzibel, $q_i \hat{\neq} q_j$, für $i \neq j$, $f_1, \dots, f_s \in \mathbb{N}$, dann ist $r = s$ und nach Umnummerierung ist $p_i \hat{=} q_i$, $e_i = f_i$ für $i = 1, \dots, r$

10. Euklidische Ringe

In diesem Abschnitt sei R stets ein kommutativer Ring

Definition 10.1. R nullteilerfrei
R heißt ein Euklidischer Ring $\Leftrightarrow$ Es existiert eine Abbildung $\delta : R\backslash\{0\} \to \mathbb{N}_0$, sodass gilt: Für alle $f, g \in R$, $g \neq 0$ existieren $q, r \in R$ mit $f = qg + r$ und ($\delta(r) < \delta(g)$ oder $r = 0$)
δ heißt eine Normabbildung auf R

Beispiel 10.2.
(a) $R = \mathbb{Z}$ mit $\delta = |.|$ ist ein euklidischer Ring (vgl. EZT- Skript, Satz 1.3)
(b) K Körper $\Rightarrow R = K[t]$ mit $\delta = \deg$ ist ein euklidischer Ring (vgl. 7.6) (c) $R = \mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{C}\} \in \mathbb{C}$ mit $\delta(x + iy) = x^2 + y^2$ ist ein euklidischer Ring (Ring der ganzen Gaußschen Zahlen)
(d) K Körper mit $\delta : K\backslash\{0\} \to \mathbb{N}_0, x \mapsto 1$ ist ein euklidischer Ring (Hier ist stets "$r = 0$")

Satz 10.3. R Euklidischer Ring. Dann ist R ein HIR

Folgerung 10.4. R euklidischer Ring. Dann ist R faktoriell

Folgerung 10.5. K Körper, $f \in K[t], f \neq 0$
Dann besitzt f eine bis auf Reihenfolge der Faktoren eindeutige Darstellung $f = cp_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ mit $c \in K^*$, $r \geq 0$, $e_1, \ldots, e_r \in \mathbb{N}_0$ und paarweise verschiedene normierte irreduzible Polynome $p_1, \ldots, p_r$

Satz 10.6. (Euklidischer Algorithmus) R euklidischer Ring mit Normabbildung $\delta, a, b \in R\backslash\{0\}$
Wir betrachten eine Folge $a_0, a_1, ...$ von Elementen aus R, die induktiv wie folgt gegeben ist:
$a_0 := a$
$a_1 := b$
$a_0 = q_0 a_1 + a_2$ mit $\delta(a_2) < \delta(a_1)$ oder $a_2 = 0$

Falls $a_2 \neq 0$: $a_1 = q_1 a_2 + a_3$ mit $\delta(a_3) < \delta(a_2)$ oder $a_3 = 0$

Falls $a_i \neq 0$: $a_{i-1} = q a_i + a_{i+1}$ mit $\delta(a_{i+1}) < \delta(a_i)$ 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 $d := a_n \in GGT(a, b)$
Durch Rückwärtseinsetzen lässt sich d als Linearkombination von a, b darstellen (vgl. 8.22):
$d = a_n = a_{n-2} - q_{n-2} a_{n-1} = \ldots = ua + vb$ mit $u, v \in R$ ("erweiterter euklidsicher Algorithmus")

Beispiel 10.7. $R = \mathbb{Z}$, $a = 24$, $b = 15$
$24 = 1 \cdot 15 + 9$
$15 = 1 \cdot 9 + 6$
$9 = 1 \cdot 6 + 3$
$6 = 2 \cdot 3 + 0$
$\Rightarrow ggT(24, 15) = 3$
$3 = 9 - 1 \cdot 6 = 9 - (15 - 1 \cdot 9) = 2 \cdot 9 - 1 \cdot 15 = 2(24 - 1 \cdot 15) - 15 = 2 \cdot 24 - 3 \cdot 15$

Anmerkung: Für Matrizen aus $M(m \times n, R)$ kann man analog zu LA1 (vgl. 10.5) elementare Zeilen- und Spaltenoperationen erklären.

Satz 10.8. (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 Spaltenumformungen vom Typ III (Addition des λ-fachen einer Zeile/Spalte zu einer anderen Zeile/Spalte), sowie des Typs II (Zeilen/Spaltenvertauschung) in eine Matrix der Gesalt:

$$\left(\begin{array}{cccc|c} c_1 & & & & \\ & c_2 & & & 0 \\ & & \ddots & & \\ & & & c_r & \\ \hline 0 & & & & 0 \end{array}\right) \text{ mit } c_1, \ldots, c_r \in R \setminus \{0\},\ c_1 | c_2 | \ldots | c_r \text{ überführen}$$

Beweis. (= Algorithmus zur Durchführung)
Falls $A = 0$, dann fertig. Im Folgenden sei $A \neq 0$. Sei δ eine Normabbildung auf R

1.Schritt: Durch Zeilen- und Spaltenvertauschungen erreichen wir $a_{11} \neq 0$ und $\delta(a_{11}) \leq \delta(a_{ij})$ für alle i, j mit $a_{ij} \neq 0$

2.Schritt: Bringe A auf die Form $\left(\begin{array}{c|c} * & 0 \\ \hline 0 & * \end{array}\right)$

1. Fall: In der ersten Spalte/Zeile stehen keine Elemente $\neq 0$ außer $a_1 1$; dann fertig
2. Fall: In der ersten Spalte/Zeile stehen noch Elemente $\neq 0$, oE $a_{21} \neq 0$
$\Rightarrow$ Es existiert ein $q \in R$ mit $a_{21} = qa_{11}$ oder $\delta(a_{21} - qa_{11}) < \delta(a_{11})$ (*)
Addiere das $(-q)$-fache der 1. Zeile zur 2. Zeile
$\Rightarrow$ Erhalte Matrix $A' = (a'_{ij})$ mit $a'_{21} = 0$ oder $\delta(a'_{21}) < \delta(a_{11})$
erhalte durch Zeilen sowie ggf. Spaltenvertauschungen 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 $\delta(a''_{11}) \leq (a_{11})$ (”<”,falls Division in (*) nicht aufgegangen)
Dieser Prozess bricht nach endlich vielen Iterationen ab, und wir erhalten eine Matrix der Form

$$D = (d_{ij}) \left(\begin{array}{c|c} d_{11} & 0 \\ \hline 0 & * \end{array}\right) \quad d_{11} \neq 0, \delta(d_{11}) \leq \delta(d_{ij}) \text{ falls } d_{ij} \neq 0\ \delta(d_{11}) \leq \delta(a_{11})$$

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

$$\begin{array}{rc} \text{i-te Zeile} \rightarrow & \left(\begin{array}{c|ccccc} d_{11} & 0 & \dots & \dots & \dots & 0 \\ \hline 0 & & & & & \\ \vdots & & & * & & \\ d_{11} & d_{i2} & \dots & d_{ij} & \dots & d_{in} \\ 0 & & & & & \\ \vdots & & & * & & \\ 0 & & & & & \end{array}\right) \\ & \hookleftarrow \text{ j-te Zeile} \end{array}$$

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

$$D' = (d'_{ij}) = \left(\begin{array}{c|ccccccc} d_{11} & 0 & \dots & 0 & -qd_{11} & 0 & \dots & 0 \\ \hline 0 & & & & & & & \\ \vdots & & & & * & & & \\ 0 & & & & & & & \\ d_{11} & & * & & d_{ij} - qd_{11} & & * & \\ 0 & & & & & & & \\ \vdots & & & & * & & & \\ 0 & & & & & & & \end{array}\right) \text{mit } d'_{ij} = d_{ij} - qd_{11},\, \delta(d'_{ij}) < \delta(d_{11}) \leq d_{(}a_{11})$$

Wiederhole die gesamte bisherige Prozedur für die Matrix D'. Dieser Prozess bricht nach endlich vielen Schnitten ab. Wir erhalten eine Matrix

$$C = (c_{ij}) = \left(\begin{array}{c|c} c_{11} & 0 \\ \hline & \\ C' & * \\ & \end{array}\right) c_{11} \neq 0, \delta(c_{11}) \leq \delta(a_{11}),\, c_{11}|c_{ij} \text{ für alle } i, j$$

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

$$\left(\begin{array}{ccc|c} c_1 & & & \\ & \ddots & 0 & 0 \\ 0 & & c_r & \\ \hline 0 & & 0 & 0 \end{array}\right) \text{mit } c_1|c_2|c_3|\dots|c_r$$

bringen. □

Beispiel 10.9.
(a) $R = \mathbb{Z}$ mit $\delta = |.|$:

$$A = \begin{pmatrix} 4 & 3 \\ 6 & 5 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 3 & 4 \\ 5 & 6 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 3 & 1 \\ 5 & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 3 \\ 1 & 5 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

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

$$A = \begin{pmatrix} t-1 & 0 \\ -1 & t-1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -1 & t-1 \\ t-1 & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -1 & t-1 \\ 0 & (t-1)^2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -1 & 0 \\ 0 & (t-1)^2 \end{pmatrix}$$

Anmerkung: Wir haben bei der Gauß-Diagonalisierung nur elementare Operatoren vom Typ III, IV verwendet. Umformungen vom Typ I (Multiplikation von einer Zeile/Spalte mit $\lambda \in R^*$) sowie Typ II (Addition einer Zeile/-Spalte auf eine andere Zeile oder Spalte) sind auch erlaubt.

Frage Eindeutigkeitsaussage für $c_1, \dots, c_r$?

Bemerkung 10.10. $Gl(n,R) := \{A \in M(n \times n, R) |$ Es existiert ein $B \in M(n \times n, R)$ mit $AB = BA = E_n\}$ ist eine Gruppe bzgl "$\cdot$", die allgemeine lineare Gruppe über R vom Rang n.
Es ist $Gl(n,R) = \{A \in M(n \times n, R) | \det(A) \in R^*\}$

Bemerkung 10.11. $A, B \in M(m \times n, R)$
A heißt äquivalent zu B ($A \sim B$) $\Leftrightarrow$ Es existiert ein $S \in Gl(m,R), T \in Gl(n,R)$ mit $B = SAT^{-1}$
Falls $m = n$, dann heißt A ähnlich zu B ($A \approx B$) $\Leftrightarrow$ Es existiert ein $S \in Gl(n,R)$ mit $B = SAS^{-1}$
$\sim, \approx$ sind Äquivalenzrelationen auf $M(m \times n, R)$ bzw. $M(n \times n, R)$

Erinnerung: In LA1 gezeigt (vgl. 16.11): K Körper, $A, B \in M(m \times n, K)$
Dann gilt: $A \sim B \Leftrightarrow Rang(A) = Rang(B)$
Ist $Rang(A) = r$, 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 10.12. $A \in M(m \times n, R)$, $1 \leq k \leq m$, $1 \leq l \leq n$
$B \in M(k \times l, R)$ heißt eine Untermatrix von $A \Leftrightarrow B$ 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.
$Fit_l(A) = (\det(B) | B$ ist $l \times l$- 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 10.13. $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in M(2 \times 2, \mathbb{Z})$
$Fit_1(A) = (\det(1), \det(2), \det(3), \det(4)) = (1,2,3,4) = (1) = \mathbb{Z}$
$Fit_2(A) = (\det \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}) = (-2) = (2)$

Satz 10.14. (Fittings Lemma) $A \in M(m \times n, R)$, $S \in Gl(m,R)$, $T \in Gl(n,R)$, $l \leq min\{m,n\}$
Dann gilt: $Fit_l(A) = Fit_l(SA) = Fit_l(AT)$

Folgerung 10.15. $A, B \in M(m \times n, R)$ mit $A \sim B$
Dann gilt: $Fit_l(A) = Fit_l(B)$ für alle $1 \leq l \leq min\{m,n\}$

Bemerkung 10.16. R nullteilerfreier Ring, $A = \left(\begin{array}{ccc|c} c_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & c_r & \\ \hline & 0 & & 0 \end{array}\right)$ mit $c_1 | \dots | c_r$

Dann gilt: $Fit_l(A) = \begin{cases} (c_1 \cdot \dots \cdot c_l), & \text{falls } 1 \leq l \leq r \\ (0), & \text{sonst} \end{cases}$
Insbesondere gilt: $Fit_r(A) \subseteq Fit_{r-1}(A) \subseteq \dots \subseteq Fit_1(A)$

Satz 10.17. (Elementarteilersatz über euklidischen Ringen)
R Euklidischer Ring, $A \in M(m \times n, R)$
Dann existieren $c_1, \ldots, c_r \in R \backslash \{0\}$ mit $c_1 | c_2 | \ldots | c_r$, sodass

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

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

Satz 10.18. R euklidischer Ring, $A, B \in M(m \times n, R)$. Dann sind äquivalent:
(i) $A \sim B$
(ii) Die Elementarteiler von A und B stimmen bis auf Assoziiertheit überein.
(iii) $Fit_l(A) = Fit_l(B)$ für alle $1 \leq l \leq min\{m, n\}$

Beispiel 10.19. $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in M(2 \times 2, \mathbb{Z}) \overset{10.13}{\Rightarrow} Fit_1(A) = (1), Fit_2(A) = (2)$

$\Rightarrow$ Elementarteiler von A: $1, 2$, insbesondere $A \sim \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$

Sei $B = \begin{pmatrix} 4 & 3 \\ 2 & 2 \end{pmatrix} \in M(2 \times 2, \mathbb{Z}) \Rightarrow Fit_1(B) = (2, 3, 4) = (1)$, $Fit_2(B) = (2) \overset{10.18}{\Rightarrow} A \sim B$

11. 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 bzgl. "$\approx$" ($\rightsquigarrow$ Normalformen)
- In Termen von Endomorphismen: Gegeben sei $\varphi \in End(V)$, V endlichdimensionaler K-Vektorraum. Wir suchen Basis B von V, sodass $M_B(\varphi)$ möglichst einfach ist.

Definition 11.1. $A \in M(n \times n, K)$
$P_A := tE_n - A \in M(n \times n, K[t])$ heißt die charakteristische Matrix von A.

Anmerkung: Insbesondere ist $\chi_A^{char} = \det(P_A)$

Satz 11.2. (Satz von Frobenius)
$A, B \in M(n \times n, K)$. Dann sind äquivalent:
(i) $A \approx B$ (in $M(n \times n, K)$)
(ii) $P_A \sim P_B$ (in $M(n \times n, K[t])$)

Bemerkung 11.3. $A \in M(n \times n, K)$. Dann gilt:
(a) Es gibt eindeutig bestimmte normierte Polynome $c_1(A), \dots, c_n(A) \in K[t]$ mit

$$P_A \sim \begin{pmatrix} c_1(A) & & 0 \\ & \ddots & \\ 0 & & c_n(A) \end{pmatrix}, c_1(A)|c_2(A)|\dots|c_n(A)$$

$c_1(A), \dots, c_n(A)$ heißen die Invariantenteiler von A.

(b) Es gibt eindeutig bestimmte normierte Polynome $d_1(A), \dots, d_n(A) \in K[t]$ mit
$Fit_l(P_A) = (d_l(A))$ für $l = 1, \dots, n$
Es ist $d_l(A) = ggT(\det(B)|B$ ist $l \times l$-Untermatrix von $P_A)$
Insbesondere ist $d_n(A) = \chi_A^{char}$
$d_1(A), \dots, d_n(A)$ heißen die Determinantenteiler von A

Anmerkung: Also: Invariantenteiler von A = normierte Elementarteiler von P_A
Determinantenteiler von A = normierte Erzeuger der Fittingideale von P_A

Folgerung 11.4. $A \in M(n \times n, K)$
Dann gilt: $d_l(A) = c_1(A) \cdot \ldots \cdot c_l(A)$ für alle $l = 1, \dots, n$
Inbesondere gilt: $\chi_A^{char} = d_n(A) = c_1(A) \cdot \ldots \cdot c_n(A)$ sowie $d_1(A)|\dots|d_n(A)$

Satz 11.5. (Invariantenteilersatz)
$A, B \in M(n \times n, K)$
Dann sind äquivalent:
(i) $A \approx B$
(ii) Die Invariantenteiler von A stimmen mit den Invariantenteilern von B überein: $c_1(A) = c_1(B), \dots, c_n(A) = c_n(B)$
(iii) Die Determinantenteiler von A stimmen mit den Determinantenteilern von B überein:
$d_1(A) = d_1(B), \dots, d_n(A) = d_n(B)$

Beispiel 11.6.

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

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

Bestimmen der Determinantenteiler von A: $d_1(A) = ggT(-1, \ldots) = 1$

$d_2(A) = ggT((-1) \cdot 4 - (-3)(t-1), (-3)(-1) - 2(t-1), \ldots) = ggT(3t-7, -2t+5, \ldots) = 1$

$d_3(A) = \chi_A^{char} = (t-2)^3$

$\Rightarrow c_1(A) = 1$, $c_2(A) = 1$, $c_3(A) = (t-2)^3$

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

Bestimmen der Invariantenteiler von B:

$$P_B = \begin{pmatrix} t-1 & -1 & -2 \\ -1 & t-1 & 2 \\ 1 & -1 & t-4 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -1 & t-1 & 2 \\ t-1 & -1 & -2 \\ 1 & -1 & t-4 \end{pmatrix}$$

$$\rightsquigarrow \begin{pmatrix} -1 & t-1 & 2 \\ 0 & (t-1)^2-1 & -2+2(t-1) \\ 0 & t-2 & t-2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -1 & 0 & 0 \\ 0 & t^2-2t & 2t-4 \\ 0 & t-2 & t-2 \end{pmatrix}$$

$$\rightsquigarrow \begin{pmatrix} -1 & 0 & 0 \\ 0 & t-2 & t-2 \\ 0 & t^2-2t & 2t-4 \end{pmatrix} \rightsquigarrow \begin{pmatrix} -1 & 0 & 0 \\ 0 & t-2 & 0 \\ 0 & t^2-2t & -t^2+4t-4 \end{pmatrix}$$

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

$\Rightarrow c_1(B) = 1, c_2(B) = t-2, c_3(B) = (t-2)^2$

$d_1(B) = 1, d_2(B) = t-2, d_3(B) = (t-2)^3$

$\Rightarrow A \not\approx B$

Bemerkung 11.7. $A, B \in M(n \times n, K)$, K Teilkörper eines Körpers L. Dann sind äquivalent:

(i) $A \approx B$ in $M(n \times n, K)$

(ii) $A \approx B$ in $M(n \times n, L)$

Ziel: Suche möglichst einfache Matrizen, die vorgebene Invarianten- bzw. Determinantenteiler haben.

Definition 11.8. $g = t^n + a_{n-1} * t^{n-1} + \ldots + a_1 * t + a_0 \in K[t]$, $n \geq 1$

$$B_g = \begin{pmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & -a_{n-2} \\ & & & 1 & -a_{n-1} \end{pmatrix} \in M(n \times n, K) \text{ (für } n = 1 : B_g = (-a_0))$$

heißt die Begleitmatrix zu g.

Bemerkung 11.9. $g \in K[t]$ nichtkonstant, normiert
Dann ist $c_1(B_g) = \ldots = c_{n-1}(B_g) = 1$, $c_n(B_g) = g$, also

$$P_{B_g} \sim \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & g \end{pmatrix},$$

$d_1(B_g) = \ldots = d_{n-1}(B_g) = 1$, $d_n(B_g) = \chi^{char}_{B_g} = g$

Bemerkung 11.10. $g_1, \ldots, g_r \in K[t]$ normiert, nichtkonstant mit $g_1|g_2|\ldots|g_r$,
$n := \deg(g_1) + \ldots + \deg(g_r)$

$$B_{g_1,\ldots,g_r} := \begin{pmatrix} B_{g_1} & & & \\ & B_{g_2} & & \\ & & \ddots & \\ & & & B_{g_r} \end{pmatrix} \in M(n \times n, K)$$

Dann gilt: $c_1(B_{g_1,\ldots,g_r}) = 1, \ldots, c_{n-r}(B_{g_1,\ldots,g_r}) = 1$,
$c_{n-r+1}(B_{g_1,\ldots,g_r}) = g_1, \ldots, c_n(B_{g_1,\ldots,g_r}) = g_r$

Satz 11.11. (Frobenius-Normalform $A \in M(n \times n, K)$
Dann existiert eindeutig bestimmte $r \in \mathbb{N}$ sowie eindeutg bestimmte normierte nichtkonstante Polynome $g_1, \ldots, g_r \in K[t]$ mit $g_1|\ldots|g_r$ und
$A \approx B_{g_1,\ldots,g_r}$
$g_1, \ldots g_r$ sind genau die nichtkonstanten Invariantenteiler von A.
$B_{g_1,\ldots,g_r}$ heißt die Frobenius-Normalform (FNF) von A.

Beispiel 11.12. (vgl. 11.6)
(a) $A = \begin{pmatrix} 0 & 1 & 3 \\ 3 & 1 & -4 \\ -2 & 1 & 5 \end{pmatrix} \in M(3 \times 3, \mathbb{Q})$
$\Rightarrow c_1(A) = 1$, $c_2(A) = 1$, $c_3(A) = (t-2)^3 = t^3 - 6t^2 + 12t - 8 =: g_1$
$\Rightarrow A \approx B_{g_1} = \begin{pmatrix} 0 & 0 & 8 \\ 1 & 0 & -12 \\ 0 & 1 & 6 \end{pmatrix}$ (FNF von A)
(b) $A = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 1 & -2 \\ -1 & 1 & 4 \end{pmatrix} \in M(3 \times 3, \mathbb{Q})$
$\Rightarrow c_1(A) = 1$, $c_2(A) = t - 2 =: g_1$, $c_3(A) = (t-2)2 = t^2 - 4t + 4 =: g_2$
$\Rightarrow A \approx B_{g_1,g_2} = \left(\begin{array}{c|cc} 2 & 0 & 0 \\ \hline 0 & 0 & -4 \\ 0 & 1 & 4 \end{array}\right)$ (FNF von A)
(c) $\begin{pmatrix} 4 & -1 & -2 & 3 \\ -1 & 5 & 2 & -4 \\ 0 & 1 & 3 & -1 \\ -1 & 2 & 2 & 1 \end{pmatrix} \in M(4 \times 4, \mathbb{Q})$
$\Rightarrow c_1(A) = 1, c_2(A) = 1, c_3(A) = t - 3 =: g_1$, $c_4(A) = (t-3)^2(t-2) = t^3 - 8t^2 + 21t - 18 =: g_2$
$A \approx B_{g_1,g_2} = \left(\begin{array}{c|ccc} 3 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 18 \\ 0 & 1 & 0 & -21 \\ 0 & 0 & 1 & 8 \end{array}\right)$ (FNF von A)

Bemerkung 11.13. $A \in M(n \times n, K)$. Dann ist $c_n(A) = \chi_A^{min}$

Bemerkung 11.14. $g \in K[t]$, $g = h_1 \cdot \ldots \cdot h_k$ mit $h_1, \ldots, h_k \in K[t]$ normiert, nicht konstant, paarweise teilerfremd

$$\Rightarrow B_g \approx \begin{pmatrix} B_{h_1} & & \\ & \ddots & \\ & & B_{h_k} \end{pmatrix}$$

Satz 11.15. (Weierstrass-Normalform) $A \in M(n \times n, K)$

Dann existieren eindeutig bestimmte $m \in \mathbb{N}$, Polynome $h_1, \ldots, h_m \in K[t]$, die Potenzen von irreduziblen normierten Polynomen sind, sodass:

$A \approx B_{h_1,\ldots,h_m}$

$h_1, \ldots, h_m$ heißt eine Weierstrass-Normalform von A (WNF).

$h_1, \ldots, h_m$ sind die Potenzen irreduzibler Polynome, die in den Primfaktorzerlegungen nicht konstanter Invarianteiler von A auftauchen.

Beispiel 11.16.

(a) $A = \begin{pmatrix} -2 & 1 & 5 \\ 1 & 1 & -2 \\ 3 & 1 & 6 \end{pmatrix} \in M(3 \times 3, \mathbb{Q})$

$\Rightarrow c_1(A) = 1$, $c_2(A) = 1$, $c_3(A) = (t-1)(t-2)^2$

Mit $h_1 = t - 1$, $h_2 = (t-2)^2 = t^2 - 4t + 4$ ist

$A \approx B_{h_1,h_2} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -4 \\ 0 & 1 & 4 \end{pmatrix}$ (WNF von A)

(b) (vgl 11.12(c))

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

$\Rightarrow c_1(A) = 1$, $c_2(A) = 1$, $c_3(A) = t - 3$, $c_4(A) = (t-3)^2(t-2)$

Mit $h_1 := t - 3$, $h_2 := (t-3)^2$, $h_3 := t - 2$ ist $= t^2 - 6t + 9$

$A \approx B_{h_1,h_2,h_3} = \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 0 & -9 & 0 \\ 0 & 1 & 6 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$ (WNF von A)

Ziel: Einfache Normalform, falls χ_A^{char} in Linearfaktoren zerfällt (und damit alle Weierstrassteiler Potenzen lineare Polynome sind.)

Bemerkung 11.17. $\lambda \in K$, $f = (t - \lambda)^e \in K[t]$. Dann gilt:

$$B_f \approx \begin{pmatrix} \lambda & & & 0 \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ 0 & & 1 & \lambda \end{pmatrix} =: J(\lambda, e) \in M(e \times e, K) \; (e = 1 : J(\lambda, 1) = (\lambda))$$

Eine Matrix der Form $J(\lambda, e)$ heißt Jordanmatrix über K

Satz 11.18. (Jordansche Normalform)
$A \in M(n \times n, K)$, χ_A^{char} zerfällt in $K[t]$ in Linearfaktoren
Dann existieren Jordanmatrizen $J_1 = J(\lambda_1, e_1), \ldots, J_m = J)\lambda_m, e_m)$ über K, sodass

$$A \approx \begin{pmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_m \end{pmatrix} =: J$$

Hierbei sind $\lambda_1, \ldots, \lambda_m$ die (nicht notwendig paarweise verschiedenen) EW von$A$ (= NS von χ_A^{char})
$J_1, \ldots, J_m$ sind bis auf Reihenfolge eindeutig bestimmt.
Die Matrix J heißt eine Jordansche Normalform (JNF) von A.

Anmerkung:

- Üblicherweise gruppiert man in der JNF Jordanmatrizen zu gleichen EW zusammen (zu einem Block mit aufsteigenden e'is)
- Es gilt: A diagonalisierbar $\Leftrightarrow$ JNF A ist eine Diagonalmatrix (denn: $'' \Leftarrow ''$ trivial $'' \Rightarrow ''$ da Diagonalmatrizen bereits in JNF sind (mit 1×1-Jordanmatrizen))

Satz 11.19. (Algorithmus zur JNF)
Eingabe: $A \in M(n \times n, K)$, sodass χ_A^{char} in Linearfaktoren zerfällt
Ausgabe: JNF von A
Durchführung:

1. Bestimme die nicht-konstanten Invariantenteiler $g_1, \ldots, g_r$ von A
2. Bestimme die Primfaktorzerlegung $g_i = (t - \lambda_{i,1})^{m_{i,1}} \cdot \ldots \cdot (t - \lambda_{i,k_i})^{m_{i,k_i}}$, $i = 1, \ldots, r$
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 EWen zusammen (jeweils nach aufsteigender Größe geordnet)

Beispiel 11.20.

(a) (vgl. 28.16 (b)) $A = \begin{pmatrix} 4 & -1 & -2 & 3 \\ -1 & 5 & 2 & -4 \\ 0 & 1 & 3 & -1 \\ -1 & 2 & 2 & 1 \end{pmatrix} \in M(4 \times 4, \mathbb{Q})$

$\Rightarrow c_1(A) = 1, c_2(A) = 1, c_3(A) = t-3 =: g_1, c_4(A) = (t-3)^2(t-2) =: g_2$

Weierstrassteiler von A: $h_1 := t-3$, $h_2 := (t-3)^2$, $h_3 := t-2$

$$\Rightarrow A \approx B_{h_1,h_2,h_3} = \begin{pmatrix} B_{h_1} & & \\ & B_{h_2} & \\ & & B_{h_3} \end{pmatrix} \approx \begin{pmatrix} J(3,1) & & \\ & J(3,2) & \\ & & J(2,1) \end{pmatrix} = \begin{pmatrix} 3 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 1 & 3 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$$

(b) (vgl. 28.6)

$A = \begin{pmatrix} 0 & 1 & 3 \\ 3 & 1 & -4 \\ -2 & 1 & 5 \end{pmatrix} \in M(3 \times 3, \mathbb{Q}) \Rightarrow c_1(A) = 1, c_2(A) = 1, c_3(A) = (t-2)^3$

$\Rightarrow$ Weierstrassteiler von A: $h_1 = (t-2)^3$

$$\Rightarrow A \approx B_{h_1} \approx J(2,3) = \begin{pmatrix} 2 & 0 & 0 \\ 1 & 2 & 0 \\ 0 & 1 & 2 \end{pmatrix}$$

(c) $A = \begin{pmatrix} 1 & 1 & 2 \\ 1 & 1 & -2 \\ -1 & 1 & 4 \end{pmatrix} \in M(3 \times 3, \mathbb{Q}) \Rightarrow c_1(A) = 1, c_2(A) = t-2, c_3(A) = (t-2)^2$

$\Rightarrow$ Weierstrassteiler von A: $h_1 = t-2$, $h_2 = (t-2)^2$

$$\Rightarrow A \approx B_{h_1,h_2} = \begin{pmatrix} B_{h_1} & \\ & B_{h_2} \end{pmatrix} \approx \begin{pmatrix} J(2,1) & \\ & J(2,2) \end{pmatrix} = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 1 & 2 \end{pmatrix}$$

12. Moduln

In diesem Abschnitt sei R stets ein kommutativer Ring.

Definition 12.1. Eine Menge M zusammen mit einer Verknüpfung
$+ : M \times M \to M$, $(x,y) \mapsto x+y$ (genannt Addition)
und einer äußeren Verknüpfung
$\cdot : R \times M \to M$, $(a,x) \mapsto ax$ (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:

- $(a+b)x = ax+bx$
- $a(x+y) = ax+ay$
- $(ab)x = a(bx)$
- $1 \cdot x = x$

für alle $a,b \in R$, $x,y \in M$

Beispiel 12.2.
(a) K Körper, V K-VR $\Rightarrow V$ ist ein K-Modul
(b) $(G,+)$ abelsche Gruppe wird zum $\mathbb{Z}$-Modul durch

$$\mathbb{Z}\times G\to G,\ (n,g)\mapsto \begin{cases}\underbrace{g+\ldots+g}_{n\text{-mal}}, & \text{falls } n\in\mathbb{N}\\ 0, & \text{falls } n=0\\ -(\underbrace{g+\ldots+g}_{-n-mal}), & \text{falls } -n\in\mathbb{N}\end{cases}$$

Umgekehrt ist jeder $\mathbb{Z}$-Modul eine abelsche Gruppe bzgl "+"
(c) $I\subseteq R$ Ideal $\Rightarrow I$ ist ein R-Modul
(Addition: auf I eingeschränkte Addition von R, skalare Mult.: $R\times I$, $(a,x)\mapsto ax$)
Insbesondere ist R ein R-Modul
(d) $I\subseteq R$ Ideal $\Rightarrow R/I$ ist ein R-Modul (skalare Mult.: $R\times R/I\to R/I$, $(a,\overline{x})\mapsto\overline{ax}$)
(e) K Körper, V K-VR, $\varphi\in End(V)\Rightarrow V$ ist $K[t]$-Modul via skalare Mult: $K[t]\times V\to V$, $(f,v)\mapsto f(\varphi)(v)$

Definition 12.3. M,N R-Moduln. $\varphi: M\to N$
φ heißt (R-Modul)-Homomorphismus $\Leftrightarrow$ Für alle $x,y\in M$, $a\in R$ gilt:
$\varphi(x+y)=\varphi(x)+\varphi(y)$, $\varphi(ax)=a\varphi(x)$
φ heißt (R-Modul)-Isomorphismus $\Leftrightarrow$ φ ist ein bijektiver R-Modul-Homomorphismus.
Existiert ein Isomorphismus zwischen M,N, so schreiben wir $M\cong N$.

Definition 12.4. M R-Modul, $N\subseteq M$
N heißt Untermodul von $N\Leftrightarrow$ Folgende Bedingungen sind erfüllt:
(U1) $0\in N$
(U2) $x,y\in N\Rightarrow x+y\in N$
(U3) $a\in R, x\in N\Rightarrow ax\in N$

Beispiel 12.5.
(a) K Körper, V K-VR $\Rightarrow$ Untermoduln von V = UVR von V
(b) $M=R$ als R-Modul $\Rightarrow$ Untermodul von M = Ideale in R

Bemerkung 12.6. M R-Modul, $N\subseteq M$ Untermodul
Dann gilt: Durch $x\sim y\Leftrightarrow x-y\in N$ ist eine Äquivalenzrelation auf M definiert.
Die Äquivalenzklasse $\overline{x}$ von $x\in M$ ist gegeben durch
$\overline{x}=x+N=\{x+y|y\in N\}$
Die Menge aller Äquivalenzklassen bezeichnen wir mit M/N
M/N wird mit den Verknüpfungen
$+: M/N\times M/N\to M/N, \overline{x}+\overline{y}:=\overline{x+y}$,
$\cdot: R\times M/N\to, a\cdot\overline{x}:=\overline{ax}$
zu einem R-Modul, dem Faktormodul M/N
Die kanonische Projektion $\pi: M\to M/N$, $x\mapsto\overline{x}$ ist ein surjektiver R-Modulhomomorphismus

Bemerkung 12.7. M,N R-Moduln, $\varphi: M\to N$ Homomorphismus. Dann gilt:
(a) $\ker(\varphi):=\{x\in M|\varphi(x)=0\}$ ist ein Untermodul von M
(b) φ ist injektiv $\Leftrightarrow\ker(\varphi)=\{0\}$
(c) $\iota(\varphi):=\varphi(M)$ ist ein Untermodul von N
(d) $coker(\varphi):=N/im(\varphi)$ heißt Cokern von φ, es gilt: φ surjektiv $\Leftrightarrow coker(\varphi)=\{0\}$
(e) (Homomorphiesatz) φ induziert einen Isomorphismus $\underline{\overline{\phi}}: M/\ker(\varphi)\to im(\varphi)$, $x+\ker(\varphi)\mapsto\varphi(x)$

Bemerkung 12.8. M R-Modul, $(M_i)_{i\in I}$ Familie von Untermoduln von M. Dann gilt:
(a) $\sum\limits_{i\in I} M_i := \{\sum\limits_{i\in I} x_i | x_i \in M_i,\, x_i = 0$ für fast alle $i \in I\}$ ist ein Untermodul von M und heißt die Summe der $M_i, i \in I$
(b) $\bigcap\limits_{i\in I} M_i$ ist ein Untermodul von M.

Bemerkung 12.9. $(M_i)_{i\in I}$ Familie von R-Moduln. Dann gilt:
(a) $\prod\limits_{i\in I} M_i := \{(x_i)_{i\in I} | x_i \in M_i\}$ wird mit komponentenweiser Addition und skalarer Mult. ein R-Modul, das direkte Produkt der $M_i, i \in I$. (b) $\bigoplus\limits_{i\in I} M_i := \{(x_i)_{i\in I} | x_i \in M_i,\, x_i = 0$ für fast alle $i \in I\}$ wird mit komponentenweiser Addition und skalarer Mult. ein R-Modul, die direkte Summe der M_i, $i \in I$.
Falls I endlich, dann ist $\prod\limits_{i\in I} M_i = \bigoplus\limits_{i\in I} M_i$
Spezialfall $R^n = \bigoplus\limits_{i=1}^{n} R$
Anmerkung: Zusammenhang zur direkten Summe von UVR aus LA1:
Sei M R-Modul, $M_1, M_2 \subseteq M$ Untermoduln
$M_1 \oplus M_2 = \{(m_1, m_2) | m_1 \in M_1, m_2 \in M_2\}$
$\Rightarrow$ Erhalte surjektiven Homomorphimus $\varphi : M_1 \oplus M_2 \to M_1 + M_2$, $(m_1, m_2) \mapsto m_1 + m_2$
Ist $M_1 \cap M_2 = \{0\}$, dann ist $\ker(\varphi) = \{(m_1, m_2) \in M_1 \oplus M_2 | m_1 + m_2 = 0\} = \{0\}$,
denn: $m_1 + m_2 = 0 \Rightarrow m_1 = -m_2 \in M_1 \cap M_2 = \{0\}$, also $m_1 = m_2 = 0$, d.h. 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 12.10. $I \subseteq R$ Ideal, M R-Modul, $(x_i)_{i\in I}$ Familie von Elementen aus M.
Dann gilt:
(a) $IM := \{\sum\limits_{i=1}^{n} a_i x_i | a_i \in I, x_i \in M, n \in \mathbb{N}\}$ ist ein Untermodul von M.
(b) $Lin((x_i)_{i\in I}) := \{\sum\limits_{i\in I} a_i x_i | a_i \in R, a_i = 0$ für fast alle $i \in I\}$ ist ein Untermodul von M, die lineare Hülle von $(x_i)_{i\in I}$

Definition 12.11. M R-Modul, $(x_i)_{i\in I}$ Familie von Elementen aus M
$(x_i)_{i\in I}$ heißt
Erzeugendensystem von $M \Leftrightarrow M = Lin((x_i)_{i\in I})$
linear unabhängig $\Leftrightarrow$ Aus $\sum\limits_{i\in I} a_i x_i = 0$, wobei $a_i \in R$, $a_i = 0$ für fast alle $i \in I$ folgt $a_i = 0$ für alle $i \in I$
Basis von $M \Leftrightarrow (x_i)_{i\in I}$ ist ein linear unabhängiges Erzeugendensystem von M

M heißt
endlich erzeugt (ee) $\Leftrightarrow M$ besitzt ein endliches Erzeugendensystem
frei $\Leftrightarrow M$ besitzt eine Basis
endlichfrei $\Leftrightarrow M$ besitzt eine endliche Basis.

Beispiel 12.12.
(a) K Körper $\Rightarrow$ Jeder K-VR ist frei (Satz 9.15)
(b) R ist einer freier R-Modul ((1) ist eine Basis)
(c) Sei $n \in \mathbb{N}$, $n > 1$

- $\mathbb{Z}/n\mathbb{Z}$ ist ee $\mathbb{Z}$-Modul, denn:
  - $\mathbb{Z}/n\mathbb{Z}$ ist als abelsche Gruppe ein $\mathbb{Z}$-Modul
  - $Lin((\overline{1})) = \{r \cdot \overline{1} | r \in \mathbb{Z}\} = \{\overline{r} | r \in \mathbb{Z}\} = \mathbb{Z}/n\mathbb{Z}$, d.h. $(\overline{1})$ ist ein ES von $\mathbb{Z}$ als $\mathbb{Z}$-Modul
- $\mathbb{Z}/n\mathbb{Z}$ ist kein freier $\mathbb{Z}$-Modul, denn:
  Sei $x = \overline{a} \in \mathbb{Z}/n\mathbb{Z} \Rightarrow n \cdot x = n \cdot \overline{a} = \overline{na} = \overline{0}$, aber $n \neq 0$. $\Rightarrow (x)$ linear abhängig $\Rightarrow$ Jede Form $\neq \{\}$ 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 (b))

Fazit: Es gibt Moduln, die keine Basis haben.

Bemerkung 12.13. *M freier R-Modul, $B = (x_i)_{i\in I}$ Basis von M*
Dann existiert ein Modulisomorphismus
$\underline{\overline{\phi_B}} : \bigoplus\limits_{i\in I} R \to M,\ (a_i)_{i\in I} \mapsto \sum\limits_{i\in I} a_i x_i$
(Beachte: $a_i = 0$ für fast alle $i \in I$)

Anmerkung:

- Man kann zeigen: Sind $(x_i)_{i\in I}$, $(y_j)_{j\in J}$ Basen des freien R-Moduls M, dann existiert eine Bijektion $I \to J$, d.h. $|I| = |J|$.
- Man kann zeigen: M ee, frei $\Leftrightarrow$ M endlich frei
- Achtung: Es gilt im Allgemeinen kein Analogon des Basisauswahlsatzes: $(2,3)$ ist ein ES des freien $\mathbb{Z}$-Moduls $\mathbb{Z}$ wegen $1 = (-1)\cdot 2 + 1\cdot 3$, aber (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 $\varphi : M \to N$ nach Wahl von Basen A von M, B von N durch eine Darstellungsmatrix $M_B^A(\varphi)$ beschreiben. Es gilt die Basiswechselformel $M_{B'}^{A'}(\varphi) = T_{B'}^B M^A$ wobei $T_A^{A'} = M_A^{A'}(id_M)$, T^B

Bemerkung 12.14. *M,N R-Moduln. $\varphi : M \to N$ Homomorphismus, sodass $\ker(\varphi), im(\varphi)$ endlich erzeugt. Dann ist M ein endlich erzeugter R-Modul.*

Bemerkung 12.15. *M R-Modul*
$x \in M$ heißt Torsionselement von $M \Leftrightarrow$ Es existiert ein $a \in R$, a kein Nullteiler, mit $ax = 0$
$T(M) = \{x \in M | x \text{ ist ein Torsionselement}\}$ ist ein Untermodul von M, der Torsionsuntermodul von M.
M heißt:
Torsions-R-Modul $\Leftrightarrow T(M) = M$
torsionsfreier R-Modul $\Leftrightarrow T(M) = \{0\}$

Anmerkung: Falls R nullteilerfrei, dann $T(M) = \{x \in M| \text{ Es existiert } a \in R, a \neq 0 \text{ mit } ax = 0\}$

Beispiel 12.16.
(a) K Körper, V K-VR $\Rightarrow V$ ist torsionsfreier K-Modul, denn:
$T(V) = \{x \in V| \text{ es existiert } \lambda \in K, \lambda \neq 0 \text{ mit } \lambda x = 0\} = \{0\}$
(b) $\mathbb{Z}$ ist torsionsfreier $\mathbb{Z}$-Modul, denn:
$T(\mathbb{Z}) = \{x \in \mathbb{Z}| \text{ es existiert } a \in \mathbb{Z}, a \neq 0 \text{ mit } ax = 0\} = \{0\}$
(c) Für $n \in \mathbb{N}$, $n > 1$ ist $\mathbb{Z}/n\mathbb{Z}$ ein Torsions-$\mathbb{Z}$-Modul, denn für alle $\overline{a} in \mathbb{Z}/n\mathbb{Z}$ ist $n \cdot \overline{a} = \overline{na} = \overline{0}$, d.h. $T(\mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$.

Bemerkung 12.17. *F freier R-Modul. Dann ist F torsionsfrei, d.h. $T(F) = \{0\}$*

Anmerkung: Die Umkehrung ist falsch: $\mathbb{Q}$ ist ein torsionsfreier $\mathbb{Z}$-Modul, aber kein freier $\mathbb{Z}$-Modul

- $\mathbb{Q}$ ist torsionsfreier $\mathbb{Z}$-Modul, denn: $T(\mathbb{Q}) = \{x \in \mathbb{Q}| \text{ es existiert} a \in \mathbb{Z}, a \neq 0 \text{ mit } ax = 0\} = \{0\}$
- $\mathbb{Q}$ 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 $a = \frac{m_1}{m_2} \neq 0$, $b = \frac{m_2}{n_2} \neq 0$ dann ist $m_2 n_1 a - m_1 n_2 b = 0$
  - leere Familie bzw. eindeutige Familien sind keine Erzeugendensysteme von $\mathbb{Q}$ als $\mathbb{Z}$-Modul

Definition 12.18. M R-Modul
$l_R(M) := sup\{l \in \mathbb{N}_0 | M_0 = \{0\} \subsetneq M_1 \subsetneq M_2 \subsetneq \ldots \subsetneq M_l = M$ ist eine Kette von Untermoduln von M$\} \in \mathbb{N}_0 \cup \{\infty\}$ heißt die Länge von M.

Beispiel 12.19.
(a) K Körper, V K-VR $\Rightarrow l_K(V) = \dim_K(V)$, denn:

- $\dim_K(V) = n < \infty \Rightarrow$ Wähle Basis $(v_1,\ldots,v_n)$ von V, dann ist $M_0 = \{0\} \subsetneq Lin(v_1) \subsetneq Lin(v_1,v_2) \subsetneq \ldots \subsetneq Lin(v_1,\ldots,v_n) = V$ eine Kette von UVR von $V \Rightarrow l_K(V) \geq n$. Ist $M_0 = \{0\} \subsetneq M_1 \subsetneq \ldots \subsetneq M_l = V$ eine Kette von Untermoduln dann ist $0 < \dim \mu_1 < \ldots < \dim M_l = \dim V = n$, insbesondere $\dim V = \dim M_l \geq l$, also $l_K(V) \leq n$
- $\dim_K(V) = \infty \Rightarrow l_K(V) = \infty$.

(b) $l_{\mathbb{Z}}(\mathbb{Z}) = \infty$, denn: für alle $n \in \mathbb{N}$ ist $0 \subsetneq 2^n\mathbb{Z} \subsetneq 2^{n-1}\mathbb{Z} \subsetneq \ldots \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$ eine Kette von Untermoduln von $\mathbb{Z}$ (c) $l_{\mathbb{Z}}(\mathbb{Z}/6\mathbb{Z}) = 2$, denn: Für $\overline{a} \in \mathbb{Z}/6\mathbb{Z}$ ist

$$Lin(\overline{a}) = \begin{cases} \mathbb{Z}/6\mathbb{Z}, \text{ falls } \overline{a} \in \{\overline{1},\overline{5}\} \\ \{\overline{0}\}, \text{ falls } \overline{a} = \overline{0} \\ \{\overline{0},\overline{3}\}, \text{ falls } \overline{a} = \overline{3} \\ \{\overline{0},\overline{2},\overline{4}\}, \text{ falls } \overline{a} \in \{\overline{2},\overline{4}\} \end{cases}$$

$\Rightarrow$ Die beiden Ketten $\{\overline{0}\} \subsetneq Lin(\overline{3}) \subsetneq \mathbb{Z}/6\mathbb{Z}$, $\{\overline{0}\} \subseteq Lin(\overline{2}) \subsetneq \mathbb{Z}/6\mathbb{Z}$ können nicht weiter verfeinert werden, also $l_{\mathbb{Z}}(\mathbb{Z}/6\mathbb{Z}) = 2$
(d) $l_R(M) = 0 \Leftrightarrow M = \{0\}$

Bemerkung 12.20. M R-Modul, $N \subseteq M$ Untermodul
Dann gilt: $l_R(N) \leq l_R(M)$

Bemerkung 12.21. M', M'' R-Moduln. Dann gilt:
$l_R(M' \oplus M'') = l_R(M') + l_R(M'')$

13. Moduln über Hauptidealringen

In diesem Abschnitt sei R stets ein HIR.

Ziel: Struktursatz für endlich erzeugte R-Moduln.

Bemerkung 13.1. F endlich freier R-Modul
Dann gilt: Je zwei Basen von F haben dieselbe Kardinalität. Diese heißt der Rang von F

Satz 13.2. $A \in M(m \times n, R)$
Dann existiert ein $r \in \mathbb{N}_0$, $c_1,\ldots c_r \in R \backslash \{0\}$, sodass

$$A \sim \begin{pmatrix} c_1 & & & & & \\ & \ddots & & & & \\ & & c_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix} \text{ mit } c_1 | \ldots | c_r$$

r ist eindeutig bestimmt, $c_1,\ldots,c_r$ sind eindeutig bestimmt bis auf Assoziiertheit und heißen die Elementarteiler von A

Bemerkung 13.3. R HIR, $a \in R\backslash(R^* \cup \{0\})$, $a = p_1 \cdot \ldots \cdot p_r$ mit irreduziblen Elementen $p_1, \ldots, p_r$ (nicht notwendig paarweise verschieden). Dann ist
$l_R(R/aR) = r$, insbesondere ist $l_R(R/aR) < \infty$

Bemerkung 13.4. $c_1, \ldots c_r \in R\backslash(R^* \cup \{0\})$ mit $c_1 | \ldots | c_r$
M R-Modul mit $M \cong \bigoplus_{i=1}^{r} R/c_iR$
Dann gilt: r ist eindeutig bestimmt, $c_1, \ldots, c_r$ sind eindeutig bestimmt bis auf Assoziiertheit durch M

Satz 13.5. (Elementarteilersatz)
F endlich freier R-Modul, $M \subseteq F$ Untermodul
Dann existiert eine Basis $(x_1, \ldots, x_m)$ von F sowie $s \in \mathbb{N}_0$, $c_1, \ldots, c_s \in R\backslash\{0\}$ mit folgenden Eigenschaften:
(I) $(c_1x_1, \ldots, c_sx_s)$ ist eine Basis von M
(II) $c_1 | \ldots | c_s$
s ist eindeutig, $c_1, \ldots, c_s$ sind eindeutig bis auf Assoziiertheit durch M bestimmt (sind insbesondere unabhängig von der Wahl der Basis $(x_1, \ldots, x_m)$) und heißen die Elementarteiler von $M \subseteq F$

Folgerung 13.6. F eindlichfreier R-Modul, $M \subseteq F$ Untermodul
Dann ist M endlich frei und $Rang(M) \leq Rang(F)$

Anmerkung:

- Aus $M \subsetneq M$ folgt nicht $Rang(M) < Rang(F)$: z.B. ist $\mathbb{Z}$ ein freier $\mathbb{Z}$-Modul von Rang 1, $2\mathbb{Z} \subsetneq \mathbb{Z}$ ist freier $\mathbb{Z}$-Modul mit $Rang(2\mathbb{Z}) = 1 = Rang(\mathbb{Z})$

- Man kann zeigen (unter Verwendung des Auswahlaxioms): F freier R-Modul, $M \subseteq F$ Untermodul $\Rightarrow M$ frei (R HIR!)

- ohne die Voraussetzung, dass R HIR ist, wird 13.6 falsch:
  Bsp.: $F = \mathbb{Q}[X,Y]$ als $R = \mathbb{Q}[X,Y]$-Modul (R ist kein HIR!), $M = Lin((X,Y))$ ist nicht frei als R-Modul.

Satz 13.7. (Hauptsatz für endlich erzeugte Moduln über HIR, Variante 1)
M endlich erzeugter R-Modul. Dann gilt:
(a) Es gibt einen endlich freien Untermodul ($F \subseteq M$, etwa $F \cong R^d$, mit $M = F \oplus T(M)$. Hierbei ist $d = Rang(F)$ eindeutig bestimmt. (b) Es gibt $s \in \mathbb{N}_0$, $c_1, \ldots, c_s \in R\backslash(R^* \cup \{0\})$ mit $T(M) \cong \bigoplus_{j=1}^{s} R/c_jR$ mit $c_1 | \ldots | c_s$
(c) Die Zahl s ist eindeutig bestimmt, $c_1, \ldots, c_s$ sind eindeutig bestimmt bis auf Assoziiertheit und heißen die Elementarteiler von M.
Also: $M \cong R^d \oplus R/c_1R \oplus \ldots \oplus R/c_sR$

Anmerkung: Ohne die Voraussetzung "M e. e." 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

Folgerung 13.8. M R-Modul. Dann sind äquivalent:
(i) M ist endlich erzeugt und frei
(ii) M ist endlich frei

Folgerung 13.9. (Hauptsatz über e. e. abelsche Gruppen, Variante 1)
G endlich erzeugte abelsche Gruppe (= e. e. $\mathbb{Z}$-Modul)
Dann existiert ein Isomorphismus $G \cong \mathbb{Z}^d \oplus \mathbb{Z}/c_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/c_s\mathbb{Z}$ mit d $\in \mathbb{N}_0, c_1, \ldots, c_s \in \mathbb{N}_0 > 1$, $c_1 | \ldots | c_s$
d sowie s, $c_1, \ldots, c_s$ sind eindeutig bestimmt.
Es ist G endlich $\Leftrightarrow d = 0$. In diesem Fall ist $|G| = c_1 \cdot \ldots \cdot c_s$

Beispiel 13.10.
(a) abelsche Gruppen mit 4 Elementen bis auf Isomorphie:
1. Fall: $s=1$, $c_1=4$: $\mathbb{Z}/4\mathbb{Z}$
2. Fall: $s=2$, $c_1=2$, $c_2=2$: $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$
$\Rightarrow$ Bist auf Isomorphie gibt es 2 abelsche Gruppen mit 4 Elementen
(b) abelsche Gruppen mit 24 Elementen bis auf Isomorphie:
1. Fall: $s=1$, $c_1=24$: $\mathbb{Z}/24\mathbb{Z}$
2. Fall: $s=2$, $c_1=2$, $c_2=12$: $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/12\mathbb{Z}$
3. Fall: $s=3$, $c_1=2$, $c_2=2$, $c_3=6$: $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z}$
$\Rightarrow$ 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 13.10(b) ist diese isomorph?

Bemerkung 13.11. (Spezialfall des Chinesischen Restsatzes)
$a\in R\backslash(R*\cup\{0\})$, $a=cp_1^{n_1}\cdot\ldots p_r^{n_r}$ mit $c\in R^*$, $p_1,\ldots,p_r$ irreduzibel, paarweise nicht-assoziiert,
$\pi_i: R\to R/(p_i^{n_i})$, $b\mapsto b+(p_i^{n_i})$ kanonische Projektion für $i=1,\ldots,r$
Dann ist die Abbildung $\varphi: R\to R/(p_1^{n_1})\times\ldots\times R/(p_r^{n_r})$, $b\mapsto(\pi_1(b),\ldots,\pi_r(b))=(b+(p_1^{n_1}),\ldots,b+(p_r^{n_r}))$ ein surjektiver Ringhomomorphismus mit $\ker\varphi=(a)$, d.h. wir erhalten eine Ringisomorphismus
$\overline{\underline{\phi}}: R/(a)\to R/(p_1^{n_1})\times\ldots\times R/(p_r^{n_r})$
Hierbei ist $R/(p_1^{n_1})\times\ldots\times R/(p_r^{n_r})$ ein Ring via komponentenweiser Addition und Multiplikation.
Insbesondere erhalten wir einen Isomorphismus von R-Moduln
$R/(a)\cong R/(p_1^{n_1})\oplus\ldots\oplus R/(p_r^{n_r})$

Beispiel 13.12. Nach 13.11 ist $\mathbb{Z}/24\mathbb{Z}\cong\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/8\mathbb{Z}$

Satz 13.13. (Hauptsatz für e. e. Moduln über HIR, Variante 2)
M e. e. R-Modul, $\mathbb{P}$ sei ein Vertretersystem der Primelemente von R bis auf Assoziiertheit,
für $p\in\mathbb{P}$ sei $M_p:=\{x\in M|$ Es existiert ein $n\in\mathbb{N}$ mit$p^nx=0\}\subseteq T(M)$ (ist offenbar ein Untermodul)
Dann gilt:
(a) Es gibt einen e. e. freien Untermodul $F\subseteq M$, sodass $M=F\oplus T(M)$, $d:=Rang(F)$ ist eindeutig bestimmt.
(b) $T(M)=\bigoplus\limits_{p\in\mathbb{P}}M_p$, wobei $M_p=0$ für fast alle $p\in\mathbb{P}$
(c) Für jedes $p\in\mathbb{P}$ mit $M_p\neq0$ gibt es eindeutig bestimmte natürliche Zahlen $1\leq n_{p,1}\leq\ldots\leq n_{p,s_p}$ mit $M_p\cong R/p^{n_{p,1}}R\oplus\ldots\oplus R/p^{n_{p,s_p}}R$
Also $M\cong R^d\oplus\bigoplus\limits_{p\in\mathbb{P}}(R/p^{n_{p,1}}R\oplus\ldots\oplus R/p^{n_{p,s_p}})$

Folgerung 13.14. (HS für e.e. abelsche Gruppen, Variante 2)
G e. e. abelsche Gruppe, $\mathbb{P}$ Menge der Primzahlen in $\mathbb{N}$
Dann existiert ein Isomorphismus $G\cong\mathbb{Z}^d\oplus\bigoplus\limits_{p\in\mathbb{P}}(\mathbb{Z}/p^{n_{p,1}}R\oplus\ldots\oplus\mathbb{Z}/p^{n_{p,s_p}})$, $1\leq n_{p,1}\leq\ldots\leq n_{p,s_p}$
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 $\Leftrightarrow d=0$. In diesem Fall ist $|G|=\prod\limits_{p\in\mathbb{P}}p^{n_{p,1}+\ldots+n_{p,s_p}}$

Beispiel 13.15. (vgl. 13.10) Endliche abelsche Gruppen mit 24 Elementen bis auf Isomorphie:
Es ist $24=2^3\cdot3=2\cdot2^2\cdot3=2\cdot2\cdot2\cdot3$
$\Rightarrow$ Isomorphietypen: $\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}$, $\quad\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}$, $\quad\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}$
Es ist $\mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}\cong\mathbb{Z}/24\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}\underset{chin.RS}{\cong}\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/12\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}\underset{chin.RS}{\cong}\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z}$