LINEARE ALGEBRA II: LEHRPLAN

VICTORIA HOSKINS

Webseite: `http://userpage.fu-berlin.de/hoskins/LAII.html`

Inhaltsverzeichnis

1. Jordan-Normalform

Mit der Jordan-Normalform werden wir alle komplexen Matrizen bis auf Ähnlichkeit klassifizieren. Wir werden eine Normalform, *die Jordan-Normalform* finden, so dass es in jeder Ähnlichkeitsklasse genau eine[1] komplexe Matrix in Normalform gibt. Wir werden Invarianten für die Ähnlichkeitsklassen (d.h. etwas, dass das Gleiche für zwei ähnliche Matrizen ist) entdecken: alte Invarianten (das charakteristische Polynom, Eigenwerte) und neue Invariante (das Minimalpolynom, geometrische und algebraische Vielfachheit der Eigenwerte).

[16.04.18]

1.1. Erinnerung an Eigenwerte und Diagonalisierung.
Sei K ein Körper.

Definition.

(1) Für einen linearen Endomorphismus $f \in \mathrm{End}_K(V)$ eines K-Vektorraumes V sagen wir, dass $v \in V$ mit $v \neq 0_V$ ein *Eigenvektor zum Eigenwert* $\lambda \in K$ ist, falls
$$f(v) = \lambda \cdot v.$$
Für $\lambda \in K$ definieren wir den λ-*Eigenraum* von f
$$\mathrm{Eig}(f, \lambda) := \{v \in V : f(v) = \lambda \cdot v\}.$$
Die *geometrische Vielfachheit* von λ ist $\mu_g(f, \lambda) := \dim_K(\mathrm{Eig}(f, \lambda))$.

(2) Für eine Matrix $A \in \mathrm{Mat}_{n\times n}(K)$ sagen wir, dass $x \in K^n$ mit $x \neq \mathbf{0}$ ein *Eigenvektor zum Eigenwert* $\lambda \in K$ ist, falls
$$Ax = \lambda x.$$
Der λ-*Eigenraum* von A ist $\mathrm{Eig}(A, \lambda) = \{x \in K^n : Ax = \lambda x\}$ und die *geometrische Vielfachheit* von λ ist $\mu_g(A, \lambda) := \dim_K(\mathrm{Eig}(A, \lambda))$.

Bemerkung. Nach [LAI, Satz 5.10] gelten:

(1) Wenn V endlichdimensional ist (so dass $\det(f)$ für $f \in \mathrm{End}_K(V)$ definiert ist), gilt: λ ist ein Eigenwert von $f \iff \det(\lambda \cdot \mathrm{Id}_V - f) = 0$.

(2) λ ist genau dann ein Eigenwert von $A \in \mathrm{Mat}_{n\times n}(K)$, wenn $\det(\lambda I_n - A) = 0$.

Definition.

[1](bis auf die Reihenfolge der *Jordanblöcke*)

(1) Für $A \in \mathrm{Mat}_{n\times n}(K)$ ist das *charakteristische Polynom* von A
$$\chi_A(t) = \det(tI_n - A) \in K[t].$$
Die *algebraische Vielfachheit* von λ ist $\mu_a(f,\lambda) := \mu(\chi_f,\lambda) := \max\{n : (t-\lambda)^n | \chi_f(t)\}$.

(2) Für einen linearen Endomorphismus $f : V \to V$ eines endlichdimensionalen K-Vektorraumes V ist das *charakteristische Polynom* von f
$$\chi_f(t) = \det(t\mathrm{Id}_V - f) \in K[t].$$
Die *algebraische Vielfachheit* von λ ist $\mu_a(A,\lambda) := \mu(\chi_A,\lambda)$.

Bemerkung. Wenn $\dim_K(V) = n$ (bzw. $A \in \mathrm{Mat}_{n\times n}(K)$), ist $\chi_f(t)$ (bzw. $\chi_A(t)$) ein normiertes[2] Polynom vom Grad n und die Nullstellen des charakteristischen Polynoms sind die Eigenwerte von f (bzw. A) [LAI, Satz 5.13].

Lemma.[LAI] Die algebraische Vielfachheit ist größer oder gleich die geometrische Vielfachheit für jeden Eigenvektor eines linearen Endomorphismus von einem endlichdimensionalen K-Vektorraum.

Definition.

(1) Ein linearer Endomorphismus $f : V \to V$ eines endlichdimensionalen K-Vektorraumes V heißt *diagonalisierbar*, wenn es eine geordnete Basis $\mathcal{B}$ von V gibt, so dass $M^{\mathcal{B}}_{\mathcal{B}}(f)$ eine Diagonalmatrix ist.
(2) Eine Matrix $A \in \mathrm{Mat}_{n\times n}(K)$ heißt *diagonalisierbar*, wenn der Endomorphismus $F_A \in \mathrm{End}_K(K^n)$ mit $F_A(x) = Ax$ diagonaliserbar ist.
(3) Zwei Matrizen $A, B \in \mathrm{Mat}_{n\times n}(K)$ heißen *ähnlich* (schreibweise: $A \sim B$), wenn es $S \in \mathrm{GL}_n(K)$ gibt mit $A = SBS^{-1}$.

Übung.

(1) Ähnlichkeit auf $\mathrm{Mat}_{n\times n}(K)$ ist eine Äquivalenzrelation.
(2) Eine Matrix $A \in \mathrm{Mat}_{n\times n}(K)$ ist genau dann diagonalisierbar, wenn A ähnlich zu einer Diagonalmatrix ist.
(3) Wenn $f : V \to V$ ein linearer Endomorphismus eines K-Vektorraumes der Dimension n ist, sind alle zugehörigen Matrizen von f ähnlich (d.h. für geordnete Basen $\mathcal{A}$ und $\mathcal{B}$ von V gilt $M^{\mathcal{A}}_{\mathcal{A}}(f) \sim M^{\mathcal{B}}_{\mathcal{B}}(f)$).
(4) Für zwei ählinche Matrizen $A \sim B$ gilt $\chi_A(f) = \chi_B(f)$.

Bermerkung. Sei V ein endlichdimensionaler K-Vektorraum und $f \in \mathrm{End}_K(V)$.

(1) Nach [LAI, Satz 5.11] ist f genau dann diagonalisierbar, wenn V eine Basis aus Eigenvektoren von f besitzt.
(2) Nach [LAI, Satz 5.12] ist f diagonalisierbar, wenn f genau $n = \dim(V)$ paarweise verschiedene Eigenwerte $\lambda_1, \dots, \lambda_n$ hat.
(3) Nach [LAI, Satz 5,14] ist äquivalent:
  (a) f ist diagonalisierbar.
  (b) Das charakteristische Polynom $\chi_f(t)$ zerfällt in Linearfaktoren und die geometrische und algebraische Vielfachheiten aller Eigenwerte $\lambda \in K$ übereinstimmen:
  $$\mu_g(f,\lambda) = \mu_a(f,\lambda).$$
  (c) Wenn $\lambda_1, \cdots, \lambda_k$ die paarweise verschiedene Eigenwerte von f sind, dann gilt
  $$V = \bigoplus_{i=1}^{k} \mathrm{Eig}(f,\lambda_i) := \mathrm{Eig}(f,\lambda_1) \oplus \cdots \oplus \mathrm{Eig}(f,\lambda_k).$$

[2] $P(t) = a_n t^n + \cdots a_0$ ist *normiert*, falls $a_n = 1$

1.2. **Nullstellen von Polynomen.** Für einen Körper K kann man fragen, wann zerfällt jedes Polynom $P(t) \in K[t]$ in Linearfaktoren? Oder wann hat jedes nicht-konstante Polynom mit Koeffizienten in K eine Nullstelle?

Definition. Ein Körper K heißt *algebraisch abgeschlossen*, wenn jedes nicht-konstante Polynom mit Koeffizienten in K eine Nullstelle in K hat.

Beispiel. Für $K = \mathbb{R}$ hat das Polynom $P(t) = t^2 + 1$ keine Nullstelle in $\mathbb{R}$ und deshalb ist $\mathbb{R}$ nicht algebraisch abgeschlossen.

Lemma. Wenn K algebraisch abgeschlossen ist, zerfällt jedes Polynom $P(t) \in K[t]$ in Linearfaktoren.

Satz 1.1 (Fundamentalsatz der Algebra)**.** *Die komplexen Zahlen sind algebraisch abgeschlossen, d.h. jedes nicht-konstante Polynom mit $\mathbb{C}$-Koeffizienten besitzt mindestens eine Nullstelle in $\mathbb{C}$.* [3]

Bemerkung. Es gibt einen Körper-Homomorphismus $\mathbb{R} \to \mathbb{C}$ mit $x \mapsto x + i0$. Deshalb gibt es einen Ring-Homomorphismus $\mathbb{R}[t] \to \mathbb{C}[t]$, der auch injektiv ist. Da $\mathbb{C}$ algebraisch abgeschlossen ist, hat jedes nicht-konstante Polynom $P(t) \in \mathbb{R}[t]$ mindestens eine Nullstelle in $\mathbb{C}$. Ferner gilt für $P(t) \in \mathbb{R}[t]$ und eine Nullstelle $\alpha \in \mathbb{C}$ von $P(t)$

(1) Die konjugiert komplexe Zahl $\overline{\alpha}$ ist auch eine Nullstelle von P. Ferner haben α und $\overline{\alpha}$ die gleiche Vielfachheit: $\mu(P, \alpha) = \mu(P, \overline{\alpha})$.
(2) $Q(t) := (t - \alpha)(t - \overline{\alpha}) \in \mathbb{R}[t]$ und es gibt eine Zerlegung $P(t) = Q(t)R(t)$ in $\mathbb{R}[t]$.
(3) Wenn $\mathrm{Grad}(P)$ ungerade ist, hat P mindestens eine Nullstelle in $\mathbb{R}$.

Lemma. Für $P(t) \in K[t]$ gibt es einen injektiven Körper-Homomorphismus $K \to L$ (was wir *eine Körpererweiterung* nennen), so dass $P(t)$ in Linearfaktoren aus $L[t]$ zerfällt.[4]

Beispiel. Für $K = \mathbb{R}$ oder $K = \mathbb{C}$ könner wir $L = \mathbb{C}$ wählen, weil $\mathbb{C}$ algebraisch abgeschlossen ist. Dann zerfällt jedes Polynom $P(t) \in K[t]$ in Linearfaktoren in $L[t]$.

1.3. **Trigonalisierung.** Sei V ein endlichdimensionaler K-Vektorraum und $f \in \mathrm{End}_K(V)$. Was können wir über f und die zugehörige Matrizen $M^{\mathcal{A}}_{\mathcal{A}}(f)$ folgern, wenn nur $\chi_f(t)$ in Linearfaktoren zerfällt (aber die geometrische und algebraische Vielfachheiten der Eigenwerte nicht übereinstimmen)?

Definition. Sei $f : V \to V$ ein linearer Endomorphismus.

(1) Ein Untervektorraum $U \subset V$ heißt f-invariant, falls $f(U) \subset U$.
(2) Eine *Fahne* in einem n-dimensionalen K-Vektorraum V ist eine Kette von Untervektorräume
$$\{0_V\} = V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_{n-1} \subsetneq V_n = V$$
mit $\dim_K(V_r) = r$. Diese Fahne heißt f-invariant, wenn jeder Unterraum V_r in der Fahne f-invariant ist.

Beispiel.

(1) Für alle $f \in \mathrm{End}_K(V)$ sind $\{0_V\}$ und V offensichtlich f-invariant.
(2) Die Eigenräume $\mathrm{Eig}(f, \lambda)$ sind f-invariant.
(3) Für $V = K^n$ gibt es die Standard-Fahne mit $V_r := \mathrm{Span}(e_1, \ldots, e_r)$.
(4) Jede Fahne von V ist Id_V-invariant.

[3] Für den Beweis, siehe den faszinierenden Kurs ‘Funktionentheorie’.
[4] Diese Lemma wird in der Algebra und Zahlentheorie bewiesen.

(5) Sei $A \in \mathrm{Mat}_{n\times n}(K)$ eine obere Dreiecksmatrix, d.h. $a_{ij} = 0$ für $i > j$. Für die zugehörige lineare Abbildung $F_A : K^n \to K^n$ ist die Standard-Fahne F_A-invariant.

[18.04.18] **Lemma.** Für einen linearen Endomorphismus $f : V \to V$ eines n-dimensionalen K-Vektorraumes ist äquivalent:

(1) Es gibt eine f-invariante Fahne von V,
(2) Es gibt eine geordnete Basis $\mathcal{A}$ von V, so dass $M^{\mathcal{A}}_{\mathcal{A}}(f)$ eine obere Dreiecksmatrix ist.

Definition.

(1) Ein linearer Endomorphismus $f : V \to V$ eines n-dimensionalen K-Vektorraumes heißt *trigonalisierbar*, wenn es eine f-invariante Fahne von V gibt.
(2) Eine Matrix $A \in \mathrm{Mat}_{n\times n}(K)$ heißt *trigonalisierbar*, wenn A ähnlich zu einer oberen Dreiecksmatrix ist.

Bemerkung.

(1) $A \in \mathrm{Mat}_{n\times n}(K)$ ist genau dann trigonalisierbar, wenn es $F_A : K^n \to K^n$ ist.
(2) $f \in \mathrm{End}_K(V)$ ist genau dann triangonalisierbar, wenn es $M^{\mathcal{A}}_{\mathcal{A}}(f)$ (für eine geordnete Basis $\mathcal{A}$ von V) ist.
(3) Jeder diagonalisierbare Endomorphismus ist auch trigonalisierbar, aber die Umkehrung ist falsch: zum Beispiel ist

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

trigonalisierbar aber nicht diagonalisierbar, weil $1 = \mu_g(A, 1) < 2 = \mu_a(A, 1)$ [LAII, Satz 5.14].

Satz 1.2. *Für einen linearen Endomorphismus $f : V \to V$ eines n-dimensionalen K-Vektorraumes ist äquivalent:*

(1) f ist trigonalisierbar,
(2) $\chi_f(t)$ zerfällt in Linearfaktoren.

Korollar.

(1) Jede komplexe Matrix $A \in \mathrm{Mat}_{n\times n}(\mathbb{C})$ ist trigonalisierbar.
(2) Jeder Endomorphismus eines endlichdimensionalen $\mathbb{C}$-Vektorraumes ist trigonalisierbar.

Beispiel. Sind die folgende reelle Matrizen diagonalisierbar (bzw. trigonalisierbar)?

$$A = \begin{pmatrix} 2 & -3 \\ 0 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} 3 & -2 \\ 0 & 3 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$$

Wir berechnen die charakteristische Polynome und Vielfachheiten jeder Matrix:

- A ist trigonaliserbar, weil $\chi_A(t) = (t-2)(t-1)$ in Linearfaktoren zerfällt. Ferner ist A diagonalisierbar, weil

$$\mathrm{Eig}(A, 1) = \mathrm{Span}\begin{pmatrix} 3 \\ 1 \end{pmatrix} \qquad \mathrm{Eig}(A, 2) = \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

so dass $\mu_g(A, \lambda) = 1 = \mu_a(A, \lambda)$ für $\lambda = 1, 2$.
- B ist trigonalisierbar, weil $\chi_B(t) = (t-3)^2$, aber B ist nicht diagonalisierbar, weil

$$\mu_g(B, 3) = \dim_K \mathrm{Eig}(B, 3) = \dim_K \mathrm{Span}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1 < 2 = \mu_a(B, 3).$$

- C ist nicht trigonalisierbar (und deshalb auch nicht diagonalisierbar), weil

$$\chi_C(t) = (t-1)(t-1) + 1 = t^2 - 2t + 2$$

keine Nullstellen in $\mathbb{R}$ hat (die Diskriminante von χ_C ist negativ: $(-2)^2 - 4\times 2 = -4 < 0$).

1.4. **Der Satz von Cayley-Hamilton.** Für einen K-Vektorraum V ist $\mathrm{End}_K(V)$ ein K-Vektorraum und ein Ring: man kann Polynome miteinander punktweise addieren und die Komposition von Abbildung liefert eine Multiplikation auf $\mathrm{End}_K(V)$. Deshalb können wir die Potenzen eine Abbildung $f \in \mathrm{End}_K(V)$ betrachten: $f^0 := \mathrm{Id}_V$, $f^1 := f$, $f^2 := f \circ f$, u.s.w. Für ein Polynom $P(t) = a_n t^n + a_{n-1}t^{n-1} + \cdots + a_0 \in K[t]$ definieren wir

$$P(f) := a_n f^n + a_{n-1} f^{n-1} + \cdots + a_0 \mathrm{Id}_V \in \mathrm{End}_K(V)$$

und wir schreiben $P(f) = 0$, wenn dieser Endomorphismus die Nullabbildung ist.

Lemma. Sei V ein n-dimensionaler K-Vektorraum und $f \in \mathrm{End}_K(V)$. Dann gibt es ein nicht-Null Polynom $P(t) \in K[t]$ mit $P(f) = 0$. [23.04.18]

Definition. Sei V ein endlichdimensionaler K-Vektorraum und $f \in \mathrm{End}_K(V)$. Ein normiertes nicht-Null Polynom $m_f(t) \in K[t]$ heißt *Minimalpolynom* von f wenn

i) $m_f(f) = 0$.
ii) Für alle andere nicht-Null Polynome $P(t) \in K[t]$ mit $P(f) = 0$ gilt $\mathrm{Grad}(m_f) \leq \mathrm{Grad}(P)$.

Ebenso definieren wir das Minimialpolynom von $A \in \mathrm{Mat}_{n\times n}(K)$, so dass $m_A(t) = m_{F_A}(t)$ für $F_A : K^n \to K^n$, $x \mapsto Ax$.

Bemerkung.

(1) Sei V ein endlichdimensionaler K-Vektorraum und $f \in \mathrm{End}_K(V)$ mit dem Minimalpolynom $m_f(t) \in K[t]$. Für alle $P(t) \in K[t]$ mit $P(f) = 0$ gilt $m_f(t)|P(t)$: nach der Division mit Rest für Polynome gilt

$$P(t) = Q(t)m_f(t) + r(t) \quad \text{ und } \mathrm{Grad}(r) < \mathrm{Grad}(m_f)$$

und falls $r \neq 0$, gilt $r(f) = 0$, was ein Widerspruch zu der Minimalität von m_f gibt.
(2) Das Minimalpolynom existiert nach dem Lemma oben und es ist eindeutig (weil es normiert ist).
(3) Zwei ähnlich Matrizen $A \sim B$ haben das gleiche Minimalpolnom: $m_A(t) = m_B(t)$.

Satz 1.3 (Satz von Cayley-Hamilton). *Sei V ein endlichdimensionaler K-Vektorraum und $f \in \mathrm{End}_K(V)$ mit dem charakteristischen Polynom $\chi_f(t) \in K[t]$. Dann gilt $\chi_f(f) = 0$. Insbesondere gilt $m_f(t)|\chi_f(t)$.*

Korollar. Sei V ein n-dimensionaler K-Vektorraum und $f \in \mathrm{End}_K(V)$. Dann gilt $\chi_f | m_f^n$.

Beispiel. Die Matrix

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

hat das charakteristische Polynom $\chi_A(t) = (t-1)^2 = t^2 - 2t + 1$. Das Minimalpolynom von A ist entweder $t-1$ oder $(t-1)^2$, da $m_A(t)|\chi_A(t)$ nach dem Satz von Cayley–Hamilton. Da $A - I_2 \neq 0$, ist $t-1$ nicht das Minimalpolynom von A. Deshalb ist $m_A(t) = \chi_A(t) = (t-2)^2$. Nach dem Satz von Cayley–Hamilton gilt

$$A^2 - 2A + I_2 = 0.$$

Es folgt, dass $A(A - 2I_2) = -I_2$, so dass $A(2I_2 - A) = I_2$. Insbesonder ist $A^{-1} = 2I_2 - A$.

Bemerkung. Mit dem Satz von Cayley-Hamilton können wir für jede invertierbare Matrix $A \in \mathrm{Mat}_{n\times n}(K)$ die inverse Matrix A^{-1} finden. Wir erinnern uns, dass A genau dann invertierbar ist, wenn $\det(A) \neq 0$. Für das charakteristiche Polynom

$$\chi_A(t) := \det(tI_n - A) = t^n + c_{n-1}t^{n-1} + \cdots + c_1 t + c_0$$

gilt $\chi_A(0) = \det(-A) = (-1)^n \det(A) = c_0$. Insbesondere $c_0 \neq 0 \iff \det(A) \neq 0$. Nach dem Satz von Cayley-Hamilton gilt

$$A^n + c_{n-1}A^{n-1} + \cdots + c_1 A + c_0 I_n = 0.$$

Diese Gleichung ist äquivalent zu

$$A(A^{n-1} + c_{n-1}A^{n-2} + \cdots c_1 I_n) = -c_0 I_n$$

und wenn $c_0 \neq 0$ ist die inverse Matrix $A^{-1} = \frac{-1}{c_0}(A^{n-1} + c_{n-1}A^{n-2} + \cdots c_1 I_n)$.

1.5. **Nilpotente Endomorphismen und Haupträume.** Haupträume sind verallgemeinerte Eigenräume[5] und wir werden Haupträume benutzen, um die *Jordan-Zerlegung* zu beschreiben.

[25.04.18] **Definition.**

(1) Ein linearer Endomorphismus $f : V \to V$ eines K-Vektorraumes heißt *nilpotent*, falls es gibt $r \in \mathbb{N}$ mit $f^r = 0$ (die Nullabbildung).
(2) Eine Matrix $A \in \mathrm{Mat}_{n\times n}(K)$ heißt *nilpotent*, falls es gibt $r \in \mathbb{N}$ mit $A^r = 0$ (die Nullmatrix).

Lemma. Sei $f : V \to V$ ein linearer Endomorphismus eines n-dimensionalen K-Vektorraumes. Dann ist äquivalent:

(1) f ist nilpotent,
(2) Es gibt $1 \leq r \leq n$ mit $f^r = 0$,
(3) $\chi_f(t) = t^n$,
(4) Es gibt eine geordnete Basis $\mathcal{A}$ von V mit

$$M^{\mathcal{A}}_{\mathcal{A}}(f) = \begin{pmatrix} 0 & * & * \\ \vdots & \ddots & * \\ 0 & \cdots & 0 \end{pmatrix}.$$

Bemerkung. Sei V ein endlichdimensionaler K-Vektorraum. Für $h \in \mathrm{End}_K(V)$ und die Potenzen von h gilt

$$\{0_V\} = \ker(h^0) \subset \ker(h) \subset \ker(h^2) \subset \cdots$$

und

$$V = \mathrm{Bild}(h^0) \supset \mathrm{Bild}(h) \supset \mathrm{Bild}(h^2) \supset \cdots$$

und $\dim_K(V) = \dim_K(\ker(h^r)) + \dim_K(\mathrm{Bild}(h^r))$ nach der Dimensionsformel für h^r, aber im allgemeinen ist diese Summe nicht direkt: $\ker(h^r) \cap \mathrm{Bild}(h^r) \neq \{0_V\}$. Da V endlichdimensional ist, können beide Ketten nicht endlos aufsteigen (bzw. absteigen).

Lemma (von Fitting). Sei V ein endlichdimensionaler K-Vektorraum. Für $h \in \mathrm{End}_K(V)$ sei

$$d = \min\{r \in \mathbb{N} : \ker(h^r) = \ker(h^{r+1})\}.$$

Dann gilt

(i) $d = \min\{r \in \mathbb{N} : \mathrm{Bild}(h^r) = \mathrm{Bild}(h^{r+1})\}$,
(ii) $U := \ker(h^d)$ und $W := \mathrm{Bild}(h^d)$ sind h-invariante Untervektorräume von V,
(iii) $h|_W : W \to W$ ist ein Isomorphismus,
(iv) $h|_U : U \to U$ ist nilpotent mit dem Minimalpolynom $m_{h|_U}(t) = t^d$,
(v) $\ker(h^d) = \ker(h^{d+i})$ und $\mathrm{Bild}(h^d) = \mathrm{Bild}(h^{d+i})$ für alle $i \in \mathbb{N}$,
(vi) $V = U \oplus W$,
(vii) $d \leq \dim_K(U) = \mu_a(h, 0)$.

[5]Ein Hauptaum eines Eigenwertes λ (eines Endomorphismuses) ist größer als der λ-Eigenraum und die Dimension eines Hauptraumes ist die algebraische Vielfachheit von λ. Wir erinnern uns, dass die Dimension eines Eigenraumes (d.h. die geometrische Vielfachheit) ist kleiner oder gleich die algebraische Vielfachheit.

(viii) Es gibt eine geordnete Basis $\mathcal{A}$ von V, so dass
$$M_{\mathcal{A}}^{\mathcal{A}}(h) = \begin{pmatrix} N & 0 \\ 0 & B \end{pmatrix} \quad \text{mit} \quad N^d = 0 \text{ (nilpotent) und } B \text{ invertierbar.}$$

Bemerkung. Sei $f : V \to V$ ein linearer Endomorphismus eines endlichdimensionalen K-Vektorraumes. Wir erinnern uns, dass f genau dann diagonalisierbar ist, wenn V die direkte Summe der Eigenräume von f ist. In diesem fall zerfällt das charakteristische Polynom von f in Linearfaktoren und es gilt
$$\mu_g(f,\lambda) := \dim_K \operatorname{Eig}(f,\lambda) = \mu_a(f,\lambda)$$
für alle Eigenwerte λ von f. Wenn f nicht diagonalisierbar ist, dann ist die Summe aller Eigenräume von f kleiner als V. In diesem Fall können wir das obige Lemma verwenden, um größere Räume (sogenannte Haupträume) zu finden. Wir erinnern uns daran, dass jeder Eigenraum der Kern eines Endomorphismus ist:
$$\operatorname{Eig}(f,\lambda) = \ker(f - \lambda \mathrm{Id}_V).$$
Nach dem Lemma von Fitting für $h := f - \lambda\mathrm{Id}_V$ gibt es eine eindeutig bestimmte Zahl d mit
$$\{0_V\} \subsetneq \ker(f - \lambda\mathrm{Id}_V) \subsetneq \ker((f-\lambda\mathrm{Id}_V)^2) \subsetneq \cdots \subsetneq \ker((f-\lambda\mathrm{Id}_V)^d) = \ker((f-\lambda\mathrm{Id}_V)^{d+i})$$
für alle $i \in \mathbb{N}$. Für $U := \ker((f-\lambda\mathrm{Id}_V)^d)$ gilt $\dim_K(U) = \mu_a(h,0) \geq d$ und U ist h-invariant. Wir haben
$$\chi_h(t) := \det(t\mathrm{Id}_V - h) = \det(t\mathrm{Id}_V - (f - \lambda\mathrm{Id}_V)) = \det((t+\lambda)\mathrm{Id}_V - f) = \chi_f(t+\lambda)$$
und daher folgt $\mu_a(f,\lambda) = \mu_a(h,0)$. Insbesondere gilt $U = \ker((f-\lambda\mathrm{Id}_V)^{\mu_a(f,\lambda)})$, da $\mu_a(f,\lambda) = \mu_a(h,0) \geq d$. Nach dem Lemma von Fitting haben wir
$$V = U \oplus W$$
wobei $W := \operatorname{Bild}((f-\lambda\mathrm{Id}_V)^d)$ und $\operatorname{Eig}(f,\lambda) \subset U$. Insbesondere ist $h|_U : U \to U$ nilpotent und $h|_W : W \to W$ ist ein Isomorphismus.

Definition. Sei $f : V \to V$ ein linearer Endomorphismus eines endlichdimensionalen K-Vektorraumes. Für einen Eigenwert λ von f definieren wir den *Hauptraum* von f zum Eigenwert λ durch [30.04.18]
$$\operatorname{Hau}(f,\lambda) := \ker((f-\lambda\mathrm{Id}_V)^{\mu_a(f,\lambda)}).$$

Satz 1.4 (Jordan-Zerlegung)**.** *Sei $f : V \to V$ ein linearer Endomorphismus eines endlichdimensionalen K-Vektorraumes, so dass*
$$\chi_f(t) = \prod_{i=1}^{k} (t-\lambda_i)^{r_i}$$
in Linearfaktoren in $K[t]$ zerfällt, wobei $\lambda_1, \ldots, \lambda_k$ die paarweise verschiedene Eigenwerte sind und $r_i = \mu_a(f,\lambda_i)$. Dann gelten:

(1) Jeder Hauptraum $\operatorname{Hau}(f,\lambda_i)$ *ist f-invariant mit Dimension r_i,*

(2) V ist die direkte Summe der Haupträume von f:
$$V = \bigoplus_{i=1}^{k} \operatorname{Hau}(f,\lambda_i),$$

(3) Es gibt eine Jordan-Zerlegung $f = f_N + f_D$ *mit f_N nilpotent, f_D diagonalisierbar und $f_N \circ f_D = f_D \circ f_N$.*

Korollar. Jeder lineare Endomorphismus f eines endlichdimensionalen $\mathbb{C}$-Vektorraumes V hat eine Jordan-Zerlegung $f = f_D + f_N$ (und die entsprechende Aussage für komplexe Matrizen gilt).

Beispiel. Sei
$$A = \begin{pmatrix} 2 & -3 \\ 3 & -4 \end{pmatrix} \in \operatorname{Mat}_{2\times 2}(K).$$

Dann $\chi_A(t) = (t+1)^2$, also $\lambda := -1$ ist ein Eigenwert von A mit $\mu_a(A, -1) = 2$. Da das charakteristische Polynom von A in Linearfaktoren zerfällt, hat A (und die entsprechende Abbildung $F_A : K^2 \to K^2$) eine Jordan-Zerlegung. Es gilt

$$\mathrm{Eig}(A, -1) = \mathrm{Span}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \subsetneq \mathrm{Hau}(A, -1) := \ker((-I_2 - A)^2) = \ker\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = K^2.$$

Deshalb haben wir die Jordan-Zerlegung $K^2 = \mathrm{Hau}(A, -1)$. Ferner gibt es eine nilpotente Matrix N und eine diagonale Matrix D mit $ND = DN$, so dass $A \sim D + N$ (nach Teil (3) des Satzes 1.4). Die Matrix

$$B := A - (-1I_2) = \begin{pmatrix} 3 & -3 \\ 3 & -3 \end{pmatrix}$$

ist nilpotent (B ist analog zu der Abbildung $g_i = f - \lambda_i \mathrm{Id}_V$ in dem Beweis des Satzes 1.4) und deshalb gibt es eine geordnete Basis

$$\mathcal{A} = \left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right) \quad \text{mit} \quad M_{\mathcal{A}}^{\mathcal{A}}(F_B) = \begin{pmatrix} 0 & 6 \\ 0 & 0 \end{pmatrix} =: N$$

Dann gilt

$$A \sim M_{\mathcal{A}}^{\mathcal{A}}(F_A) = M_{\mathcal{A}}^{\mathcal{A}}(-1\mathrm{Id}_{K^2}) + M_{\mathcal{A}}^{\mathcal{A}}(B) = D + N$$

mit $D = -I_2$.

1.6. **Jordan-Normalform.** Für $d \in \mathbb{N}$ definieren wir den (nilpotenten) Jordanblock

$$J_d := \begin{pmatrix} 0 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{pmatrix} \in \mathrm{Mat}_{d \times d}(K)$$

und für $\lambda \in K$ definieren wir den *Jordan-Block* $J_d(\lambda) = \lambda I_d + J_d \in \mathrm{Mat}_{d \times d}(K)$.

Definition. Wir sagen eine Matrix A in *Jordan-Normalform* (JNF) ist, falls A eine blockdiagonale Form hat, die aus Jordan-Blöcke entsteht, d.h.

$$A = \begin{pmatrix} J_{d_1}(\mu_1) & & 0 \\ & \ddots & \\ 0 & & J_{d_s}(\mu_s) \end{pmatrix},$$

wobei $\mu_i = \mu_j$ und $d_i = d_j$ möglich ist. Wir sagen, dass A eine *Jordan-Normalform* hat, wenn A ähnlich zu einer Matrix in JNF ist. Für einen Endomorphismus $f \in \mathrm{End}_K(V)$ eines endlichdimensionalen K-Vektorraumes V sagen wir, dass f eine Jordan-Normalform hat, wenn für eine geordnete Basis $\mathcal{A}$ von V die Matrix $M_{\mathcal{A}}^{\mathcal{A}}(f)$ eine JNF hat.

[02.05.18]

Satz 1.5 (Jordan-Normalform für nilpotente Endomorphismen)**.** *Sei $g : V \to V$ ein nilpotenter Endomorphismus eines n-dimensionalen K-Vektorraumes V und $d := \min\{r \in \mathbb{N} : g^r = 0\}$. Dann gibt es eindeutig bestimmte Zahlen $s_1, \dots, s_d \in \mathbb{N}$ mit*

$$\sum_{k=1}^{d} k s_k = n$$

und eine geordnete Basis $\mathcal{A}$ von V, so dass $M^{\mathcal{A}}_{\mathcal{A}}(g)$ in JNF ist:

$$M^{\mathcal{A}}_{\mathcal{A}}(g) = \begin{pmatrix} J_d & & & & & & \\ & \ddots & & & & & \\ & & J_d & & & & \\ & & & \ddots & & & \\ & & & & \ddots & & \\ & & & & & J_1 & \\ & & & & & & \ddots & \\ & & & & & & & J_1 \end{pmatrix}$$

mit s_k Kopien von J_k.

Bemerkung. Nach dem Beweis des Satzes 1.5 folgt, dass $s_d > 0$.

Beispiel. Für die folgende nilpotente Matrix

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{mit} \quad A^2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad A^3 = 0$$

finden wir eine JNF von A wie folgt. Sei $d := \min\{r \in \mathbb{N} : A^r = 0\} = 3$ und für $0 \le i \le 3$ sei $U_i := \ker(A^i) = \{x \in K^3 : A^i x = 0\}$, dann

$$\{0\} = U_0 \subsetneq U_1 = \operatorname{Span}(e_1) \subsetneq U_2 = \operatorname{Span}(e_1, e_2) \subsetneq U_3 = K^3.$$

Wir finden eine Zerlegung $K^3 = U_2 \oplus W_3$ mit $W_3 = \operatorname{Span}(e_3)$. Es gilt $A(W_3) = A(\operatorname{Span}(e_3)) = \operatorname{Span}(Ae_3) = \operatorname{Span}(e_1 + e_2) \subset U_2$. Wir müssen eine Zerlegung $K^3 = U_1 \oplus W_2 \oplus W_3$ finden mit $A(W_3) \subset W_2$. Aus $\dim(U_1) = \dim(W_3) = 1$ folgt $\dim(W_2) = 1$, also $W_2 = \operatorname{Span}(e_1 + e_2)$. Dann ist $W_1 = U_1 = \operatorname{Span}(e_1)$ und

$$K^3 = W_1 \oplus W_2 \oplus W_3 = \operatorname{Span}(e_1) \oplus \operatorname{Span}(e_1 + e_2) \oplus \operatorname{Span}(e_3).$$

Es gilt $s_3 = \dim(W_3) = 1$ und $s_2 = \dim(W_2) - \dim(W_3) = 0$ und $s_1 = \dim(W_1) - \dim(W_2) = 0$. Wir wählen eine Basis von K^3 wie folgt: sei $v_1^{(3)} := e_3$ eine Basis von W_3 und wir erweitern $A(v_1^{(3)}) = Ae_3 = e_1 + e_2$ zu einer Basis von W_2 (da $s_2 = 0$ haben wir die triviale Erweiterung mit 0 zusätzlichen Vektoren) und wir erweitern $A(e_1 + e_2) = A^2(e_3) = e_1$ zu einer Basis von W_1 (wegen $s_1 = 0$ ist diese Erweiterung trivial).

$$\begin{array}{ll} \text{Basis von } W_3: & v_1^{(3)} = e_3 \\ \text{Basis von } W_2: & A(v_1^{(3)}) = e_1 + e_2 \\ \text{Basis von } W_3: & A^2(v_1^{(3)}) = e_1 \end{array}$$

Für $\mathcal{A} = (A^2(v_1^{(3)}), A(v_1^{(3)}), v_1^{(3)}) = (e_1, e_1 + e_2, e_3)$ ist

$$M^{\mathcal{A}}_{\mathcal{A}}(F_A) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

in Jordan-Normalform. Für die standard Basis $\mathcal{B} = (e_1, e_2, e_3)$ ist $M^{\mathcal{B}}_{\mathcal{B}}(F_A) = A$ und nach dem Basiswechselsformel gilt

$$M^{\mathcal{A}}_{\mathcal{A}}(F_A) = SAS^{-1} \text{ mit } S := M^{\mathcal{B}}_{\mathcal{A}}(\mathrm{Id}_{K^3}) = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

[07.05.18]

Satz 1.6. *Sei $f : V \to V$ ein linearer Endomorphismus eines endlichdimensionalen K-Vektorraumes V, so dass das charakteristische Polynom von f*

$$\chi_f(t) = \prod_{i=1}^{k} (t - \lambda_i)^{r_i}$$

in Linearfaktoren zerfällt mit $\lambda_1, \dots, \lambda_k$ die paarweise verschiedenen Eigenwerte von f. Dann gibt es eine Basis $\mathcal{A}$ von V, so dass

$$M_{\mathcal{A}}^{\mathcal{A}}(f) = \begin{pmatrix} \lambda_1 I_{r_1} + N_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 I_{r_2} + N_2 & \ddots & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \dots & 0 & \lambda_k I_{r_k} + N_k \end{pmatrix}$$

mit $N_i \in \mathrm{Mat}_{r_i \times r_i}(K)$ nilpotente Matrizen in Jordan-Normalform. Insbesondere ist $M_{\mathcal{A}}^{\mathcal{A}}(f)$ in JNF, also hat f eine JNF.

Lemma.

(1) Zwei Jordan-Blöcke $J_r(\lambda)$ und $J_s(\mu)$ sind genau dann ähnlich, wenn $r = s$ und $\lambda = \mu$.
(2) Zwei Matrizen in JNF A und B sind genau dann ähnlich, wenn sie die gleiche Anzahl von jedem Jordan-Block $J_r(\lambda)$ haben.

[09.05.18]

Satz 1.7. *Die Jordan-Normalform eines Endomorphismus f eines endlichdimensionalen K-Vektorraumes mit einem charakteristischen Polynom, das in Linearfaktoren zerfällt, ist bis auf die Reihenfolge der Jordan-Blöcke eindeutig durch f bestimmt, d.h. unabhängig von der Wahl der Basis.*

Korollar. Jede komplexe Matrix hat eine JNF, d.h. in der Ähnlichkeitsklasse der komplexen Matrix gibt es eine Matrix in JNF. Ferner klassifiziert die Jordan-Normalform (bis auf die Reihenfolge der Jordan-Blöcke) alle komplexen Matrizen bis auf Ähnlichkeit, d.h. in jeder Ähnlichkeitsklasse einer komplexen Matrix gibt es genau eine Matrix in JNF (bis auf die Reihenfolge der Jordan-Blöcke).

Beispiel. Sei A eine Matrix mit dem charakteristischen Polynom $\chi_A(t) = (t-5)(t-3)^2$. Mit nur diesen Informationen können wir die mögliche JNF wie folgt bestimmen. Die Eigenwerte sind $\lambda_1 = 5$ und $\lambda_2 = 3$ und es gilt für jeder Eigenwert λ_i von A:

$$\dim_K(\mathrm{Hau}(A, \lambda_i)) = \mu_a(A, \lambda_i) \geq \mu_g(A, \lambda_i) \geq 1.$$

Wegen $\mu_a(A, 5) = 1$, folgt $\mu_g(A, 5) = 1$ und wegen $\mu_a(A, 3) = 2$, folgt $\mu_g(A, 3) = 1$ oder $\mu_g(A, 3) = 2$. Um die JNF zu berechnen, betrachen wir die nilpotente Abbildungen

$$g_i := (F_A - \lambda_i \mathrm{Id})|_{\mathrm{Hau}(A,\lambda_i)} : \mathrm{Hau}(A, \lambda_i) \to \mathrm{Hau}(A, \lambda_i)$$

und wenn $d_i := \min\{r \in \mathbb{N} : g_i^r \equiv 0\}$, gibt es Zahlen $s_1^{(i)}, \dots, s_{d_i}^{(i)} \in \mathbb{N}$, die eindeutig durch g_i definiert wird, mit

$$\sum_{j=1}^{d_i} j s_j^{(i)} = \mu_a(A, \lambda_i) \tag{1}$$

(Satz 1.5). Ferner gilt

$$0 < d_i \leq \dim_K(\mathrm{Hau}(A, \lambda_i)) = \mu_a(A, \lambda_i). \tag{2}$$

Dann hat die JNF von A den Jordan-Block $J_j(\lambda_i)$ mit der Vielfalt $s_j^{(i)}$.

Für $\lambda_1 = 5$ folgt es, dass $d_1 = 1$ nach (2) und $s_1^{(1)} = 1$ nach (1). Dann die JNF von g_1 hat $1 = s_1^{(1)}$ Jordan-Block J_1 und die JNF von A hat $1 = s_1^{(1)}$ Jordan-Block $J_1(5)$.

Für $\lambda_2 = 3$ folgt es, dass $d_2 = 1$ oder $d_2 = 2$ nach (2). Wenn $d_2 = 1$, dann ist $s_1^{(2)} = 2$ nach (1) und g_2 hat $2 = s_1^{(2)}$ Jordan-Blöcke J_1 und A hat $2 = s_1^{(2)}$ Jordan-Blöcke $J_1(3)$. Wenn $d_2 = 2$ gibt es Zahlen $s_1^{(2)}, s_2^{(2)} \in \mathbb{N}$ mit $1s_1^{(2)} + 2s_2^{(2)} = \mu_a(A, \lambda_2) = 2$ und wegen $s_{d_i}^{(i)} > 0$ (siehe die Bemerkung nach dem Satz 1.5) haben wir $s_1^{(2)} = 0$ und $s_2^{(2)} = 1$. In diesem Fall hat g_2 einen (da $s_2^{(2)} = 1$) Jordan-Block J_2 und A hat $1 = s_2^{(2)}$ Jordan-Block $J_2(3)$.

Abschließend gibt es zwei Möglichkeiten:

a) Wenn ($d_1 = 1, s_1^{(1)} = 1$) und ($d_2 = 1, s_1^{(2)} = 2$), ist die JNF von A
$$\begin{pmatrix} 5 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$
und das Minimalpolynom von A ist $m_A(t) = (t-5)(t-3)$.

b) Wenn ($d_1 = 1, s_1^{(1)} = 1$) und ($d_2 = 2, s_1^{(2)} = 0, s_2^{(2)} = 2$), ist die JNF von A
$$\begin{pmatrix} 5 & 0 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 3 \end{pmatrix}$$
und das Minimalpolynom von A ist $m_A(t) = (t-5)(t-3)^2$.

Definition. Eine Funktion $j : \mathrm{Mat}_{n\times n}(K) \to X$ (für eine Menge X) heißt *Invariant* für Matrizen (bis auf Ähnlichkeit), falls j konstant auf jeder Ähnlichkeitsklasse ist, so dass, es eine induziierte Abbildung gibt [14.05.18]
$$\bar{j} : \mathrm{Mat}_{n\times n}(K)/\sim \ \to X.$$

Beispiel. Die folgenden Funktionen sind Invarianten für Matrizen (bis auf Ähnlichkeit):

(1) das charakteristische Polynom $\chi : \mathrm{Mat}_{n\times n}(K) \to K[t]$,
(2) das Minimalpolynom $m : \mathrm{Mat}_{n\times n}(K) \to K[t]$,
(3) die Determinante $\det : \mathrm{Mat}_{n\times n}(K) \to K$,
(4) die Spurabbildung $\mathrm{Spur} : \mathrm{Mat}_{n\times n}(K) \to K$,
(5) der Rang einer Matrix $\mathrm{Rang} : \mathrm{Mat}_{n\times n}(K) \to \mathbb{N}$,
(6) die Menge der Eigenwerte $\mathrm{Eig} : \mathrm{Mat}_{n\times n}(K) \to \{\text{endliche Teilmenge von } K\}$,
(7) die algebraische (bzw. geometrische) Vielfachheiten von $\lambda \in K$:
$$\mu_a(-, \lambda) : \mathrm{Mat}_{n\times n}(K) \to \mathbb{N} \quad (\text{bzw. } \mu_g(-, \lambda) : \mathrm{Mat}_{n\times n}(K) \to \mathbb{N}).$$
(8) (falls K algebraisch abgeschlossen ist, so dass jede Matrix eine JNF hat) die Anzahl $s_k(\lambda) : \mathrm{Mat}_{n\times n}(K) \to \mathbb{N}$ von jedem Jordan-Block $J_k(\lambda)$ in einer JNF einer Matrix.

2. Bilinearformen und quadratische Formen

2.1. **Bilinearformen.** Seien V, W und U Vektorräume über einen Körper K. Zur Erinnerung: eine Abbildung $f : V \to W$ heißt K-linear (oder linear), wenn für alle $v, v' \in V$ und $\lambda \in K$ gilt
$$f(v + v') = f(v) + f(v') \quad \text{und} \quad f(\lambda \cdot v) = \lambda \cdot f(v),$$
oder, äquivalent, für alle $v, v' \in V$ und $\mu, \lambda \in K$ gilt
$$f(\mu v + \lambda v') = \mu f(v) + \lambda f(v').$$

Definition.

(1) Eine Abbildung $f : V \times W \to U$ heißt *bilinear*[6], wenn für alle Vektoren $v, v' \in V$ und $w, w' \in W$ und Elemente $\mu, \lambda \in K$ gilt

i) $f(\mu v + \lambda v', w) = \mu f(v, w) + \lambda f(v', w)$,
ii) $f(v, \mu w + \lambda w') = \mu f(v, w) + \lambda f(v, w')$.

[6]Man kann diese Definition erweitern: wenn $V_1, \cdots, V_n$ und W K-Vektorräume sind, heißt eine Abbildung $f : V_1 \times V_2 \times \cdots \times V_n \to W$ *multilinear*, wenn f in jeder Komponente linear ist, d.h. für alle $1 \le i \le n$ und für alle $v_j \in V_j$ für $j \neq i$ ist die Abbildung $V_i \to W$, die durch $v_i \mapsto f(v_1, \cdots, v_n)$ definiert wird, linear.

(2) Eine *bilineare Paarung* zwischen V und W ist eine bilineare Abbildung $f : V \times W \to K$.
(3) Eine *Bilinearform* (BLF) auf V ist eine bilinear Abbildung $b : V \times V \to K$. Wenn $\dim_K V = n \in \mathbb{N}$ und $\mathcal{A} = (v_1, \cdots, v_n)$ eine geordnete Basis von V ist, dann nennen wir die Matrix $B := (b(v_i, v_j))_{1 \leq i,j \leq n} \in \mathrm{Mat}_{n\times n}(K)$ *die Matrix zu der Bilinearform b bezüglich der Basis $\mathcal{A}$* und wir schreiben $B = b(\mathcal{A}, \mathcal{A})$. Die Menge der Bilinearformen auf V wird mit $\mathrm{Bil}_K(V)$ bezeichnet.

Beispiel.

(1) Die Abbildung $b : K^2 \times K^2 \to K$, die durch

$$b\left(\left(\begin{array}{c} x_1 \\ x_2 \end{array}\right), \left(\begin{array}{c} y_1 \\ y_2 \end{array}\right)\right) := x_1y_2 - x_2y_1$$

definiert wird, ist bilinear. Für die geordnete Basis (e_1, e_2) von K^2 ist die zugehörige Matrix

$$B = \left(\begin{array}{cc} 0 & 1 \\ -1 & 0 \end{array}\right).$$

(2) Die *kanonische Bilinearform* auf K^n ist die Abbildung $b : K^n \times K^n \to K$

$$b(x, y) = \sum_{i=1}^{n} x_iy_i$$

und die zugehörige Matrix für die geordnete Standardbasis $\mathcal{A} = (e_1, \ldots, e_n)$ von K^n ist die Einheitsmatrix: $I_n = b(\mathcal{A}, \mathcal{A})$.

(3) Für jeder K-Vektorraum V mit dem Dualraum $V^* := \mathrm{Hom}_K(V, K)$ ist die Abbildung $b : V^* \times V \to K$

$$b(\varphi, v) := \varphi(v)$$

eine bilineare Paarung zwischen V^* und V.

Bemerkung. Sei V ein K-Vektorraum der endlichen Dimension n und $\mathcal{A} = (v_1, \cdots, v_n)$ eine geordnete Basis von V. Dann gibt es genau einen linearen Isomorphismus $\Phi_{\mathcal{A}} : V \to K^n$ mit $\Phi_{\mathcal{A}}(v_i) = e_i$ für $1 \leq i \leq n$ [LAI, Satz 4.4].

(1) Wenn $b : V \times V \to K$ eine Bilinearform ist und B die Matrix zu b bzgl. der Basis $\mathcal{A}$ ist, dann gilt für alle $v, v' \in V$

$$b(v, v') = \Phi_{\mathcal{A}}(v)^t \, B \, \Phi_{\mathcal{A}}(v').$$

(2) Umgekehrt definiert $B \in \mathrm{Mat}_{n\times n}(K)$ eine Bilinearform $b_B^{\mathcal{A}}$ auf V durch

$$b_B^{\mathcal{A}}(v, v') := \Phi_{\mathcal{A}}(v)^t \, B \, \Phi_{\mathcal{A}}(v')$$

und die zugehörige Matrix dieser Bilinearform $b_B^{\mathcal{A}}$ bzgl. der Basis $\mathcal{A}$ ist wieder B.

Bemerkung. Man kann Bilinearformen auf V punktweise addieren: für Bilinearformen $b_1, b_2 : V \times V \to K$ definieren wir $b_1 + b_2 : V \times V \to K$ durch

$$(b_1 + b_2)(v, v') := b_1(v, v') + b_2(v, v'),$$

und $b_1 + b_2$ ist auch bilinear. Man kann auch eine Bilinearform $b : V \times V \to K$ mit einem Skalar $\lambda \in K$ multiplizieren, um eine neue Bilinearform $\lambda \cdot b : V \times V \to K$ zu definieren

$$(\lambda \cdot b)(v, v') := \lambda \cdot b(v, v').$$

Deshalb ist die Menge der Bilinearformen auf V ein Untervektorraum des K-Vektorraumes $\mathrm{Abb}(V \times V, K)$ der Abbildungen von $V \times V$ nach K.

Satz 2.1. *Sei V ein K-Vektorraum der endlichen Dimension n und $\mathcal{A} = (v_1, \cdots, v_n)$ eine geordnete Basis von V. Die Abbildung*

$$\Psi_{\mathcal{A}} : \mathrm{Bil}_K(V) \to \mathrm{Mat}_{n\times n}(K),$$

die zu jeder Bilinearform b die zugehörige Matrix $B = b(\mathcal{A}, \mathcal{A})$ bzgl. der Basis $\mathcal{A}$ zuordnet, ist ein linearer Isomorphismus.

[16.05.18]

Satz 2.2 (Basiswechsel)**.** *Seien $\mathcal{A}, \mathcal{B}$ geordnete Basen eines endlichdimensionalen K-Vektorraumes V. Dann gilt für eine Bilinearform b auf V*

$$b(\mathcal{B}, \mathcal{B}) = M^{\mathcal{B}}_{\mathcal{A}}(Id_V)^t\, b(\mathcal{A}, \mathcal{A})\, M^{\mathcal{B}}_{\mathcal{A}}(Id_V)$$

wobei $M^{\mathcal{B}}_{\mathcal{A}}(Id_V)$ die Basiswechselmatrix für die Identität auf V ist.

Definition. Zwei Matrizen $A, B \in \mathrm{Mat}_{n\times n}(K)$ heißen *kongruent*, wenn es eine Matrix $S \in \mathrm{GL}_n(K)$ gibt mit $A = S^tBS$. Schreibweise: $A \approx B$.

Übung. Die Relation der Kongruenz auf $\mathrm{Mat}_{n\times n}(K)$ ist eine Äquivalenzrelation. Für eine Bilinearform b auf einem K-Vektorraum der Dimension n sind alle die Matrizen $b(\mathcal{A}, \mathcal{A})$ für verschiedene geordnete Basen $\mathcal{A}$ von V kongruent (nach der Basiswechsel-Formel).

Bemerkung. Wenn $b : V \times V \to K$ eine Bilinearform auf V ist, können wir eine Abbildung $f_b : V \to V^*$ durch

$$f_b(v) := b(-, v) : V \to K$$

definieren. Wegen der Linearität von b im ersten Argument ist f_b wohldefiniert. Wegen der Linearität von b im zweiten Argument ist f_b linear.

Wenn $\dim_K(V) = n$ und $\mathcal{A} = (v_1, \ldots, v_n)$ eine geordnete Basis von V ist, können wir die zugehörige Matrix $C := M^{\mathcal{A}}_{\mathcal{A}^*}(f_b) \in \mathrm{Mat}_{n\times n}(K)$ betrachten (wobei $\mathcal{A}^*$ die duale Basis ist). Es gilt

$$f_b(v_j) = \sum_{i=1}^{n} c_{ij} v_i^*$$

und deshalb folgt es, dass

$$b(v_k, v_j) =: f_b(v_j)(v_k) = \sum_{i=1}^{n} c_{ij} v_i^*(v_k) = c_{kj}$$

d.h. $M^{\mathcal{A}}_{\mathcal{A}^*}(f_b)$ ist die Matrix $b(\mathcal{A}, \mathcal{A})$ zu b bzgl. $\mathcal{A}$.

Satz 2.3. *Sei V ein endlichdimensionalen K-Vektorraum. Dann ist die Abbildung*

$$\begin{array}{ccc} \mathrm{Bil}_K(V) & \to & \mathrm{Hom}_K(V, V^*) \\ b & \mapsto & f_b : V \to V^* \end{array}$$

ein linearer Isomorphismus.

2.2. **Symmetrische Formen.** Zur Erinnerung: eine Matrix $A \in \mathrm{Mat}_{n\times n}(K)$ heißt symmetrisch, wenn $A^t = A$. Sei $\mathrm{Mat}^{\mathrm{Sym}}_{n\times n}(K)$ die Teilmenge von $\mathrm{Mat}_{n\times n}(K)$, die symmetrische Matrizen enthält.

Definition. Eine Bilinearform b auf einem K-Vektorraum V heißt

(1) *symmetrisch*, wenn $b(v, v') = b(v', v)$ für alle $v, v' \in V$. Die Menge aller symmetrischen Bilinearformen auf V bildet ein Untervektorraum $\mathrm{Bil}^{\mathrm{sym}}(V)$ von $\mathrm{Bil}(V)$.
(2) *antisymmetrisch*, wenn $b(v, v') = -b(v', v)$ für alle $v, v' \in V$.

Eine Matrix $A \in \mathrm{Mat}_{n\times n}(K)$ heißt *antisymmetrisch*, wenn $A^t = -A$.

Bemerkung.

(1) Die Menge $\mathrm{Bil}^{\mathrm{sym}}(V)$ (bzw. $\mathrm{Bil}^{\text{a-sym}}(V)$) aller symmetrischen (bzw. antisymmetrischen) Bilinearformen ist ein Untervektorraum von $\mathrm{Bil}(V)$. Ebenso ist die Menge $\mathrm{Mat}^{\mathrm{sym}}_{n\times n}(K)$ (bzw. $\mathrm{Mat}^{\text{a-sym}}_{n\times n}(K)$) aller symmetrischen (bzw. antisymmetrischen) ein Untervektorraum von $\mathrm{Mat}_{n\times n}(K)$.

(2) Wenn $2 := 1 + 1 = 0$ in K stimmen die Begriffe symmetrische und antisymmetrisch überein.

(3) Wenn $2 \neq 0$ in K (so dass $2 \in K$ invertierbar ist), dann gilt

$$\mathrm{Mat}_{n\times n}(K) = \mathrm{Mat}^{\mathrm{sym}}_{n\times n}(K) \oplus \mathrm{Mat}^{\text{a-sym}}_{n\times n}(K),$$

weil eine $n \times n$-Matrix A die Form $A = \frac{1}{2}(A + A^t) + \frac{1}{2}(A - A^t)$ hat.

Lemma. Sei b eine Bilinearform auf einem K-Vektorraum V der Dimension n. Die zugehörige Matrix $B = b(\mathcal{A}, \mathcal{A})$ bzgl. einer geordneten Basis $\mathcal{A}$ von V ist genau dann symmetrisch (bzw. antisymmetrisch), wenn b symmetrisch (bzw. antisymmetrisch) ist. Ferner gibt es einen linearen Isomorphismus

$$\begin{array}{ccc} \mathrm{Bil}^{\mathrm{sym}}(V) & \to & \mathrm{Mat}^{\mathrm{sym}}_{n\times n}(K) \\ b & \mapsto & b(\mathcal{A}, \mathcal{A}) \end{array}.$$

Beispiel. Die *kanonische Bilinearform* $b : K^n \times K^n \to K$

$$b(x, y) = \sum_{i=1}^{n} x_i y_i$$

ist symmetrisch.

Definition. Eine Bilinearform b auf einem K-Vektorraum V heißt alternierend, wenn $b(v, v) = 0$ für alle $v \in V$.

Lemma. Sei $b : V \times V \to K$ eine Bilinearform.

(1) Wenn b alternierend ist, dann ist b antisymmetrisch.

(2) Wenn $2 \neq 0 \in K$ und b antisymmetrisch ist, dann ist b alternierend.

[23.05.18]

2.3. Orthogonalität und nicht ausgeartete Formen.

Definition. Sei $b : V \times V \to K$ eine Bilinearform auf einem K-Vektorraum V. Wir sagen, dass $v \in V$ *orthogonal* zu $w \in V$ ist (bzgl. b), wenn $b(v, w) = 0$ und wir schreiben $v \perp w$. Für eine Teilmenge $M \subset V$ definieren wir die Menge $M^\perp$ aller Vektoren, die *rechtsorthogonal* auf M bzgl. b sind

$$M^\perp := \{v \in V : b(m, v) = 0\, \forall m \in M\}$$

und die Menge ${}^\perp M$ aller Vektoren, die *linksorthogonal* auf M bzgl. b sind

$${}^\perp M := \{v \in V : b(v, m) = 0\, \forall m \in M\}.$$

Die Menge $M^\perp$ (bzw. ${}^\perp M$) heißt Rechtsorthogonalraum (bzw. Linksorthogonalraum) von M in V.

Bemerkung. Wenn b symmetrisch oder alternierend ist, dann gilt $v \perp w \iff w \perp v$. Insbesondere ist $M^\perp = {}^\perp M$ für alle $M \subset V$.

Beispiel. Für die kanonische Bilinearform auf K^3 und $M = \{e_1, e_2\}$ gilt

$$M^\perp := \left\{ x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} : b(e_1, x) = b(e_2, x) = 0 \right\} = \mathrm{Span}(e_3) = {}^\perp M.$$

Lemma. Sei $b : V \times V \to K$ eine Bilinearform auf einem K-Vektorraum V und $M \subset V$ eine Teilmenge. Dann sind $M^\perp$ und ${}^\perp M$ Untervektorräume von V.

Definition. Eine Bilinearform b auf einem K-Vektorraum V heißt *nicht ausgeartet*, wenn für alle $v \in V$ gelten die folgende Aussagen:

(1) $b(v', v) = 0$ für alle $v' \in V \implies v = 0$ (d.h. $V^\perp = \{0_V\}$),
(2) $b(v, v') = 0$ für alle $v' \in V \implies v = 0$ (d.h. ${}^\perp V = \{0_V\}$).

Sonst sagen wir, dass b *ausgeartet* ist.

Beispiel.

(1) Die kanonische Bilinearform auf K^n

$$b(x, y) = \sum_{i=1}^{n} x_i y_i$$

ist nicht ausgeartet: aus $b(x, y) = 0$ für alle $y \in K^n$ folgt $x = 0$, da $b(x, e_i) = x_i$, und aus $b(x, y) = 0$ für alle $x \in K^n$ folgt $y = 0$.

(2) Sei $b : K^2 \times K^2 \to K$ die Bilinearform

$$b\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}\right) := x_1 y_1 + x_2 y_1$$

mit zugehörigen Matrix

$$b(\mathcal{A}, \mathcal{A}) = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$$

bzgl. der Standardbasis $\mathcal{A} = (e_1, e_2)$. Diese Bilinearform ist nicht symmetrisch und für $M = \{e_2\}$ gilt $M^\perp \neq {}^\perp M$:

$$b\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}\right) = y_1 \quad \text{so dass} \quad M^\perp = \left\{\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \in K^2 : y_1 = 0\right\}$$

und

$$b\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = 0 \quad \text{so dass} \quad {}^\perp M = K^2.$$

Diese Bilinearform b ist ausgeartet, weil

$$(K^2)^\perp = \left\{\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \in K^2 : y_1 = 0\right\} \neq \{0_V\}.$$

Zur Erinnerung: für einen K-Vektorraum V und eine Bilinearform $b : V \times V \to K$ gibt es eine lineare Abbildung $f_b : V \to V^*$ mit

$$f_b(v) := b(-, v) : V \to K$$

und wenn $\mathcal{A} = (v_1, \ldots, v_n)$ eine geordnete Basis von V ist, gilt $M^{\mathcal{A}}_{\mathcal{A}^*}(f_b) = b(\mathcal{A}, \mathcal{A})$.

Satz 2.4. *Sei $b : V \times V \to K$ eine Bilinearform auf einem endlichdimensionalen K-Vektorraum V mit einer geordneten Basis $\mathcal{A}$. Dann sind die folgenden Bedingungen äquivalent:*

(1) b ist nicht ausgeartet,
(2) $V^\perp = \{0_V\}$,
(3) ${}^\perp V = \{0_V\}$,
(4) die zugehörige Matrix $B = b(\mathcal{A}, \mathcal{A})$ ist invertierbar,
(5) die lineare Abbildung $f_b : V \to V^*$, die durch $v \mapsto b(-, v)$ definiert wird, ist ein Isomorphismus.

Beispiel. Die Einschränkung einer nicht ausgearteten Bilinearform kann ausgeartet sein: für $V = K^2$ und die Bilinearform

$$b(x,y) := x_1y_2 + x_2y_1,$$

ist $b|_{U\times U} \equiv 0$ für $U := \mathrm{Span}(e_1) \subset V$. Insbesondere ist b nicht ausgeartet, aber $b|_{U\times U}$ ist ausgeartet.

Definition. Sei U ein Untervektorraum eines K-Vektorraumes V. Dann definieren wir den *Annullator* von U

$$\mathrm{Ann}(U, V^*) := \{\varphi \in V^* : \varphi(u) = 0_V \ \forall\, u \in U\} \subset V^*.$$

Für $W \subset V^*$, definieren wir $\mathrm{Ann}(W, (V^*)^*) \subset (V^*)^*$ wie oben und

$$\mathrm{Ann}(W, V) := \{v \in V : \varphi(v) = 0_V \ \forall\, \varphi \in W\} \subset V.$$

Bemerkung. Sei V ein K-Vektorraum und $U \subset V$ und $W \subset V^*$ Untervektorräume.

(1) Der Annullator $\mathrm{Ann}(U, V^*)$ ist ein Untervektorraum von V^*.
(2) Wenn V endlichdimensional ist, wir behaupten dass

$$\dim_K(\mathrm{Ann}(U, V^*)) = \dim_K(V) - \dim_K(U).$$

Seien $\{u_1, \cdots, u_r\}$ eine Basis von U und $\mathcal{B} = \{u_1, \cdots, u_r, v_1, \cdots, v_s\}$ eine Basis von V, dann sind die Linearformen $v_i^* \in \mathrm{Ann}(U, V^*) \subset V^*$ für $1 \leq i \leq s$ linear unabhängig. Es gilt

$$\mathrm{Span}(v_1^*, \ldots, v_s^*) = \mathrm{Ann}(U, V^*),$$

da '$\subset$' klar ist, und jede Abbildung $\varphi \in \mathrm{Ann}(U, V^*) \subset V^*$ als eine Linearkombination der Basisvektoren $\mathcal{B}^*$ geschrieben werden kann:

$$\varphi = \lambda_1 u_1^* + \cdots + \lambda_r u_r^* + \mu_1 v_1^* + \cdots + \mu_s v_s^*$$

mit $\lambda_i = \varphi(u_i) = 0_K$ für $1 \leq i \leq r$. Daher ist $\{v_1^*, \ldots, v_s^*\}$ eine Basis von $\mathrm{Ann}(U, V^*)$.
(3) Wenn V endlichdimensional ist, haben wir einen linearen Isomorphismus

$$\begin{array}{cccc} \Phi : & V & \to & (V^*)^* \\ & v & \mapsto & \Phi_v : V^* \to K, \end{array}$$

wobei $\Phi_v(\varphi) := \varphi(v)$. Dann gilt $\Phi(\mathrm{Ann}(W, V)) = \mathrm{Ann}(W, (V^*)^*)$.

Satz 2.5. *Sei $b : V \times V \to K$ eine Bilinearform auf einem endlichdimensionalen K-Vektorraum V und U ein Untervektorraum von V. Dann gilt*

$$\dim(U) + \dim({}^{\perp}U) = \dim(V) + \dim(U \cap V^{\perp}).$$

und

$$\dim(U) + \dim(U^{\perp}) = \dim(V) + \dim(U \cap {}^{\perp}V).$$

[28.05.18] **Korollar.** Sei $b : V \times V \to K$ eine nicht ausgeartete Bilinearform auf einem endlichdimensionalen K-Vektorraum V. Für einen Untervektorraum $U \subset V$ gilt

$$\dim(V) = \dim(U) + \dim({}^{\perp}U) = \dim(U) + \dim(U^{\perp}).$$

Ferner haben wir $U = {}^{\perp}(U^{\perp}) = ({}^{\perp}U)^{\perp}$.

Korollar. Sei $b : V \times V \to K$ eine Bilinearform auf einem endlichdimensionalen K-Vektorraum V. Für einen Untervektorraum $U \subset V$ ist äquivalent:

(1) $b|_{U\times U}$ ist nicht ausgeartet,
(2) $V = U \oplus U^{\perp}$.

Übung. Sei K ein Korper mit $1+1\neq 0$ und V ein endlichdimensionaler K-Vektorraum. Für jede antisymmetrische Bilinearform $b: V\times V\to K$ beweisen Sie (durch Induktion nach $\dim(V)$), dass es eine Basis $\mathcal{A}$ von V gibt mit

$$b(\mathcal{A},\mathcal{A}) = \begin{pmatrix} 0 & 0 & & \cdots & & 0 \\ 0 & \ddots & \ddots & & & \\ & \ddots & 0 & \ddots & & \vdots \\ \vdots & & \ddots & S & \ddots & \\ & & & \ddots & \ddots & 0 \\ 0 & & \cdots & & 0 & S \end{pmatrix} \qquad \text{für } S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Was ist eine notwendige Bedingung für V eine nicht ausgeartete antisymmetrische Bilinearform zu haben?

2.4. **Quadratische Formen.**

Definition. Ein *Polynom in n Variablen $t_1,\cdots,t_n$ über K* ist ein formaler Ausdruck P der Form

$$P(t_1,\ldots,t_n) = \sum_{I=(i_1,\ldots,i_n)\in\mathbb{N}^n} a_I t_1^{i_1} t_2^{i_2}\cdots t_n^{i_n}$$

mit Koeffizienten $a_I\in K$, so dass nur endliche viele Koeffizienten a_I ungleich Null sind. Der Grad eines nicht-Null Polynoms P ist

$$\operatorname{grad}(P) := \max\{i_1+\cdots+i_n : a_I\neq 0\}.$$

Ein Polynom P heißt *homogen* vom Grad d, wenn für alle $I=(i_1,\ldots,i_n)\in\mathbb{N}^n$ gilt

$$a_I\neq 0 \implies i_1+\cdots+i_n = d.$$

Insbesondere ist das Nullpolynom homogen von jedem Grad d. Die Menge aller Polynome in n Variablen $t_1,\ldots,t_n$ über K wird mit $K[t_1,\ldots,t_n]$ bezeichnet; diese Menge ist eine Teilmenge der Menge $\operatorname{Abb}(K^n,K)$. Die Menge $K[t_1,\ldots,t_n]$ mit der Addition und Multiplikation von Polynome bildet einen Ring und ist auch ein K-Vektorraum. Die Teilmenge $K[t_1,\ldots,t_n]_d\subset k[t_1,\ldots,t_n]$ von allen homogenen Polynome des Grads d ist ein endlichdimensionalen Untervektorraum.

Übung. Ein Polynom $P(t_1,\cdots,t_n)$ in n Variablen über K ist homogen vom Grad d genau dann, wenn für alle $\lambda\in K$ gilt

$$P(\lambda\cdot t_1,\ldots,\lambda\cdot t_n) = \lambda^d P(t_1,\ldots,t_n).$$

Definition. Eine *quadratische Form* auf V ist eine Abbildung $q: V\to K$ mit den folgenden Eigenschaften:

(1) $q(\lambda\cdot v) = \lambda^2\cdot q(v)$ für alle $\lambda\in K$ und $v\in V$,
(2) Die Abbildung $\beta_q: V\times V\to K$

$$\beta_q(v,v') := q(v+v') - q(v) - q(v')$$

ist eine Bilinearform auf V. (Wir nennen β_q die zu q assoziierte Bilinearform).

Die quadratische Form q heißt *nicht ausgeartet*, falls β_q nicht ausgeartet ist. Die Menge aller quadratischen Formen auf V wird mit $\mathrm{QF}_K(V)$ bezeichnet.

Bemerkung. Insbesondere, wenn $q\not\equiv 0$ ist q nicht linear nach (1). Die assoziierte Bilinearform β_q ist symmetrisch. Ferner ist die Teilmenge $\mathrm{QF}_K(V)\subset\operatorname{Abb}(V,K)$ ein Untervektorraum.

Satz 2.6. *Sei $\mathcal{A}=(v_1,\cdots,v_n)$ eine geordnete Basis eines K-Vektorraumes V. Für eine Abbildung $q: V\to K$ definieren wir eine Abbildung $f_q^{\mathcal{A}}: K^n\to K$ durch*

$$f_q^{\mathcal{A}}(x_1,\ldots,x_n) := q(x_1\cdot v_1+\cdots+x_n\cdot v_n).$$

Die Abbildung q ist genau dann eine quadratische Form, wenn $f_q^{\mathcal{A}}$ ein homogenes Polynom vom Grad 2 ist.

Bemerkung. Sei V ein K-Vektorraum.

(1) Wenn b eine Bilinearform auf V ist, dann ist $q_b(v) := b(v,v)$ eine quadratische Form von V mit $\beta_{q_b}(v,v') = b(v,v') + b(v',v)$. Wenn $\mathcal{A}$ eine geordnete Basis von V ist, gilt
$$\beta_{q_b}(\mathcal{A},\mathcal{A}) = b(\mathcal{A},\mathcal{A}) + b(\mathcal{A},\mathcal{A})^t.$$
(2) Wenn b ist eine symmetrische Bilinearform auf V, gilt
$$2b(v,v') = b(v+v', v+v') - b(v,v) - b(v',v').$$
Die folgende 'Polarisierungs-Identität' folgt für die quadratische Form $q_b(v) := b(v,v)$
$$2b(v,v') = q_b(v+v') - q_b(v) - q_b(v')$$
Insbesondere gilt für die zugehörige Bilinearform β_{q_b} zu q_b die Gleichung $2b = \beta_{q_b}$.
(3) Falls $2 := 1+1 \neq 0 \in K$ und b eine symmetrische Bilinearform auf V ist, dann können wir b aus der quadratischen Form $q_b(v) := b(v,v)$ zurückgewinnen durch die Formel $b = \frac{1}{2}\beta_{q_b}$.

Beispiel. Für die kanonische symmetrische Bilinearform b auf K^n ist $q_b(x_1,\dots,x_n) = \sum_{i=1}^n x_i^2$.

[30.05.18] **Definition.** Die Charakteristik eines Körpers K ist
$$\mathrm{Char}(K) := \begin{cases} 0 & \text{falls } n := 1+\cdots+1 \neq 0 \in K \ \forall n \in \mathbb{N}^*, \\ \min\{n \in \mathbb{N}^* : n = 0 \in K\} & \text{sonst.} \end{cases}$$

Übung. Die Charakteristik eines Körpers ist entweder Null oder eine Primzahl.

Beispiel.

(1) $\mathrm{Char}(\mathbb{Q}) = \mathrm{Char}(\mathbb{R}) = \mathrm{Char}(\mathbb{C}) = 0$.
(2) $\mathrm{Char}(\mathbb{F}_p) = p$ für eine Primzahl p.

Satz 2.7. *Sei K ein Körper mit $\mathrm{Char}(K) \neq 2$ und V ein K-Vektorraum. Dann gibt es einen linearen Isomorphismus*
$$\begin{array}{ccc} \mathrm{Bil}_K^{sym}(V) & \to & \mathrm{QF}_K(V) \\ b & \mapsto & q_b \end{array}$$
mit $q_b(v) := b(v,v)$.

Bemerkung. Wenn $\dim_K(V) = n \in \mathbb{N}$ und $\mathrm{Char}(K) \neq 2$, dann gibt es Bijektionen
$$\mathrm{Mat}_{n\times n}^{\mathrm{sym}}(K) \cong \mathrm{Bil}_K^{\mathrm{sym}}(V) \cong \mathrm{QF}_K(V).$$
Wenn $q(x) = \sum_{1\leq i\leq j\leq n} a_{ij}x_ix_j$ eine quadratische Form auf K^n ist, dann ist die zugehörige symmetrische Matrix $C = (c_{ij})$ mit
$$c_{ij} = \begin{cases} a_{ij}/2 & i<j \\ a_{ii} & i=j \\ a_{ji}/2 & i>j, \end{cases}$$
da $\frac{1}{2}\beta_q(e_i,e_j) = c_{ij}$, so dass $\frac{1}{2}\beta_q(\mathcal{B},\mathcal{B}) = C$ für $\mathcal{B} = (e_1,\dots,e_n)$.

Definition. Sei b eine symmetrische Bilinearform auf einem K-Vektorraum V. Eine *Orthogonalbasis* von V bzgl. b ist eine Basis $\mathcal{A}$ von V mit $b(v_i,v_j) = 0$ für alle $v_i \neq v_j \in \mathcal{A}$ (d.h. $v_i \perp v_j$).

Bemerkung. Sei V ein endlichdimensionaler K-Vektorraum und $\mathcal{A}$ eine geordnete Basis von V. Die Basis $\mathcal{A}$ ist genau dann orthogonal bzgl. einer Bilinearform b auf V, wenn die zugehörige Matrix $b(\mathcal{A},\mathcal{A})$ diagonal ist.

Beispiel. Für die kanonische Bilinearform auf K^n

$$b(x,y) := \sum_{i=1}^{n} x_i y_i$$

ist die Standardbasis eine Orthogonalbasis.

Satz 2.8. *Sei K ein Körper mit $\mathrm{Char}(K) \neq 2$ und b eine symmetrische Bilinearform auf einem endlichdimensionalen K-Vektorraum V. Dann gibt es eine Orthogonalbasis von V bzgl. b.*

Korollar. Wenn $\mathrm{Char}(K) \neq 2$, ist jede symmetrische Matrix $A \in \mathrm{Mat}^{\mathrm{Sym}}_{n\times n}(K)$ kongruent zu einer Diagonalmatrix, d.h. es gibt $S \in \mathrm{GL}_n(K)$ mit $SAS^t = D$, eine Diagonalmatrix.

Korollar. Wenn $K = \mathbb{C}$ und b eine symmetrische Bilinearform auf einem $\mathbb{C}$-Vektorraum V der Dimension $n \in \mathbb{N}$ ist, dann gibt es $0 \leq r \leq n$ und eine geordnete Basis $\mathcal{A}$ von V so dass die Matrix $B = b(\mathcal{A}, \mathcal{A})$ zu b die folgende Form hat

$$B = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}.$$

Korollar.(Trägheitssatz von Sylvester - Version I). Sei $K = \mathbb{R}$ und b eine symmetrische Bilinearform auf einem $\mathbb{R}$-Vektorraum V der Dimension n. Dann gibt es $r, s \in \mathbb{N}$ mit $r + s \leq n$ und eine geordnete Basis $\mathcal{A}$ von V so, dass die zu b gehörige Matrix $B = b(\mathcal{A}, \mathcal{A})$ die folgende Form hat

$$B = \begin{pmatrix} I_r & 0 & 0 \\ 0 & -I_s & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Korollar. Sei K ein Körper mit $\mathrm{Char}(K) \neq 2$. Jedes homogene quadratische Polynom $q(x_1, \ldots, x_n) = \sum_{1\leq i\leq j\leq n} a_{ij} x_i x_j$ in n Variablen $x_1, \ldots, x_n$ lässt sich schreiben in der Form

$$q(x) = \sum_{1\leq i,j\leq n} d_i \cdot (b_{i1}x_1 + \cdots + b_{in}x_n)^2$$

mit b_{ij} und $d_i \in K$.

Bemerkung. Aus diesem Korollar folgt:

(1) Für jede quadratische Form q auf einem $\mathbb{C}$-Vektorraum der Dimension n gibt es $0 \leq r \leq n$ und eine geeignete Basis $\mathcal{A}$ von V, so dass das zugehörige homogene quadratische Polynom $f_q^{\mathcal{A}}$ (siehe Satz 2.6) die folgende Form hat

$$f_q^{\mathcal{A}}(t_1, \ldots, t_n) = t_1^2 + \cdots + t_r^2.$$

(2) Für jede quadratische Form q auf einem $\mathbb{R}$-Vektorraum der Dimension n gibt es $r, s \in \mathbb{N}$ mit $r + s \leq n$ und eine geeignete Basis $\mathcal{A}$ von V, so dass das zugehörige homogene quadratische Polynom $f_q^{\mathcal{A}}$ die folgende Form hat

$$f_q^{\mathcal{A}}(t_1, \ldots, t_n) = t_1^2 + \cdots + t_r^2 - t_{r+1}^2 - \cdots - t_{r+s}^2.$$

3. Euklidische und unitäre Vektorräume

[04.06.18]

3.1. **Euklidische Vektorräume.** In diesem Abschnitt sei $K = \mathbb{R}$. Der Körper $\mathbb{R}$ ist angeordnet, d.h. es gibt eine Ordnung $\leq$ auf $\mathbb{R}$. Ferner gibt es einen Betrag auf $\mathbb{R}$, der eine Abbildung $|-| : \mathbb{R} \to \mathbb{R}_{\geq 0} := \{x \in \mathbb{R} : x \geq 0\}$ ist.

Definition. Sei V ein $\mathbb{R}$-Vektorraum.

(1) Eine symmetrische Bilinearform $b : V \times V \to \mathbb{R}$ heißt *positiv semi-definit* (bzw. *positiv definit*), falls $b(v,v) \geq 0$ (bzw. $b(v,v) > 0$) für alle $v \in V \backslash \{0_V\}$.

(2) Eine symmetrische Bilinearform b auf V heißt *negativ (semi-)definit*, wenn $-b$ positiv (semi-)definit ist.
(3) Eine symmetrische Matrix $A \in \mathrm{Mat}^{\mathrm{Sym}}_{n\times n}(\mathbb{R})$ heißt *positiv semi-definit*, wenn $x^t A x \geq 0$ für alle $x \in \mathbb{R}^n \backslash \{0\}$ ist. Ebenso kann man die Definitionen für positiv semi-definit, negativ definit, und negativ semi-definit formulieren.
(4) Ein *Skalarprodukt* auf V ist eine positiv definite symmetrische Bilinearform $\langle -,- \rangle : V \times V \to \mathbb{R}$ auf V.
(5) Ein *euklidischer Vektorraum* $(V, \langle -,- \rangle)$ ist ein endlichdimensionaler $\mathbb{R}$-Vektorraum V mit einem Skalarprodukt $\langle -,- \rangle : V \times V \to \mathbb{R}$.

Bemerkung.
(1) Wenn V ein endlichdimensionaler $\mathbb{R}$-Vektorraum ist und $\mathcal{A}$ eine geordnete Basis von V ist, dann gilt für eine symmetrische Bilinearform b auf V:
$$b \text{ ist positiv definit} \iff b(\mathcal{A},\mathcal{A}) \text{ ist positiv definit.}$$
(2) Nach dem Trägheitssatz von Sylvester (Version I) gibt es zu jeder symmetrische Bilinearform b auf einem $\mathbb{R}$-Vektorraum V der Dimension n natürliche Zahlen r, s mit $r+s \leq n$ und eine geordnete Basis $\mathcal{A}$ von V so, dass
$$B = b(\mathcal{A},\mathcal{A}) = \begin{pmatrix} I_r & 0 & 0 \\ 0 & -I_s & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$
Die Bilinearform b ist genau dann positiv semi-definit, wenn $s = 0$. Die symmetrische Bilinearform b ist ein Skalarprodukt (d.h. positiv definit), wenn $s = 0$ und $r = n$. Insbesondere ist ein Skalarprodukt $\langle -,- \rangle$ auf V nicht ausgeartet nach dem Satz 2.4. Die Bilinearform ist negativ definit, wenn $r = 0$ und $s = n$.

Beispiel. Das Standardskalarprodukt auf $\mathbb{R}^n$ ist
$$\begin{array}{rccl} \langle -,- \rangle : & \mathbb{R}^n \times \mathbb{R}^n & \to & \mathbb{R} \\ & (x,y) & \mapsto & \langle x,y \rangle := \sum_{i=1}^n x_i y_i. \end{array}$$
Dann ist $\mathbb{E}^n := (\mathbb{R}^n, \langle -,- \rangle)$ der *standard euklidische Vektorraum* (der Dimension n).

Lemma. Eine symmetrische Matrix $A \in \mathrm{Mat}^{\mathrm{Sym}}_{n\times n}(\mathbb{R})$ ist genau dann positiv definit, wenn A kongruent zu der Einheitsmatrix I_n ist.

Satz 3.1 (Trägheitssatz von Sylvester)**.** *Sei $\langle -,- \rangle$ eine symmetrische Bilinearform auf einem endlichdimensionalen $\mathbb{R}$-Vektorraum V. Dann gibt es eine Zerlegung $V = V_+ \oplus V_- \oplus V_0$ mit den folgenden Eigenschaften.*
(1) V_0, V_+ und V_- sind paarweise orthogonal bezüglich $< -,- >$,
(2) $b|_{V_0 \times V_0} \equiv 0$,
(3) $b|_{V_+ \times V_+}$ ist positiv definit,
(4) $b|_{V_- \times V_-}$ ist negativ definit.
Ferner sind V_0, $\dim_{\mathbb{R}}(V_+)$ und $\dim_{\mathbb{R}}(V_-)$ eindeutig bestimmt.

Definition.
(1) Die *Signatur* einer symmetrische Bilinearform b auf einem endlichdimensionalen $\mathbb{R}$-Vektorraum V ist
$$\mathrm{sign}(b) := \dim(V_+) - \dim(V_-),$$
wobei $V = V_+ \oplus V_- \oplus V_0$ eine Zerlegung wie in dem Trägheitssatz von Sylvester ist.
(2) Die *Signatur* einer symmetrische Matrix $A \in \mathrm{Mat}_{n\times n}(\mathbb{R})$ ist die Signatur der zugehörigen symmetrische Bilinearform b_A.

Bemerkung. Für zwei symmetrische Matrizen $A, B \in \mathrm{Mat}_{n\times n}(\mathbb{R})$ gilt

$$A \text{ und } B \text{ sind kongruent} \iff \mathrm{Rang}(A) = \mathrm{Rang}(B) \text{ und } \mathrm{sign}(A) = \mathrm{sign}(B).$$

Definition. Sei $(V, \langle -,- \rangle)$ ein euklidischer Vektorraum.

(1) $f \in \mathrm{End}_{\mathbb{R}}(V)$ heißt *orthogonal* (bzgl. $\langle -,- \rangle$), wenn für alle $v, w \in V$ gilt
$$\langle f(v), f(w) \rangle = \langle v, w \rangle.$$
Wir schreiben $\mathrm{O}(V) := \{f \in \mathrm{End}_K(V) : f \text{ ist orthogonal}\}$.

(2) Eine Matrix $A \in \mathrm{Mat}_{n\times n}(\mathbb{R})$ mit $A^t A = I_n$ heißt *orthogonal*[7]. Wir schreiben $\mathrm{O}(n)$ für die Menge aller orthogonalen $n \times n$-Matrizen.

Bemerkung.

(1) Jede Matrix $A \in \mathrm{O}(n)$ ist invertierbar mit $A^{-1} = A^t$, also gilt $\mathrm{O}(n) \subset \mathrm{GL}_n$. Tatsächlich ist diese Teilmenge eine Untergruppe: es gilt $I_n \in \mathrm{O}(n)$ und aus $A \in \mathrm{O}(n)$ folgt $A^{-1} \in \mathrm{O}(n)$. Wir nennen $\mathrm{O}(n)$ *die orthogonale Gruppe.*

(2) Für $A \in \mathrm{Mat}_{n\times n}(\mathbb{R})$ definieren wir eine lineare Abbildung $F_A : \mathbb{R}^n \to \mathbb{R}^n$ durch $F_A(x) = Ax$ für einen Spaltenvektor $x \in \mathbb{R}^n$. Dann gilt für das Standardskalarprodukt $\langle -,- \rangle$ auf $\mathbb{R}^n$
$$\langle F_A(x), F_A(y) \rangle = \langle Ax, Ay \rangle = (Ax)^t Ay = x^t A^t Ay.$$
Insbesondere ist A genau dann orthogonal, wenn F_A orthogonal bzgl. des Standardskalarprodukt $\langle -,- \rangle$ auf $\mathbb{R}^n$ ist.

Beispiel.

(1) Sei $\lambda \in \mathbb{R}$ und V ein euklidischer Vektorraum. Dann ist $f = \lambda \cdot \mathrm{Id}_V$ genau dann orthogonal, wenn $\lambda = \pm 1$.

(2) Eine Drehung $D_\theta : \mathbb{R}^2 \to \mathbb{R}^2$ um $\mathbf{0} \in \mathbb{R}^2$ mit Winkel θ ist orthogonal bzgl. des Standardskalarprodukt $\langle -,- \rangle$ auf $\mathbb{R}^n$, weil
$$A_\theta = M_{\mathcal{B}}^{\mathcal{B}}(D_\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$$
mit $\mathcal{B} = (e_1, e_2)$ orthogonal ist:
$$A_\theta^t A_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

(3) Eine Spieglung $S_x : \mathbb{R}^2 \to \mathbb{R}^2$ in der x-Achse ist orthogonal, weil
$$A = M_{\mathcal{B}}^{\mathcal{B}}(S_x) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
orthogonal ist. Tatsächlich ist die Spieglung durch jede Gerade L durch $0 \in \mathbb{R}^2$ orthogonal.

Bemerkung. Für einen euklidischen Vektorraum V und orthogonale Endomorphismen $f, g \in \mathrm{End}_{\mathbb{R}}(V)$ gilt

(1) $f \circ g$ ist orthogonal,
(2) $\ker(f) = \{0_V\}$. Wegen $\dim_{\mathbb{R}}(V) < \infty$, ist f bijektiv und ferner ist f^{-1} orthogonal.
(3) Die Menge $\mathrm{O}(V)$ ist eine Untergruppe von $\mathrm{Aut}_{\mathbb{R}}(V) \subset \mathrm{End}_{\mathbb{R}}(V)$.
(4) Für einen Eigenwert $\lambda \in \mathbb{R}$ von f gilt $\lambda = \pm 1$.

Beispiel.

(1) $\mathrm{O}(1) = \{\pm 1\}$.

[7]In diesem Fall ist A invertierbar mit $A^{-1} = A^t$

(2) Für $n = 2$: wenn eine Matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

orthogonal ist, gilt $a^2 + c^2 = b^2 + d^2 = 1$ und $ab + cd = 0$. Seien $\alpha := a + ic$ und $\beta := b + id \in \mathbb{C}$, dann gilt $|\alpha| = |\beta| = 1$ und $\mathrm{Re}(\alpha\overline{\beta}) = 0$. Es folgt, dass $|\alpha\overline{\beta}| = 1$ und, wegen $\mathrm{Re}(\alpha\overline{\beta}) = 0$, dass $\alpha\overline{\beta} = \pm i$, d.h. $\beta = \pm i\alpha$. Jede komplexe Zahl $\alpha \in \mathbb{C}$ mit $|\alpha| = 1$ hat die Form $\alpha = \cos\theta + i \sin\theta$ für $\theta \in [0, 2\pi)$. Deshalb gibt es zwei Fälle:

$$\text{Fall } 1 : \beta = i\alpha. \qquad A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

eine Drehung um $\mathbf{0} \in \mathbb{R}^2$ mit Winkel θ, oder

$$\text{Fall } 2 : \beta = -i\alpha. \qquad A = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$$

eine Spieglung an der Geraden durch den 0 und $\sqrt{\alpha}$.

(3) Für $A \in \mathrm{O}(n)$ ist $\det(A) = \pm 1$. Ferner ist der Homomorphismus $\det : \mathrm{O}(n) \to \mathrm{O}(1) = \{\pm 1\}$ surjektiv.

[06.06.18]

3.2. **Unitäre Vektorräume.** In diesem Abschnitt sei $K = \mathbb{C} := \{x + iy : (x, y) \in \mathbb{R}^2\}$, wobei i eine Wurzel von -1 ist. Der Betrag ist eine Abbildung $|-| : \mathbb{C} \to \mathbb{R}_{\geq 0}$ mit $|x + iy| = \sqrt{x^2 + y^2}$. Die Komplexe Konjugation ist ein Körperautomorphisms $\mathbb{C} \to \mathbb{C}$, der durch $z := x + iy \mapsto \bar{z} = x - iy$ definiert wird. Es gilt $\bar{z}z = |z|^2$.

Es gibt keine Ordnung auf $\mathbb{C}$, deshalb hat der Begriff 'positive Definitheit' keinen Sinn. Ferner haben wir für die kanonische symmetrische Bilinearform b auf $\mathbb{C}^n$

$$b(z, w) := \sum_{k=1}^{n} z_k w_k$$

für $z = w = (i, \ldots, i)^t$, dass $b(z, z) < 0$. Deshalb werden wir ein Skalarprodukt auf einem komplexen Vektorraum als eine 'positiv definite hermitesche' Form definieren.

Definition. Sei V ein $\mathbb{C}$-Vektorraum.

(1) Eine Abbildung $h : V \times V \to \mathbb{C}$ heißt *Sesquilinearform* auf V, wenn
   (a) h ist $\mathbb{C}$-linear im zweiten Argument, d.h. für $v_i \in V$ und $\lambda, \mu \in \mathbb{C}$ gilt

$$h(v_1, \mu v_2 + \lambda v_3) = \mu h(v_1, v_2) + \lambda h(v_1, v_3).$$

   (b) h ist $\mathbb{C}$-antilinear im ersten Argument , d.h. für $v_i \in V$ und $\lambda, \mu \in \mathbb{C}$ gilt

$$h(\mu v_1 + \lambda v_2, v_3) = \bar{\mu} h(v_1, v_3) + \bar{\lambda} h(v_2, v_3).$$

   Die Menge aller Sesquilinearformen auf V wird mit $\mathrm{SLF}(V)$ bezeichnet.

(2) Eine Sesquilinearform h auf V heißt *Hermitesch* (bzw. *schief-Hermitesch*), wenn $\forall v_i \in V$:

$$h(v_1, v_2) = \overline{h(v_2, v_1)} \quad (\text{bzw. } h(v_1, v_2) = -\overline{h(v_2, v_1)}).$$

(3) Wenn $\mathcal{A} = (v_1, \ldots, v_n)$ eine Basis von V ist und h eine Sesquilinearform auf V ist, dann heißt $h(\mathcal{A}, \mathcal{A}) := (h(v_i, v_j))_{ij} \in \mathrm{Mat}_{n \times n}(\mathbb{C})$ die Matrix von h bezüglich $\mathcal{A}$.

(4) Für $B = (b_{ij}) \in \mathrm{Mat}_{m \times n}(\mathbb{C})$, definieren wir $B^\dagger := \bar{B}^t = (\overline{b_{ji}}) \in \mathrm{Mat}_{n \times m}(\mathbb{C})$.[8]

(5) Eine Matrix $B \in \mathrm{Mat}_{n \times n}(\mathbb{C})$ heißt *Hermitesch* (bzw. *schief-Hermitesch*), wenn $B = B^\dagger$ (bzw. $B = -B^\dagger$).

[8]Es gilt $B^\dagger := \overline{(B^t)} = (\bar{B})^t$.

Beispiel. Die kanonische Hermitesche Form auf $\mathbb{C}^n$ ist $h : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$ mit

$$h(z, w) = \sum_{k=1}^{n} \overline{z_k} w_k$$

und die Matrix von h bzgl. zu der geordneten Standardbasis $(e_1, \ldots, e_n)$ ist die Einheitsmatrix I_n.

Bemerkung. Sei V ein $\mathbb{C}$-Vektorraum der Dimension n und $\mathcal{A} = (v_1, \ldots, v_n)$ eine geordnete Basis von V. Dann gibt es genau einen linearen Isomorphismus $\Phi_{\mathcal{A}} : V \to \mathbb{C}^n$ mit $\Phi_{\mathcal{A}}(v_k) = e_k$ für $1 \leq k \leq n$ [LAI, Satz 4.4].

(1) Wenn $h : V \times V \to \mathbb{C}$ eine Sesquilinearform ist und B die Matrix von h bzgl. der Basis $\mathcal{A}$ ist, dann gilt für alle $v, v' \in V$
$$h(v, v') = \Phi_{\mathcal{A}}(v)^\dagger\, B\, \Phi_{\mathcal{A}}(v').$$
Ferner ist h genau dann eine (schief-)Hermitesche Form, wenn B eine (schief-)Hermitesche Matrix ist.

(2) Umgekehrt definiert $B \in \mathrm{Mat}_{n\times n}(\mathbb{C})$ eine Sesquilinearform auf V durch
$$h_B^{\mathcal{A}}(v, v') := \Phi_{\mathcal{A}}(v)^\dagger\, B\, \Phi_{\mathcal{A}}(v')$$
und die zugehörige Matrix dieser Sesquilinearform h bzgl. der Basis $\mathcal{A}$ ist wieder B.

(3) Die Abbildung
$$\Psi_{\mathcal{A}} : \mathrm{SLF}(V) \to \mathrm{Mat}_{n\times n}(\mathbb{C}),$$
die zu jeder Sesquilinearform h die zugehörige Matrix $B = h(\mathcal{A}, \mathcal{A})$ von h bzgl. der Basis $\mathcal{A}$ zuordnet, ist ein linearer Isomorphismus.

(4) Es gibt eine Formel für einen Basiswechsel: seien $\mathcal{A}, \mathcal{B}$ geordneten Basen von V. Dann gilt für eine Sesquilinearform h auf V
$$h(\mathcal{B}, \mathcal{B}) = M_{\mathcal{A}}^{\mathcal{B}}(\mathrm{Id}_V)^\dagger h(\mathcal{A}, \mathcal{A}) M_{\mathcal{A}}^{\mathcal{B}}(\mathrm{Id}_V)$$
wobei $M_{\mathcal{A}}^{\mathcal{B}}(\mathrm{Id}_V)$ die Basiswechselmatrix für die Identität auf V ist.

Bemerkung. Sei V ein $\mathbb{C}$-Vektorraum.

(1) Wenn h eine Hermitesche Form auf V ist, gilt $h(v, v) \in \mathbb{R}$ für alle $v \in V$, weil $h(v, v) = \overline{h(v, v)}$.
(2) Wenn h eine schief-Hermitesche Form auf V ist, gilt $h(v, v) \in i\mathbb{R}$ für alle $v \in V$.

Definition. Sei V ein $\mathbb{C}$-Vektorraum.

(1) Eine Hermitesche Form h auf einem $\mathbb{C}$-Vektorraum V heißt *positiv definit*, wenn für alle $v \in V$ mit $v \neq 0_V$ gilt $h(v, v) > 0$. Die Definitionen für *positiv semi-definit*, *negativ definit* und *negativ semi-definit* sind analog.
(2) Ein *Skalarprodukt* auf V ist eine positiv definite Hermitesche Form auf V.
(3) Ein *unitärer Vektorraum* (V, h) ist ein endlichdimensionaler $\mathbb{C}$-Vektorraum V mit einer Skalarprodukt h auf V.

Beispiel. Die kanonische Hermitesche Form auf $\mathbb{C}^n$

$$\langle z, w \rangle := \sum_{k=1}^{n} \overline{z_k} w_k$$

ist positiv definit, weil $\langle z, z \rangle := \sum_{k=1}^{n} \overline{z}_k z_k = \sum_{k=1}^{n} |z_k|^2$. Wir nennen $\langle -, - \rangle$ das Standardskalarprodukt auf $\mathbb{C}^n$. Dann heißt $(\mathbb{C}^n, \langle -, - \rangle)$ der standard unitäre Vektorraum

Definition. Sei $(V, \langle -, - \rangle)$ ein unitärer Vektorraum.

(1) $f \in \mathrm{End}_{\mathbb{C}}(V)$ heißt *unitär* (bzgl. $\langle -, - \rangle$), wenn für alle $v, w \in V$ gilt
$$\langle f(v), f(w) \rangle = \langle v, w \rangle.$$
Wir schreiben $\mathrm{U}(V) := \{f \in \mathrm{End}_{\mathbb{C}}(V) : f \text{ ist unitär}\}$.

(2) Eine Matrix $A \in \mathrm{Mat}_{n \times n}(\mathbb{C})$ mit $A^\dagger A = I_n$ heißt *unitär*[9]. Wir schreiben $\mathrm{U}(n)$ für die Menge aller unitären $n \times n$-Matrizen.

Bemerkung. Für $A \in \mathrm{Mat}_{n \times n}(\mathbb{C}^n)$ definieren wir eine lineare Abbildung $F_A : \mathbb{C}^n \to \mathbb{C}^n$ durch $F_A(x) = Ax$ für einen Spaltenvektor $x \in \mathbb{C}^n$. Dann gilt für das Standardskalarprodukt $\langle -, - \rangle$ auf $\mathbb{C}^n$
$$\langle F_A(x), F_A(y) \rangle = \langle Ax, Ay \rangle = (Ax)^\dagger Ay = x^\dagger A^\dagger Ay.$$
Insbesondere ist A genau dann unitär, wenn F_A unitär bzgl. zu dem Standardskalarprodukt $\langle -, - \rangle$ auf $\mathbb{C}^n$ ist.

Beispiel. Sei $\lambda \in \mathbb{C}$ und V ein unitärer Vektorraum. Dann ist $f = \lambda \cdot \mathrm{Id}_V$ genau dann unitär, wenn $|\lambda| = 1$.

Bemerkung. Für einen unitären Vektorraum V und unitäre Endomorphismen $f, g \in \mathrm{U}(V)$ gilt

(1) $f \circ g$ ist unitär.
(2) $\ker(f) = \{0_V\}$ und wegen $\dim_{\mathbb{C}}(V) < \infty$, ist f bijektiv und ferner ist f^{-1} unitär.
(3) Die Menge $\mathrm{U}(V)$ ist eine Untergruppe von $\mathrm{Aut}_{\mathbb{C}}(V) \subset \mathrm{End}_{\mathbb{C}}(V)$.
(4) Für einen Eigenwert $\lambda \in \mathbb{C}$ von f gilt $|\lambda| = 1$.

Definition. Die Menge aller unitäre $n \times n$-Matrizen $\mathrm{U}(n) < \mathrm{GL}_n(\mathbb{C})$ heißt die unitäre Gruppe.

Beispiel.

(1) $\mathrm{U}(1) = \{z \in \mathbb{C} : |z| = 1\}$.
(2) Für $A \in \mathrm{U}(n)$ ist $|\det(A)| = 1$. Ferner ist der Homomorphismus $\det : \mathrm{U}(n) \to \mathrm{U}(1)$ surjektiv.

[11.06.18]

3.3. **Normen und Orthogonalität.** In dieser Sektion sei $K = \mathbb{R}$ oder $K = \mathbb{C}$. Dann gibt es einen Betrag $| - | : K \to \mathbb{R}_{\geq 0}$.

Definition. Sei V ein K-Vektorraum. Eine Abbildung $|| - || : V \to \mathbb{R}_{\geq 0}$ heißt *Norm*, wenn die folgenden Eigenschaften (N1-N3) gelten:

(N1). Für $v \in V$ gilt $||v|| = 0 \implies v = 0_V$,
(N2). Für $v \in V$ und $\lambda \in K$ gilt $||\lambda \cdot v|| = |\lambda| \, ||v||$,
(N3.) Für $v, v' \in V$ gilt die Dreiecksungleichung: $||v + v'|| \leq ||v|| + ||v'||$.

Bemerkung. Für eine Norm $|| - || : V \to \mathbb{R}$ gilt:

(1) $||0_V|| = 0$ nach dem Axiom (N2).
(2) $|| - v|| = ||v||$ nach dem Axiom (N2).

Satz 3.2. *Sei V ein K-Vektorraum und $\langle -, - \rangle : V \times V \to \mathbb{R}$ ein Skalarprodukt (mit $K = \mathbb{R}$ oder $\mathbb{C}$). Dann ist $||v|| := \sqrt{\langle v, v \rangle}$ eine Norm auf V. Ferner gelten für $v, w \in V$ und $\lambda \in K$*

(a) $||v + w||^2 = ||v||^2 + ||w||^2 + 2Re < v, w >$.
(b) (Parallelogrammidentität)
$$||v + w||^2 + ||v - w||^2 = 2||v||^2 + 2||w||^2.$$
(c) (Schwarz'sche Ungleichung)
$$|\langle v, w \rangle| \leq ||v|| \, ||w||$$
mit Gleichheit genau dann, wenn v und w linear abhängig sind.

[9]In diesem Fall ist A invertierbar mit $A^{-1} = A^\dagger$

(d) $|\,||v|| - ||w||\,| \leq ||v-w||$.

Beispiel. Das Standardskalarprodukt auf $\mathbb{R}^n$

$$\begin{array}{rccl} \langle -,- \rangle : & \mathbb{R} \times \mathbb{R}^n & \to & \mathbb{R} \\ & (x,y) & \mapsto & \langle x,y \rangle := \sum_{i=1}^n x_i y_i \end{array}$$

liefert die euklidische Standardnorm $||-|| : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$

$$||x|| = \sqrt{\sum_{i=1}^n x_i^2}.$$

Ebenso liefert das Standardskalarprodukt auf $\mathbb{C}^n$

$$\begin{array}{rccl} \langle -,- \rangle : & \mathbb{C} \times \mathbb{C}^n & \to & \mathbb{C} \\ & (z,w) & \mapsto & \langle z,w \rangle := \sum_{k=1}^n \bar{z}_k w_k \end{array}$$

die unitäre Standardnorm $||-|| : \mathbb{C}^n \to \mathbb{R}_{\geq 0}$

$$||z|| = \sqrt{\sum_{k=1}^n \bar{z}_k z_k} = \sqrt{\sum_{k=1}^n |z_k|^2}.$$

Definition. Sei V ein K-Vektorraum. Eine Abbildung $d : V \times V \to \mathbb{R}_{\geq 0}$ heißt *Metrik* (oder Abstand), wenn die folgenden Eigenschaften (M1-M3) gelten:
(M1). Für $v, w \in V$ gilt $d(v,w) = 0 \iff v = w$.
(M2). Symmetrie: Für $v, w \in V$ gilt $d(v,w) = d(w,v)$.
(M3.) Dreiecksungleichung: Für $u, v, w \in V$ gilt $d(u,v) \leq d(u,w) + d(w,v)$.

Lemma. Sei $||-||$ eine Norm auf einem K-Vektorraum V. Dann ist $d(v,w) := ||v-w||$ eine Metrik auf V.

Definition. Sei $\langle -,- \rangle : V \times V \to K$ ein Skalarprodukt auf einem K-Vektorraum V.
(1) Zwei Vektoren $v, w \in V$ heißt *orthogonal*, falls $\langle v,w \rangle = 0$. In diesem fall schreiben wir $v \perp w$.
(2) Zwei Teilmengen A und B heißt *orthogonal* (schreibweise $A \perp B$), falls $a \perp b$ für alle $a \in A$ und $b \in B$.
(3) Eine direkte Summe $\oplus_{j=1}^n U_i$ von Untervektorräume U_j von V ist *orthogonal*, falls $U_j \perp U_k$ für alle $j \neq k$.
(4) Eine Familie $(v_j)_{j \in J}$ von Vektoren heißt *orthogonal*, falls für alle $j \neq k$ gilt $v_j \perp v_k$.
(5) Eine Familie $(v_j)_{j \in J}$ von Vektoren heißt *normiert*, falls für alle $j \in J$ gilt $||v_j|| = 1$.
(6) Eine Familie $(v_j)_{j \in J}$ von Vektoren heißt *orthonormal*, falls $\langle v_j, v_k \rangle = \delta_{jk}$ für alle $j, k \in J$.
(7) Eine *Orthonormal-Basis* (ON-Basis) von V ist eine Basis von V, deren Vektoren orthonormal zueinander sind.

Bemerkung. Für ein Skalarprodukt $\langle -,- \rangle : V \times V \to K$ auf einem K-Vektorraum V gelten die folgenden Aussagen.
(1) $v \perp w \iff w \perp v$ für $v, w \in V$, weil $\langle v,w \rangle = \overline{\langle w,v \rangle}$.
(2) Eine Familie ist genau dann orthonormal, wenn sie orthogonal und normiert ist.
(3) Für $v \neq 0_V$ ist $v/||v||$ normiert.
(4) Jede orthogonale Familie $(v_j)_{j \in I}$ mit $v_j \neq 0_V$ für alle $j \in J$ ist linear unabhängig: aus einer Gleichung $0_V = \sum_{k=1}^n \lambda_k v_{j_k}$ mit $\lambda_k \in K$ folgt für $1 \leq l \leq n$

$$0 = \langle v_{i_l}, 0_V \rangle = \langle v_{i_l}, \sum_{k=1}^n \lambda_k v_{j_k} \rangle = \sum_{k=1}^n \lambda_k \langle v_{i_l}, v_{j_k} \rangle = \lambda_l ||v_{j_l}||^2$$

und wegen $v_{j_l} \neq 0_V$, folgt $\lambda_l = 0$.

(5) Wenn $(v_j)_{j\in J}$ eine orthogonale Familie mit $v_j \neq 0_V$ für alle $j \in J$ ist, dann ist die Familie $(w_j)_{j\in J}$ mit $w_j := v_j/||v_j||$ orthonormal.

Beispiel. Die Standardbasis $e_1, \dots, e_n$ von K^n ist eine ON-Basis (bzgl zum Standardskalarprodukt).

Satz 3.3. *Sei $\langle -, - \rangle : V \times V \to K$ ein Skalarprodukt auf einem K-Vektorraum V (mit $K = \mathbb{R}$ oder $\mathbb{C}$) und sei $v_1, \dots, v_n$ eine ON-Basis von V.*

(1) Für alle $v \in V$ gilt

$$v = \sum_{k=1}^{n} \langle v_k, v \rangle \cdot v_k.$$

(2) Parseval-Gleichung: für alle $v, w \in V$ gilt

$$\langle v, w \rangle = \sum_{k=1}^{n} \overline{\langle v_k, v \rangle} \langle v_k, w \rangle.$$

(3) Bessel-Gleichung: für alle $v \in V$ gilt

$$||v||^2 = \sum_{k=1}^{n} |\langle v_k, v \rangle|^2.$$

[13.06.18]

Satz 3.4. *Sei $f : V \to W$ eine lineare Abbildung zwischen endlichdimensionalen K-Vektorräumen mit Skalarprodukten $\langle -, - \rangle_V : V \times V \to K$ und $\langle -, - \rangle_W : W \times W \to K$. Wenn $\mathcal{A} = (v_1, \dots, v_n)$ und $\mathcal{B} = (w_1, \dots, w_n)$ geordnete ON-Basen von V und W sind und $A = M^{\mathcal{A}}_{\mathcal{B}}(f)$, dann gilt*

$$a_{ij} = \langle w_i, f(v_j) \rangle.$$

3.4. **Gram-Schmidtsche-Orthogonalisierungsverfahren (GSOV).** Durch diese Verfahren werden wir zeigen, wie man aus einer gegebenen linear unabhängigen Familie $v_1, \dots, v_n$ von Vektoren aus einem K-Vektorraum mit Skalarprodukt $(V, \langle -, - \rangle)$ eine ON-Familie $w_1, \dots, w_n$ erhält mit $\mathrm{Span}(v_1, \dots, v_n) = \mathrm{Span}(w_1, \dots, w_n)$. Das Verfahren an den Beweis von Satz 2.8 anlehnt.

Satz 3.5 (Gram-Schmidt OV)**.** *Sei $(V, \langle -, - \rangle)$ ein K-Vektorraum mit Skalarprodukt. Wenn $v_1, \dots, v_n$ eine lineare unabhängige Familie von Vektoren aus V ist, gibt es eine ON-Familie $w_1, \dots, w_n$ von Vektoren mit*

$$\mathrm{Span}(v_1, \dots, v_r) = \mathrm{Span}(w_1, \dots, w_r) \quad \textit{für } 1 \leq r \leq n$$

Korollar. Jeder endlichdimensionale K-Vektorraum V mit Skalarprodukt hat eine ON-Basis.

Bemerkung. Sei $(V, \langle -, - \rangle)$ ein K-Vektorraum mit Skalarprodukt. Wenn $(v_j)_{j\in\mathbb{N}}$ eine lineare unabhängige Familie von Vektoren aus V ist, nach dem GSOV und Induktion gibt es eine ON-Familie $(w_j)_{j\in\mathbb{N}}$ von Vektoren, so dass für alle $n \in \mathbb{N}$ gilt

$$\mathrm{Span}(v_0, \dots, v_n) = \mathrm{Span}(w_0, \dots, w_n).$$

Korollar. Sei V ein unitärer Vektorraum und $f \in \mathrm{End}_{\mathbb{C}}(V)$. Dann gibt es eine ON Basis $\mathcal{A}$ von V so dass $M^{\mathcal{A}}_{\mathcal{A}}(f)$ eine obere Dreiecksmatrix ist.

Korollar.(Satz von Schur) Sei $A \in \mathrm{Mat}_{n\times n}(\mathbb{C})$. Dann gibt es $U \in \mathrm{U}(n)$ so dass $U^\dagger A U$ eine obere Dreiecksmatrix ist.

Übung: QR-Zerlegung. Sei $A \in \mathrm{GL}_n(\mathbb{R})$ mit Spaltenvektoren $\{a_1, \dots, a_n\}$. Sei $\{q_1, \dots, q_n\}$ die durch das Gram-Schmidt Verfahren aus $\{a_1, \dots, a_n\}$ konstruierte Orthonormalbasis. Warum ist $Q = (q_1|\cdots|q_n)$ orthogonal? Zeigen Sie dass $R := Q^t A$ eine obere Dreiecksmatrix ist. Dann gilt $A = QR$, wobei Q eine orthogonale Matrix ist und R eine obere Dreiecksmatrix ist. Wie kann man die QR-Zerlegung benutzt, lineare Gelichungssysteme zu lösen? (Hinweis: Für $b \in \mathbb{R}^n$, finden Sie $b' \in \mathbb{R}^n$ mit $\mathcal{L}(A, b) = \mathcal{L}(R, b')$).

3.5. **Spektralsätze.**

Satz 3.6 (Spektralsatz für Hermitesche Matrizen)**.** *Sei $A \in \mathrm{Mat}_{n\times n}(\mathbb{C})$ eine Hermitesche Matrix. Dann gilt*

(1) Alle Eigenwerte von A sind reelle.
(2) $\mathbb{C}^n$ hat eine ON-Basis von Eigenvektoren von A.
(3) Es gibt eine unitäre Matrix U so dass $U^\dagger AU$ ist diagonal mit reellen Einträge.

Korollar. (Spektralsatz für symmetrische Matrizen) Sei $A \in \mathrm{Mat}_{n\times n}(\mathbb{R})$ eine symmetrische Matrix. Dann gilt

(1) A hat n reelle Eigenwerte (wenn man mit Vielfach rechnen).
(2) $\mathbb{R}^n$ hat eine ON-Basis von Eigenvektoren von A.
(3) Es gibt eine orthogonale Matrix P so dass P^tAP ist diagonal.

[18.06.18]

Satz 3.7 (Spektralsatz für unitäre Matrizen)**.** *Sei $A \in \mathrm{Mat}_{n\times n}(\mathbb{C})$ eine unitäre Matrix. Dann gilt*

(1) Alle Eigenwerte von A haben Betrag 1.
(2) $\mathbb{C}^n$ hat eine ON-Basis von Eigenvektoren von A.
(3) Es gibt eine unitäre Matrix U so dass $U^\dagger AU$ ist diagonal mit Einträge vom Betrag 1.

3.6. **Orthogonale Projektion.**

Satz 3.8. *Sei $(V, \langle -,-\rangle)$ ein K-Vektorraum mit Skalarprodukt, $v \in V$ und $U \subset V$ ein Untervektorraum (mit $K = \mathbb{R}$ oder $K = \mathbb{C}$). Für $u \in U$ ist äquivalent:*

(1) $v - u \in U^\perp$
(2) $d(v, U) := \min\{d(v, u') : u' \in U\} = d(v, u)$.

Ferner gibt es ein $u \in U$ mit (1) *und* (2) *genau dann, wenn $v \in U + U^\perp$. In diesem Fall ist u eindeutig.*

Definition. Sei $(V, \langle -,-\rangle)$ ein K-Vektorraum mit Skalarprodukt, $v \in V$ und $U \subset V$ ein Untervektorraum. Die lineare Abbilung $\pi_U : U \oplus U^\perp \to U$ mit $\pi_U(u + u') := u$ heißt die *orthogonale Projektion.*

Korollar. Sei $(V, \langle -,-\rangle)$ ein K-Vektorraum mit Skalarprodukt und $U \subset V$ ein Untervektorraum. Die orthogonale Projektion $\pi_U : U \oplus U^\perp \to U$ erfüllt für alle $v \in U \oplus U^\perp$

(1) $\pi_U(v)$ ist gleich dem Element $u \in U$ mit minimalem Abstand zu v, d.h.
$$d(v, u) \leq d(v, u') \quad \text{für alle } u' \in U.$$
(2) $||\pi_U(v)|| \leq ||v||$ mit Gleichheit genau dann, wenn $v \in U$ (d.h. $\pi_U(v) = v$).

Bemerkung. Sei $(V, \langle -,-\rangle)$ ein endlichdimensionaler K-Vektorraum mit Skalarprodukt und $U \subset V$ ein Untervektorraum.

(1) Es gilt $V = U + U^\perp = U \oplus U^\perp$. Daher ist die orthogonale Projektion auf U eine Abbildung $\pi_U : V \to U$.
(2) Es gilt $U = (U^\perp)^\perp$.
(3) Wenn $u_1, \ldots, u_n$ eine ON-Basis von U ist, gilt $\pi_U(v) = \sum_{j=1}^n \langle u_j, v\rangle \cdot u_j$ für alle $v \in V$.

[20.06.18]

3.7. **Adjungierte Abbildungen.** In diesem Abschnitt sei $K = \mathbb{R}$ oder $\mathbb{C}$ und wir betrachen endlichdimensionale K-Vektorräume mit Skalarprodukten.

Lemma (von Riesz). Sei V ein endlichdimensionaler K-Vektorraum mit Skalarprodukt $\langle -,-\rangle$. Für $f \in V^* := \mathrm{Hom}_K(V, K)$ gibt es einen eindeutig bestimmten Vektor $v \in V$ mit $f(-) = \langle -, v\rangle$ als Elemente von V^*.

Satz 3.9. *Seien* $(V, \langle -,- \rangle_V)$ *und* $(W, \langle -,- \rangle_W)$ *endlichdimensionale* K*-Vektorräume mit Skalarprodukten. Für* $f \in \mathrm{Hom}_K(V,W)$ *gibt es eine eindeutige lineare Abbildung* $f^{\mathrm{ad}} \in \mathrm{Hom}_K(W,V)$ *mit*

$$\langle f(v), w \rangle_W = \langle v, f^{\mathrm{ad}}(w) \rangle_V \quad \textit{für alle } v \in V, w \in W.$$

Wir nennen f^{ad} *die zu* f *adjungierte Abbildung. Wenn* $\mathcal{A} = (v_1, \dots, v_n)$ *eine ON-Basis von* V *ist, dann gilt für alle* $w \in W$

$$f^{\mathrm{ad}}(w) = \sum_{j=1}^{n} \langle f(v_j), w \rangle_W \cdot v_j. \tag{3}$$

Wenn zusätzlich $\mathcal{B} = (w_1, \dots, w_m)$ *eine ON-Basis von* W *ist, dann gilt*

$$M^{\mathcal{B}}_{\mathcal{A}}(f^{\mathrm{ad}}) = M^{\mathcal{A}}_{\mathcal{B}}(f)^{\dagger}.$$

Korollar. Für $f : V \to W$ eine lineare Abbildung zwischen endlichdimensionalen K-Vektorräumen und die adjungierte Abbildung $f^{\mathrm{ad}} : W \to V$ gilt auch

$$\langle w, f(v) \rangle_W = \langle f^{\mathrm{ad}}(w), v \rangle_V \quad \text{für alle } v \in V, w \in W$$

Korollar. Sei V ein endlichdimensionaler K-Vektorraum mit Skalarprodukt $\langle -,- \rangle$. Für $f \in \mathrm{End}_K(V)$ ist äquivalent

(1) f ist orthogonal falls $K = \mathbb{R}$ (bzw. f ist unitär falls $K = \mathbb{C}$),
(2) f ist invertierbar mit $f^{-1} = f^{\mathrm{ad}}$.

Bemerkung. Seien $(U, \langle -,- \rangle_U)$, $(V, \langle -,- \rangle_V)$ und $(W, \langle -,- \rangle_W)$ drei endlichdimensionale K-Vektorräume mit Skalarprodukten. Für $f, f_i \in \mathrm{Hom}_K(U,V)$ und $g \in \mathrm{Hom}_K(V,W)$ und $\lambda_i \in K$ gelten:

(1) $(\lambda_1 \cdot f_1 + \lambda_2 \cdot f_2)^{\mathrm{ad}} = \overline{\lambda_1} f_1^{\mathrm{ad}} + \overline{\lambda_2} f_2^{\mathrm{ad}}$,
(2) $(g \circ f)^{\mathrm{ad}} = f^{\mathrm{ad}} \circ g^{\mathrm{ad}}$,
(3) $(\mathrm{Id}_V)^{\mathrm{ad}} = \mathrm{Id}_V$,
(4) $(f^{\mathrm{ad}})^{\mathrm{ad}} = f$.

Satz 3.10. *Seien* $(V, \langle -,- \rangle_V)$ *und* $(W, \langle -,- \rangle_W)$ *endlichdimensionale* K*-Vektorräume mit Skalarprodukten. Für* $f \in \mathrm{Hom}_K(V,W)$ *gilt*

(1) $\ker(f) = \mathrm{Bild}(f^{\mathrm{ad}})^{\perp}$
(2) $\ker(f^{\mathrm{ad}}) = \mathrm{Bild}(f)^{\perp}$

Korollar. Seien $(V, \langle -,- \rangle_V)$ und $(W, \langle -,- \rangle_W)$ endlichdimensionale K-Vektorräume mit Skalarprodukten. Für $f \in \mathrm{Hom}_K(V,W)$ gilt

(1) f ist genau dann injektiv, wenn f^{ad} surjektiv ist.
(2) f ist genau dann surjektiv, wenn f^{ad} injektiv ist.
(3) f ist genau dann bijektiv, wenn f^{ad} bijektiv ist.

Definition. Sei V ein endlichdimensionaler K-Vektorraum mit Skalarprodukt und $f \in \mathrm{End}_K(V)$.

(1) f heißt selbstadjungiert, falls $f = f^{\mathrm{ad}}$.
(2) f heißt antiselbstadjungiert, falls $f = -f^{\mathrm{ad}}$.
(3) f heißt normal, falls $f \circ f^{\mathrm{ad}} = f^{\mathrm{ad}} \circ f$.

Bemerkung. Wenn $\mathcal{A}$ eine ON-Basis von V ist und $A = M^{\mathcal{A}}_{\mathcal{A}}(f)$ gilt

(1) f ist selbstadjungiert $\iff A^{\dagger} = A$
(2) f ist antiselbstadjungiert $\iff A^{\dagger} = -A$.
(3) f ist normal $\iff AA^{\dagger} = A^{\dagger}A$.

Beispiel. Für einen Untervektorraum U eines endlichdimensionalen K-Vektorraumes V (mit Skalarprodukt) ist die orthogonale Projektion $\pi_U : V \to U$ selbstadjungiert: Sei $(v_1, \ldots, v_r)$ eine ON-Basis von U, dann können wir diese ON-Basis auf einer ON-Basis $\mathcal{A} = (v_1, \ldots, v_n)$ von V erweitern, so dass

$$M^{\mathcal{A}}_{\mathcal{A}}(\pi_U) = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}.$$

Satz 3.11. *Sei V ein endlichdimensionaler K-Vektorraum mit Skalarprodukt $\langle -, - \rangle$ und $f \in \mathrm{End}_K(V)$ normal. Dann gilt für jede $\lambda \in K$*

$$\mathrm{Eig}(f, \lambda) = \mathrm{Eig}(f^{\mathrm{ad}}, \overline{\lambda}))$$

und Eigenvektoren zu verschiedenen Eigenwerten sind orthogonal aufeinander. Insbesondere gilt

$$\ker(f) = \mathrm{Eig}(f, 0) = \ker(f^{\mathrm{ad}}) = \mathrm{Bild}(f^{\mathrm{ad}})^{\perp} = \mathrm{Bild}(f)^{\perp}.$$

[25.06.18]

Satz 3.12 (Spektralsatz für normale Abbildungen)**.** *Sei V ein endlichdimensionaler K-Vektorraum mit Skalarprodukt $\langle -, - \rangle$ und $f \in \mathrm{End}_K(V)$. Dann ist äquivalent*

(1) f ist normal und das charakteristische Polynom $\chi_f(t)$ zerfällt vollständig in Linearfaktoren,
(2) V ist die orthogonale Summe der Eigenräume von f,
(3) Es existiert eine ON-Basis von V aus Eigenvektoren von f.

Korollar. Eine Matrix $A \in \mathrm{Mat}_{n\times n}(\mathbb{C})$ ist genau dann normal (d.h. $A^\dagger A = AA^\dagger$), wenn es gibt eine unitäre Matrix $U \in \mathrm{U}(n)$ mit $U^\dagger AU$ diagonal.

3.8. **Anwendung in der Geometrie: Affine reelle Quadriken.** Sei K ein Körper mit $\mathrm{Char}(K) \neq 2$. Bald werden wir annehmen, dass $K = \mathbb{R}$.

Definition. Ein *quadratisches Polynom* in n Unbestimmten $x = (x_1, \cdots, x_n)$ über K ist ein Ausdruck der Form

$$Q(x_1, \ldots, x_n) = \sum_{j\leq k} a_{jk} x_j x_k + \sum_{j=1}^{n} b_j x_j + c$$

mit a_{jk}, b_j und $c \in K$. Die affine Quadrik $Z(Q) \subset K^n$, die durch Q definiert wird, ist die Menge

$$Z(Q) = \{x \in K^n : Q(x) = 0\} \subset K^n.$$

Im Fall $n = 2$ nennt man eine affine Quadrik $Z(Q) \subset K^2$ auch einen *Kegelschnitt.*

Beispiel. Sei $K = \mathbb{R}$ und $n = 2$. Dann sind die folgende Beispiele Kugelschnitte (d.h. die entsprechende affine Quadriken kann als Durchschnitt eines Kugels in $\mathbb{R}^3$ mit einer (affinen) Ebene $E \cong \mathbb{R}^2$ beschreiben werden):

(1) $Q(x, y) = x^2 + y^2 - 1$ mit $Z(Q) \subset \mathbb{R}^2$ ein Kreis.
(2) $Q(x, y) = x^2 + 2y^2 - 1$ mit $Z(Q) \subset \mathbb{R}^2$ eine Ellipse.
(3) $Q(x, y) = x^2 - y$ mit $Z(Q) \subset \mathbb{R}^2$ eine Parabel.
(4) $Q(x, y) = xy - 1$ mit $Z(Q) \subset \mathbb{R}^2$ eine Hyperbel.
(5) $Q(x, y) = x^2 + y^2 + 1$ mit $Z(Q) = \emptyset \subset \mathbb{R}^2$ die leere Menge.

Bemerkung. Wir können ein quadratisches Polynom

$$Q(x_1, \ldots, x_n) = \sum_{j\leq k} a_{jk} x_j x_k + \sum_{j=1}^{n} b_j x_j + c$$

schreiben als $Q(x) = x^t Ax + b^t x + c$ mit

$$A := \begin{pmatrix} a_{11} & \frac{a_{12}}{2} & \cdots & \frac{a_{1n}}{2} \\ \frac{a_{12}}{2} & a_{22} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ \frac{a_{n1}}{2} & \cdots & \cdots & a_{nn} \end{pmatrix} \in \mathrm{Mat}^{\mathrm{Sym}}_{n\times n}(K), \quad b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}, \; x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in \mathrm{Mat}_{n\times 1}(K).$$

Man kann Q durch eine einzige Matrix $\tilde{A}$ drücken: $Q(x_1, \ldots, x_n) = \tilde{x}^t \tilde{A} \tilde{x}$ mit

$$\tilde{A} := \begin{pmatrix} c & b^t/2 \\ b/2 & A \end{pmatrix} \in \mathrm{Mat}^{\mathrm{Sym}}_{(n+1)\times(n+1)}(K) \quad \text{und} \quad \tilde{x} := \begin{pmatrix} 1 \\ x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathrm{Mat}_{(n+1)\times 1}(K).$$

Definition. Seien Q und Q' zwei quadratische Polynome in n Unbestimmten $x_1, \cdots, x_n$ über $K = \mathbb{R}$. Dann heißen Q und Q'

(1) *affin (algebraisch) äquivalent*, wenn es $S \in \mathrm{GL}_n(\mathbb{R})$ und $v \in \mathbb{R}^n$ gibt mit $Q'(x) = Q(Sx + v)$.
(2) *kartesisch (algebraisch) äquivalent*, wenn es $S \in \mathrm{O}(n)$ und $v \in \mathbb{R}^n$ gibt mit $Q'(x) = Q(Sx + v)$.

Beispiel. Für $n = 2$ betrachten wir $Q(x_1, x_2) = x_1^2 + 4x_2^2 + 2x_1 - 8x_2 + 1$. Wir können diese Polynom schreiben als

$$Q(x_1, x_2) = (x_1 + 1)^2 + 4(x_2 - 1)^2 - 4.$$

Durch die Translation

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} := \begin{pmatrix} x_1 + 1 \\ x_2 - 1 \end{pmatrix} = I_2 x + \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

wird $Z(Q)$ zur Ellipse $Z(Q') = \{y \in \mathbb{R}^2 : y_1^2 + 4y_2^2 = 4\}$. Deshalb sind $Q(x)$ und $Q'(x) := x_1^2 + 4x_2^2 - 4$ zueinander kartesisch äquivalent.

[27.06.18]

Satz 3.13 (Normalformen für reelle Quadriken)**.** *Sei $Q(x) = x^t A x + b^t x + c$ ein quadratisches Polynom in $x = (x_1, \ldots, x_n)^t$ mit $A \in \mathrm{Mat}^{\mathrm{Sym}}_{n\times n}(\mathbb{R})$, $b \in \mathrm{Mat}_{n\times 1}(\mathbb{R})$ und $c \in \mathbb{R}$. Dann ist Q zu einer der folgenden Normalformen kartesisch äquivalent:*

Typ 1. $P(x) = d_1 x_1^2 + \cdots d_r x_r^2$,
Typ 2. $P(x) = d_1 x_1^2 + \cdots d_r x_r^2 + e$ *mit* $e \neq 0$,
Typ 3. $P(x) = d_1 x_1^2 + \cdots d_r x_r^2 + e x_{r+1}$ *mit* $e > 0$.

Jeweils mit $0 \leq r \leq n$ und $d_i \neq 0$. Dabei ist $r = \mathrm{Rang}(A)$ und $d_1, \ldots, d_r$ sind die nicht-Null Eigenwerte von A (mit Vielfach). Ferner gilt

(1) Zwei Normalformen sind genau dann äquivalent, wenn sie zum selben Typ (d.h. Typ 1,2,3) gehören, die Zahlen $d_1, \ldots, d_r$ bis auf Permutation die-selben sind und die Zahlen e übereinstimmen.
(2) Wenn man Q als $Q(x) = \tilde{x}^t \tilde{A} \tilde{x}$ schreiben mit $\tilde{x}^t = (1, x_1, \ldots, x_n)$, dann gilt

$$Q \text{ hat Typ } j \iff \mathrm{Rang}(\tilde{A}) - \mathrm{Rang}(A) = j - 1.$$

Bemerkung.

a) Eine orthogonale Matrix $S \in \mathrm{O}(n)$ definiert eine Abbildung $F_S : \mathbb{R}^n \to \mathbb{R}^n$ mit $F_S(x) = Sx$, so dass $\langle F_S(x), F_S(y)\rangle = \langle x, y\rangle$ für alle $x, y \in \mathbb{R}^n$. Insbesdondere erhält F_S Distanzen:

$$\begin{aligned} d(F_S(x), F_S(y)) &= ||F_S(x) - F_S(y)|| = ||F_S(x - y)|| = \sqrt{\langle F_S(x-y), F_S(x-y)\rangle} \\ &= \sqrt{\langle x - y, x - y\rangle} = d(x, y). \end{aligned}$$

Eine Translation $T : \mathbb{R}^n \to \mathbb{R}^n$ (d.h. eine Abbildung der Form $x \mapsto x + v$ für einen festen Vektor $v \in \mathbb{R}^n$) erhält Distanzen auch. Eine Koordinatentransformation der Form $x \mapsto Sx + v$ mit $S \in \mathrm{O}(n)$ und $v \in \mathbb{R}^n$ erhält Distanzen. Wenn Q und Q' kartesische äquivalent quadratische Polynome sind, dann gibt es eine Koordinatentransformation der Form $x \mapsto Sx + v$ mit $S \in \mathrm{O}(n)$ und $v \in \mathbb{R}^n$, die die Quadrik $Z(Q)$ zu der Quadrik $Z(Q')$ nimmt. Eine Abbildung $\mathbb{R}^n \to \mathbb{R}^n$, die Distanzen erhält, heißt *Isometrie*.[10]

[10] z.B. siehe den Kurs Elementare Geometrie.

b) Es gibt 4 Schritte, um ein quadratisches Polynom in Normalform zu schreiben:
Schritt 1: orthogonale Diagonalisierung.
Schritt 2: quadratische Ergäzung.
Schritt 3: lineare Terme kombinieren.
Schritt 4: Translation.
Die Koordinatentransformationen in den Schritte 1 und 3 sind orthogonale Transformationen und die Koordinatentransformationen in den Schritte 2 und 4 sind Translationen.

Beispiel. Für

$$Q(x_1, x_2) = 5x_1^2 + 5x_2^2 + 8x_1x_2 - 1.$$

wollen wir eine Normalform finden. Der erste Schritt ist die orthogonale Diagonalisierung der symmetrischen Matrix

$$A := \begin{pmatrix} 5 & 4 \\ 4 & 5 \end{pmatrix},$$

d.h. wir müssen eine orthonormale Basis von $\mathbb{R}^2$ von Eigenvektoren von A finden (eine solche Basis existiert nach dem Spektralsatz für symmetrische Matrizen). Es gilt $\chi_A(t) = t^2 - 10t + 9 = (t-1)(t-9)$ und deshalb sind 1 und 9 die Eigenwerte von A mit Eigenräume

$$\mathrm{Eig}(A, 1) = \mathrm{Span}\begin{pmatrix} 1 \\ -1 \end{pmatrix} \quad \text{und } \mathrm{Eig}(A, 9) = \mathrm{Span}\begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Deshalb ist

$$\mathcal{A} := \left\{ v_1 := \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{pmatrix}, v_2 := \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \right\}$$

eine ON-Basis von $\mathbb{R}^2$ von Eigenvektoren und $T := (v_1|v_2) \in \mathrm{O}(2)$ mit $T^tAT = D := \mathrm{diag}(1, 9)$. Sei $S = T^t$ so dass $A = S^tDS$ und

$$Q(x) = x^tAx - 1 = x^tS^tDSx - 1 = (Sx)^tD(Sx) - 1.$$

Dann $Q(x)$ ist kartesisch äquivalent zu $Q'(x) := x^tDx - 1$, da $Q'(Sx) = Q(x)$ (oder $Q'(x) = Q(Tx)$). Das quadrisches Polynom Q' ist schon in Normalform, deshalb müssen wir keine Translation machen. Die Quadrik $Z(Q') = \{x : x_1^2 + 9x_2^2 = 1\} \subset \mathbb{R}^2$ ist eine Ellipse. Die orthogonale Matrix T ist eine Drehung durch $\pi/4$ und deshalb ist $Z(Q)$ die Drehung von $Z(Q')$ durch $\pi/4$.

Korollar. Jedes reelle quadratische Polynom Q in $x_1, \ldots, x_n$ ist genau zu einer der folgenden Normalformen affin (algebraisch) äquivalent:

Typ 1. $P(x) = x_1^2 + \cdots x_k^2 - x_{k+1}^2 \cdots - x_r^2$ mit $0 \le k \le r \le n$,
Typ 2. $P(x) = x_1^2 + \cdots x_k^2 - x_{k+1}^2 \cdots - x_r^2 + e$ mit $0 \le k \le r \le n$ und $e \ne 0$,
Typ 3. $P(x) = x_1^2 + \cdots x_k^2 - x_{k+1}^2 \cdots - x_r^2 - x_{r+1}$ mit $0 \le k \le r \le n$,

wobei $r = \mathrm{Rang}(A)$ und $\mathrm{sign}(A) = k - (r - k) = 2k - r$.

Beispiel. Für $n = 2$ können wir alle Quadriken

$$Q(x) = \tilde{x}^t\tilde{A}\tilde{x} = x^tAx + b^tx + c$$

klassifizieren (bis auf affinen Äquivalenz): seien $r = \mathrm{Rang}(A)$, $\tilde{r} = \mathrm{Rang}(\tilde{A})$ und $s = \mathrm{sign}(A)$, $\tilde{s} = \mathrm{sign}(\tilde{A})$ und $k = (\mathrm{sign}(A) + \mathrm{Rang}(A))/2$. Dann haben wir die folgende Tabelle:

r	$\tilde{r}$	s	$\tilde{s}$	k	$\tilde{k}$	Typ	Polynom $Q(x,y)$ (in NF)	Quadrik $Z(Q) \subset \mathbb{R}^2$
2	2	2	2	2	2	I	x^2+y^2	Punkt
2	2	0	0	1	1	I	x^2-y^2	2 sich schneidende Geraden
2	2	-2	-2	0	0	I	$-x^2-y^2$	Punkt
2	3	2	1	2	0	II	x^2+y^2-1	Ellipse
2	3	0	1	1	1	II	x^2-y^2+1	Hyperbel
2	3	2	3	2	3	II	x^2+y^2+1	$\emptyset$
1	1	1	1	1	1	I	x^2	Doppelte Gerade
1	2	1	0	1	1	II	x^2-1	2 parallele Geraden
1	2	1	2	1	2	II	x^2+1	$\emptyset$
1	3	1	-1	1	1	III	x^2-y	Parabel
0	0	0	0	0	0	I	0	$\mathbb{R}^2$
0	1	0	1	0	1	II	1	$\emptyset$
0	2	0	2	0	2	III	x	Gerade

[02.07.18]

4. Ringe und Moduln

4.1. **Unterringe und Ideale.** Zur Erinnerung: Ein Ring ist eine Menge R mit zwei Verknüpfungen $+ : R \times R \to R$ und $\cdot\ : R \times R \to R$ so dass, $(R, \cdot)$ eine abelsche Gruppe ist mit neutralem Element 0_R, die Multiplikation $\cdot$ assoziativ ist, die Distributivgesetze gelten. Der Ring R heißt

- *kommutativ*, falls die Multipliktation kommutativ ist (d.h. $r_1 \cdot r_2 = r_2 \cdot r_1$ für alle $r_1, r_2 \in R$).
- *Ring mit Eins*, falls die Multiplikation ein Neutralelement $1_R \in R$ hat (d.h. $r \cdot 1_R = r = 1_R \cdot r$ für alle $r \in R$).

Beispiele

(1) $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit 1.
(2) $\mathbb{Z}_n$ mit der modularen Addition und Multiplikation ist ein kommutativer Ring mit 1.
(3) Jeder Körper ist ein kommutativer Ring mit 1.
(4) Für einen Körper K ist die Menge aller Polynome $K[t]$ ein kommutativer Ring mit 1.
(5) $\mathrm{Mat}_{n\times n}(K)$ ist ein Ring mit 1 (die Einheitsmatrix). $\mathrm{Mat}_{n\times n}(K)$ ist genau dann kommuativ, wenn $n = 1$.
(6) Für einen Vektorraum V über einem Körper K ist die Menge aller linearen Endomorphismen $\mathrm{End}_K(V)$ ein Ring mit Eins, wobei die Multiplikation die Komposition ist. Das neutralelement für die Multiplikation ist die Identität $\mathrm{Id}_V : V \to V$. Im allgemeinen ist $\mathrm{End}_K(V)$ nicht kommutativ, da $f \circ g \neq g \circ f$.
(7) Der Nullring $\{0\}$ ist ein kommutativer Ring mit Eins mit $0 = 1$. Wenn $R \neq \{0\}$ ein Ring mit Eins ist, dann gilt $1 \neq 0$ (Für $a \in R \setminus \{0\}$ gilt $1 \cdot a = a \neq 0 = 0 \cdot a$, also folgt $1 \neq 0$).

Definition. Eine Abbildung $\varphi : R \to S$ zwischen Ringen $(R, +_R, \cdot_R)$ und $(S, +_S, \cdot_S)$ ist ein *Ringhomomorphismus*, wenn für alle $r_1, r_2 \in R$

(1) $\varphi(r_1 +_R r_2) = \varphi(r_1) +_S \varphi(r_2)$,
(2) $\varphi(r_1 \cdot_R r_2) = \varphi(r_1) \cdot_S \varphi(r_2)$.
(3) (Falls R und S Ringe mit Eins sind) $\varphi(1_R) = \varphi(1_S)$.

Ein bijektiver Ringhomomorphismus heißt *Ringisomorphismus*.

Beispiel.

(1) Die Identität $\mathrm{Id}_R : R \to R$ ist ein Ringhomomorphismus.
(2) Wenn $\varphi : \mathbb{Z} \to \mathbb{Z}$ ein Ring homomorphismus ist, dann ist $\varphi(1) = 1$. Es folgt, dass $\varphi(r) = r$ (nach Induktion).
(3) Die Abbildung $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ mit $x \mapsto x \mod n$ ist ein Ringhomomorphismus.

(4) Die Abbildung $\varphi : \mathbb{C} \to \mathrm{Mat}_{2\times 2}(\mathbb{R})$ mit

$$\varphi(a+ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

ist ein Ringhomorphismus.

Bemerkung. Für einen Ringhomomorphismus $\varphi : R \to S$ gilt

(1) $\varphi(0_R) = \varphi(0_S)$ (nach dem ersten Axiom),
(2) $\varphi(-r) = -\varphi(r)$ für $r \in R$ (nach dem ersten Axiom),
(3) Die dritte Bedingung $\varphi(1_R) = \varphi(1_S)$ folgt nicht aus den anderen Axiomen (z.B. Seien $R = \{0\}$ und $S = \mathbb{Z}$, dann gelten die erste und zweite Bedingungen für die Nullabbildung $\varphi : R \to S$, aber $\varphi(1_R) = \varphi(0_R) = 0_{\mathbb{Z}} \neq 1_{\mathbb{Z}}$).
(4) φ ist genau dann injektiv, wenn $\ker(\varphi) = \{0_R\}$ (nach dem ersten Axiom),
(5) Wenn φ bijektiv ist, dann ist $\varphi^{-1} : S \to R$ auch ein Ringhomomorphismus.

Definition. Sei $(R, +, \cdot)$ ein Ring.

a) Ein *Unterring* von R ist eine Teilmenge $S \subset R$, so dass S mit der Einschränkung der Addition und Multipliktation von R ein Ring ist. Wenn R ein Ring mit Eins ist, soll ein Unterring S auch das neutralelement 1_R erhalten.
b) Ein *Ideal* von R ist eine Teilmenge $I \subset R$, so dass (I1) -(I2) gelten:
   (I1) I ist eine Untergruppe von $(R, +)$,
   (I2) Für $i \in I$ und $r \in R$ gilt $r \cdot i \in I$ und $i \cdot r \in I$.

Ein Unterring $S \subset R$ (bzw. Ideal $I \subset R$) heißt *echt* wenn $S \neq R$ (bzw. $I \neq R$).

Bemerkung. [04.07.18]

(1) Eine Teilmenge S eines Rings R (mit Eins) ist genau dann ein Unterring, wenn S unter die Subtraktion $-$ und die Multiplikation $\cdot$ abgeschlossen ist (und $1 \in S$).
(2) Wenn R kommutativ ist, dann ist (I2) äquivalent zu
   (I2') $\forall i \in I, r \in R \,:\, r \cdot i \in I$.
   Für einen nicht kommutativen Ring R gibt es Begriffe von Linksideale und Rechtsideale (aber in dieser Einführung werden wir nicht diese Begriffe benutzen).
(3) Ein Ideal ist eine Untergruppe von $(R, +)$, die unter Links- und Rechtsmultiplikation von Elemente aus R abgeschlossen ist. Insbesondere ist I unter $-$ und $\cdot$ abgeschlossen ist (also für Ringe ohne Eins ist jedes Ideal ein Unterring).

Übung. Sei $R \neq \{0\}$ ein kommutativer Ring mit Eins. Beweisen Sie, dass R genau dann ein Körper ist, wenn die einzigen Ideale (von R) genau $\{0_R\}$ und R sind.

Beispiel.

(1) R und $\{0_R\}$ sind immer Ideale von R. Wenn $R \neq \{0\}$ ein Ring mit Eins ist, dann ist $\{0_R\}$ kein Unterring von R.
(2) Sei I ein Ideal von R. Wenn $1 \in I$, folgt $I = R$.
(3) Der Ring $R = \mathbb{Z}$ hat keine echten Unterringe: die Untergruppen von $(\mathbb{Z}, +)$ sind genau die Teilmengen $n\mathbb{Z}$ für $n \in \mathbb{N}$, aber $1 \in n\mathbb{Z}$ genau dann, wenn $n = 1$. Allerdings sind die Untergruppen $n\mathbb{Z}$ Ideale: für $r \in \mathbb{Z}$ und $na \in n\mathbb{Z}$ gilt

$$r \cdot na = n(ra) \in n\mathbb{Z}.$$

(4) Die Teilmenge $\mathbb{Z}$ des Rings $(\mathbb{Q}, +, 0)$ ist ein Unterring aber kein Ideal: $1 \in \mathbb{Z}$ und $\frac{1}{2} \in \mathbb{Q}$, aber $\frac{1}{2} \cdot 1 \notin \mathbb{Z}$).

Übung. Sei R ein kommutativer Ring mit Eins. Beweisen Sie, dass jedes Ideal I von $\mathrm{Mat}_{n\times n}(R)$ die Form $I = \mathrm{Mat}_{n\times n}(J)$ für ein eindeutig bestimmtes Ideal J von R hat.

Satz 4.1. *Sei $\varphi : R \to S$ ein Ringhomomorphismus. Dann gilt*

(1) *Das Bild von φ ist ein Unterrring von S.*
(2) *Für einen Unterring $R' \subset R$ ist $\varphi(R')$ ein Unterring von S.*
(3) *Der Kern $\ker(\varphi)$ ist ein Ideal von R.*
(4) *Für ein Ideal $J \subset S$ ist das Urbild $\varphi^{-1}(J)$ ein Ideal von R.*

Beispiel.

(1) Für den Ringhomomorphismus $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ mit $x \mapsto x \mod n$ ist
$$\ker(\varphi) = \{a \in \mathbb{Z} : a \equiv 0 \mod n\} = n\mathbb{Z}.$$
und $\mathrm{Bild}(\varphi) = \mathbb{Z}_n$.
(2) Sei K ein Körper und $\lambda \in K$. Dann ist die Abbildung $\varphi : K[t] \to K$ mit
$$\varphi(P(t)) = P(\lambda)$$
ein surjetiver Ringhomomorphismus mit
$$\ker(\varphi) = \{P(t) \in K[t] : P(\lambda) = 0\} = \{P(t) \in K[t] : (t-\lambda)|P(t)\} = (t-\lambda)K[t].$$

Satz 4.2. *Sei I ein Ideal eines Rings R. Dann gilt*

(1) *Die Menge $R/I := \{r + I : r \in R\}$ ist ein Ring mit den folgenden Addition und Multiplikation:*
$$(r + I) + (r' + I) := r + r' + I \quad (r + I) \cdot (r' + I) = r \cdot r' + I$$
und das Nullelement is $0_R + I = I$.
(2) *Wenn R kommutativ ist (bzw. ein Ring mit Eins ist), dann ist R/I kommutativ (bzw. ein Ring mit Eins).*
(3) *Die Abbildung $\pi : R \to R/I$, die durch $r \mapsto r + I$ definiert wird, ist ein surjektiver Ringhomomorphismus mit $\ker(\pi) = I$.*
(4) *Die Abbildung*
$$\begin{array}{cccc} \alpha : & \{\textit{Ideale } J \textit{ von } R/I\} & \to & \{\textit{Ideale } M \textit{ von } R \textit{ mit } I \subset M\} \\ & J & \mapsto & \pi^{-1}(J) \end{array}$$
ist bijektiv mit der Umkehrfunktion $M \mapsto \pi(M)$.

Übung. Für $R = \mathbb{Z}$ und $I = n\mathbb{Z}$ mit $n \in \mathbb{N}$ ist $\mathbb{Z}/n\mathbb{Z} = \{x + n\mathbb{Z} : x \in \mathbb{Z}\} \cong \mathbb{Z}_n$. Was sind die Ideale von $\mathbb{Z}/n\mathbb{Z}$?

Satz 4.3. *(Homomorphiesatz für Ringe) Sei $\varphi : R \to S$ ein Ringhomomorphismus. Dann gibt es einen Ringisomorphismus*
$$\tilde{\varphi} : R/\ker(\varphi) \to \varphi(R)$$
mit $\tilde{\varphi} \circ \pi = \varphi$, wobei $\pi : R \to R/\ker(\varphi)$ der natürliche surjektive Ringhomomorphismus ist.

[09.07.18] **Definition.** Sei R ein kommutativer[11] Ring.

(1) Für $r \in R$ definieren wir das *von r erzeugte Ideal*
$$\langle r \rangle = rR := \{r \cdot s : s \in R\}.$$
Ideale von R der Form $\langle r \rangle$ werden *Hauptideale* genannat.
(2) Für eine Teilmenge $A \subset R$ definieren wir das *von A erzeugte Ideal*
$$\langle A \rangle = \{\sum_{i=1}^{n} r_i a_i : n \in \mathbb{N}, r_i \in R, a_i \in A\}.$$

[11]Die Definition für nicht kommutative Ringe ist ein bisschen mehr kompliziert

Übung. Der Durchschnitt einer Familie von Idealen eines Rings R ist ein Ideal. Für eine Teilmenge A eines kommutativen Rings R die Menge $\langle A\rangle$ ist eine Ideal von R und es gilt

$$\langle A\rangle = \bigcap_{\substack{A\subset J\subset R\\ J \text{ Ideal}}} J,$$

und $\langle A\rangle$ ist das kleinste Ideal in R, das A enthält.

Beispiel.

(1) Für einen kommutativen Ring mit Eins ist $\langle 1_R\rangle = R$.
(2) Für $R = \mathbb{Z}$ ist $\langle n\rangle = n\mathbb{Z}$.

4.2. **Moduln.** Zur Erinnerung: Ein Vektorraum über einem Körper K ist eine abelsche Gruppe $(V, +)$ mit einer Skalarmultiplikation $\cdot\, :\, K\times V\to V$ so dass i) $\lambda\cdot(\mu\cdot v) = (\lambda\cdot\mu)\cdot v$ für alle $v\in V$ und $\mu,\lambda\in K$ und ii) $1_K\cdot v = v$ für alle $v\in V$ und iii) die Distributivegesetze gelten.

Definition. Sei R ein Ring mit Eins. Ein R-(Links)modul ist eine abelsche Gruppe $(M, +)$ mit einer Abbildung

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

die Skalarmultiplikation genannt wird, so dass für $a, b\in R$ und $m, n\in M$ gilt

i) $a\cdot(b\cdot m) = (ab)\cdot m$,
ii) $1_R\cdot m = m$,
iii) Die Distributivegesetze: $(a+b)\cdot m = a\cdot m + b\cdot m$ und $a\cdot(m+n) = a\cdot m + a\cdot n$.

Beispiel.

(1) Sei $R = K$ ein Körper. Dann sind K-Moduln genau die K-Vektorräume.
(2) Jede abelsche Gruppe $(G, +)$ ist ein $\mathbb{Z}$-Modul mit Skalarmultiplikation $\cdot\, :\, \mathbb{Z}\times G\to G$

$$n\cdot g := \begin{cases} g+\cdots+g\ \ (n\ \text{ mal}) & \text{wenn } n>0\\ 0_G & \text{wenn } n=0\\ (-g)+\cdots+(-g)\ \ (n\ \text{ mal}) & \text{wenn } n>0\end{cases}$$

Umgekehrt ist jeder $\mathbb{Z}$-Modul eine abelsche Gruppe nach die Axiome oben. Zum Beispiel sind die abelsche Gruppen $(\mathbb{Z}/n\mathbb{Z}, +)$ Moduln über $\mathbb{Z}$.
(3) Sei V ein endlichdimensionaler Vektorraum über einem Körper K und $f\in \mathrm{End}_K(V)$. Dann ist V ein $K[t]$-Modul mit der Skalarmultiplikation $K[t]\times V\to V$

$$P(t)\cdot v := P(f)(v).$$

(4) Ein Ideal eines Ring R ist ein Modul, wobei die Skalarmultiplikation $R\times I\to I$ die Einschränkung der Multiplikation auf R ist.
(5) Für einen R-Modul M ist ein Untermodul eine Teilmenge $N\subset M$, die eine Untergruppe von $(M, +)$ ist, so dass $r\cdot n\in N$ für alle $r\in R$ und $n\in N$. Jeder Untermodul ist auch ein R-Modul.

Übung. Sei R ein Ring und $(N_i)_{i\in I}$ eine Familie von Untermoduln eines R-Moduls M. Dann ist auch der Durchschnitt $\cap_{i\in I} N_i$ ein Untermodul von M.

Definition. Seien M und N zwei R-Moduln. Eine Abbildung $\varphi : N\to M$ heißt Homomorphismus von R-Moduln (oder R-linear), wenn

(1) $\varphi(n_1+n_2) = \varphi(n_1)+\varphi(n_2)$ für alle $n_1, n_2\in N$
(2) $\varphi(r\cdot n) = r\cdot\varphi(n)$ für alle $n\in N$ und $r\in R$.

Der Kern von φ ist $\ker(\varphi) = \{n\in N : \varphi(n) = 0_M\}$ und das Bild ist $\mathrm{Bild}(\varphi) := \varphi(N)\subset M$. Der Cokern ist $\mathrm{Coker}(\varphi) := M/\,\mathrm{Bild}(\varphi) = M/\varphi(N)$.

Beispiel. Sei $R = \mathbb{Z}$ und $N = M = \mathbb{Z}$. Dann ist $\varphi : \mathbb{Z} \to \mathbb{Z}$ mit $\varphi(m) = n \cdot m$ ein Homomorphismus von $\mathbb{Z}$-Moduln (aber kein Ringhomomorphismus) mit

$$\ker(\varphi) = \{0\} \quad \text{und} \quad \mathrm{Bild}(\varphi) = n\mathbb{Z} \quad \text{und} \quad \mathrm{Coker}(\varphi) = \mathbb{Z}/n\mathbb{Z}.$$

Bemerkung. Sei M ein R-Modul und $N \subset M$ ein Untermodul. Dann gilt

(1) Die Quotientengruppe $M/N := \{m + N : m \in M\}$ mit der Skalarmultiplikation

$$r \cdot (m + N) := rm + N$$

für $r \in R$ und $m + N \in M/N$ bildet einen R-Modul.

(2) Die Abbildung $\pi : M \to M/N$ mit $\pi(m) := m + N$ ist ein surjektiver R-Modul-Homomorphismus mit $\ker(\pi) = N$.

Bemerkung.(Homomorphiesatz für Moduln). Sei $\varphi : N \to M$ ein Homomorphismus von R-Moduln. Dann gilt

(1) $\ker(\varphi) := \{n \in N : \varphi(n) = 0\}$ ist ein Untermodul von N.
(2) $\mathrm{Bild}(\varphi)$ ist ein Untermodul von M.
(3) $\mathrm{Coker}(\varphi)$ hat die Struktur eines R-Moduls, so dass $M \to \mathrm{Coker}(\varphi)$ ein Homomorphismus von R-Moduln ist.
(4) Es gibt einen Isomorphismus von R-Moduln $\tilde{\varphi} : N/\ker(\varphi) \to \mathrm{Bild}(\varphi)$ so dass $\tilde{\varphi} \circ \pi = \varphi$ für $\pi : N \to N/\ker(\varphi)$.

4.3. **Basen.** Jeder K-Vektorraum hat eine Basis (sogar unendlichdimensionale Vektorräume, wenn wir das Axiom der Wahl annehmen). Diese Eigenschaft gilt jedoch nicht für Moduln: Es gibt viele Moduln, die keine Basis haben. Dieser Unterschied ist der erste große Unterschied zwischen Vektorräumen und Moduln.

Definition. Sei M ein Modul über einem Ring R und $A \subset M$ eine Teilmenge. Der *von A erzeugte Untermodul* $\langle A \rangle$ von M ist der kleinste Untermodul von M, der A enthält, d.h.

$$\langle A \rangle = \bigcap_{\substack{A \subset N \subset M \\ N \text{ Untermodul}}} N.$$

Die Teilmenge A heißt *Erzeugendensystem* von M, wenn $\langle A \rangle = M$. Wenn A endlich ist mit $\langle A \rangle = M$, dann heißt M *endlich erzeugt*.

Bemerkung. Es gilt

$$\langle A \rangle = \left\{ \sum_{i=1}^{n} r_i a_i : n \in \mathbb{N}, r_i \in R \text{ und } a_i \in A \right\}.$$

Beispiel.

(1) Für einen Körper K, einen K-Vektorraum V und $A \subset V$ gilt

$$\langle A \rangle = \mathrm{Span}(A).$$

(2) Sei $R = \mathbb{Z}$ und $M = \mathbb{Z}/n\mathbb{Z}$. Dann ist $1 + m\mathbb{Z}$ ein Erzeugendensystem von M.
(3) Sei $R = \mathbb{Z}$. Das Element $2 + 4\mathbb{Z} \in \mathbb{Z}/4\mathbb{Z}$ erzeugt den Untermodul $\langle 2 + 4\mathbb{Z} \rangle = \{0 + 4\mathbb{Z}, 2 + 4\mathbb{Z}\}$ von $\mathbb{Z}/4\mathbb{Z}$. Dieser Untermodul ist eine Untergruppe von $\mathbb{Z}/4\mathbb{Z}$, die isomorph zu $\mathbb{Z}/2\mathbb{Z}$ ist.

Definition. Sei M ein R-Modul und $(m_i)_{i \in I}$ eine Familie von Elementen von M.

(1) Die Familie $(m_i)_{i \in I}$ heißt *linear unabhängig*, wenn für jede endliche Teilmenge $J \subset I$ gilt

$$\sum_{j \in J} r_j m_j = 0 \text{ mit } r_j \in R \implies r_j = 0 \text{ für alle } j \in J.$$

(2) Die Familie $(m_i)_{i \in I}$ heißt *Erzeugendensystem* von M, wenn $\langle \{m_i : i \in I\} \rangle = M$.

(3) Eine *Basis* von M ist eine lineare unabhängig Familie $(m_i)_{i\in I}$ von Element von M, die M erzeugt.
(4) M heißt *frei*, wenn M eine Basis besitzt.

Beispiel.
(1) R^n ist ein freier R-Modul mit Basis $\mathcal{A} = \{e_1, \ldots, e_n\}$, wobei $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ mit der 1 an i-ter Stelle.
(2) Sei K ein Körper. Jeder K-Vektorraum ist ein freier K-Moduln.
(3) Nicht jeder R-Modul ist frei: Sei $R = \mathbb{Z}$ und $M = \mathbb{Z}/n\mathbb{Z}$. Für $m = a + n\mathbb{Z} \in M$ gilt $n \cdot m = n \cdot a + n\mathbb{Z} = 0 + n\mathbb{Z}$. Daher ist die Menge $\{m\}$ linear abhängig.

Satz 4.4. *Sei $\mathcal{A} := \{m_1, \ldots, m_n\}$ eine endliche geordnete Teilmenge eines R-Modul M. Dann gibt es einen Homomorphismus von R-Moduln*

$$\begin{array}{rccc} \varphi_{\mathcal{A}}: & R^n & \to & M \\ & (r_1, \ldots, r_n) & \mapsto & \sum_{i=1}^n r_i \cdot m_i. \end{array}$$

Ferner gilt
i) $\mathcal{A}$ ist genau dann ein Erzeugendensystem von M, wenn $\varphi_{\mathcal{A}}$ surjektiv ist.
ii) $\mathcal{A}$ ist genau dann linear unabhängig, wenn $\varphi_{\mathcal{A}}$ injektiv ist.
iii) $\mathcal{A}$ ist genau dann eine Basis von M, wenn $\varphi_{\mathcal{A}}$ bijektiv ist.
Wenn M ein endlich erzeugter freier R-Modul ist, dann gibt es $n \in \mathbb{N}$ mit $M \cong R^n$.

Literatur

- S. Bosch, Lineare Algebra, 4. Auflage, Springer-Verlag, 2008.
- G. Fischer, Lineare Algebra: Eine Einführung fr Studienanfänger (vieweg studium; Grundkurs Mathematik),2013.
- W. Klingenberg, Lineare Algebra und Geometrie, Springer-Verlag, 1984.
- S. Lang, Introduction to linear algebra, Second edition, Springer, 1986.
- S. Lang, Linear Algebra, Third edition, Springer, 1987.
- J. Liesen und V. Mehrmann, Lineare Algebra, Vieweg, 2011.

Freie Universität Berlin, Arnimallee 3, Raum 011, 14195 Berlin, Germany

hoskins@math.fu-berlin.de