Mitschriebe zur Linearen Algebra 1

Raphael Michel

Stand: 20. Februar 2014

Dies ist eine nicht autorisierte Mitschrift der Linearen Algebra I, wie sie im Wintersemester 2013/14 an der Universität Heidelberg von Dr. A. Riedel gehalten wurde. Sie ist sicherlich voller Fehler, wobei ich mich über Hinweise auf solche an mail@raphaelmichel.de freue.

Inhaltsverzeichnis

I. Grundbegriffe

§ 1. Grundbegriffe

1.1. Die Mengenschreibweise

Definition 1, § 1 (*Cantor*)

Eine Menge M ist eine Zusammenfassung bestimmter wohlunterscheidbarer Objekte unserer Anschauung oder unseres Denkens zu einem Ganzen.

Interpretation:

- Objekte unserer Anschauung $\iff$ mathematische Objekte
- Zusammenfassung zu einem Ganzen $\iff$ betrachtet als neues mathematisches Objekt
- wohl unterscheidbar $\iff$ Gleichheit und Ungleichheit müssen geklärt sein

Achtung: Es gibt Zusammenfassungen, die keine Mengen sind ($\rightarrow$ Russels Paradoxon).
Schreibweise und Beispiele:

$$
\begin{aligned}
Z &= \{0, 1, \ldots, 9\} \quad \text{Menge der Ziffern} \\
A &= \{a, b, \ldots, z\} \quad \text{Menge der Buchstaben} \\
X &= \{xy | x \in Z, y \in Z\} = \{00, 01, 02, \ldots, 99\} \\
\varnothing &= \{\} \quad \text{Leere Menge} \\
1 &\in Z \\
2 &\notin A
\end{aligned}
$$

Definition 2, § 1

Seien M und N Mengen.

- *N heißt* ***Teilmenge*** *von M*

$$N \subset M \iff \forall x \in N : x \in M$$

- *N und M heißen* ***gleich****:*

$$M = N \iff N \subset M \wedge M \subset N$$

- $\mathscr{P}(M)$ *ist die Menge aller Teilmengen von M, genannt* ***Potenzmenge****.*

- *Das „Komplement von N in M“ wird genannt:*

$$M \backslash N = \{x \in M | x \notin N\}$$

- ***Durchschnitt***

$$M \cap N = \{x | x \in M \wedge x \in N\}$$

- ***Vereinigung***

$$M \cup N = \{x | x \in M \vee x \in N\}$$

Schreibweise Seien M und I Mengen, $M_i \subset M, i \in I$.

$$\bigcap_{i \in I} M_i := \{x \in M | \forall i \in I : x \in M_i\}$$
$$\bigcup_{i \in I} M_i := \{x \in M | \exists i \in I : x \in M_i\}$$

Bemerkung 1, § 1

Für Mengen $A, B, C \subset M$ gilt:

1. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
2. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
3. $A \cap B = A \iff A \subset B \iff A \cup B = B$

Beweis: 1. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

„$\subseteq$“ $a \in A \cap (B \cup C) \implies a \in A \wedge a \in B \cup C$

a) $a \in A \wedge a \in B$

b) $a \in A \wedge a \in C$

$\implies a \in (A \cap B) \cup (A \cap C)$

„$\supseteq$“ $a \in (A \cap B) \cup (A \cap C) \implies a \in A \cap B \vee a \in A \cap C \implies a \in A \wedge (a \in B \vee a \in C) \implies a \in A \wedge a \in (B \cup C) \implies a \in A \cap (B \cup C)$

2. analog
3. trivial aus Definition ■

Definition 3, § 1

Seien $M, I \neq \varnothing$ Mengen, $M_i \subset M \forall i \in I$.
*$\{M_i\}$ heißt **Partition** von M, wenn:*

1. $\forall i \in I : M_i \neq \varnothing$

2. $\bigcup_{i\in I} M_i = M$

3. $\forall i \neq j \implies M_i \cap M_j = \varnothing$

M heißt disjunkte Vereinigung der M_i:

$$M = \dot{\bigcup_{i\in I}} M_i$$

Beispiel 1, § 1

A = Menge der Vokale disjunkt vereinigt mit Menge der Konsonanten.

1.2. Relationen

Definition 4, § 1

M, N seien Mengen.

- $M \times N := \{(m,n) | m \in M, n \in N\}$ *heißt* ***Paarmenge*** *oder* ***kartesisches Produkt****.*
- $R \subseteq M \times N$ *heißt zweistellige Relation über* $M \times N$
- *R heißt* ***reflexiv*** $\iff \forall m \in M : (m,m) \in R$
- *R heißt* ***transitiv*** $\iff \forall l,m,n \in M : (l,m) \in R, (m,n) \in R \implies (l,n) \in R$
- *R heißt* ***symmetrisch*** $\iff \forall m,n \in M : (m,n) \in R \implies (n,m) \in R$
- *R heißt* ***antisymmetrisch*** $\iff \forall m,n \in M : (m,n) \in R \wedge (n,m) \in R \implies m = n$
- *R heißt* ***Äquivalenzrealation****: R ist reflexiv, transitiv und symmetrisch. Man kann schreiben:* $(m,n) \in R \iff m \sim n$
- *R heißt* ***Ordnungsrealation****: R ist reflexiv, transitiv und antisymmetrisch. Man kann auch schreiben:* $(m,n) \in R \iff m \preceq n$
- *R heißt* ***Totalordnung****: R ist Ordnungsrelation und* $\forall m,n : (m,n) \in R \vee (n,m) \in R$*. Man kann auch schreiben:* $(m,n) \in R \iff m \leqslant n$

Beispiel 2, § 1

Menge aller Menschen M.
Die Relation „m, n sind blutsverwandt“ ist reflexiv und symmetrisch.
Die Relation „m, n sind gleichgeschlechtlich“ ist Äquivalenzrelation

Beispiel 3, § 1

Menge M, $\mathscr{P}(M)$*,* $L,N \in \mathscr{P}(M)$*,* $R_i \subseteq M \times M$

- $(L,N) \in R_1 :\iff L \subseteq N$, *ist Ordnung auf* $\mathscr{P}(M)$
- $(L,N) \in R_2 :\iff L = N$ *ist Äquivalenzrelation*

Bemerkung 2, § 1

$M, I \neq \varnothing, M_i \subseteq M, i \in I$
Dann sind äquivalent:

1. $\{M_i | i \in I\}$ *ist Partition*
2. $(m,n) \in R :\iff \exists! i \in I : m \in M_i, n \in M_i$ *ist Äquivalenzrelation*

Beweis : 1. $\Longrightarrow$ **2.:** R ist reflexiv, symmetrisch und transitiv, folgt aus Definition

2. $\Longrightarrow$ **1.:** $K_n := \{m \in M | (m,n) \in R\}$

$K_n \neq \varnothing$ da R reflexiv ist und $K_n = M_i$ falls $n \in M_i$. Es reicht also zu zeigen, dass $\{K_n\}$ Partition von M ist. Dass $\bigcup K_n = M$ ist, ist trivial, das letzte Kriterium kann per Widerspruchsbeweis bewiesen werden:

Angenommen $\exists m,n \in M : K_n \neq K_m \wedge K_n \cap K_m \neq \varnothing$.

$$\Longrightarrow \exists l \in M : l \in K_m \cap K_n \Longrightarrow (l,m) \in R \wedge (l,n) \in R$$
$$\overset{\text{symm.}}{\Longrightarrow} (m,l) \in R \wedge (l,n) \in R \overset{\text{trans.}}{\Longrightarrow} (m,n) \in R \Longrightarrow k \in K_n$$
$$(k,n) \in R \overset{\text{refl./trans.}}{\Longrightarrow} (k,m) \in R \Longrightarrow k \in K_m$$
$$\Longrightarrow K_n \subseteq K_m \text{ und } K_m \subseteq K_n$$
$$\Longrightarrow K_m = K_n \lightning$$

■

Definition 5, § 1

Sei R Äquivalenzrelation auf M

- $K_n := \{m \in M | m \sim n\} =: [n], \quad n \in M$ *heißt* ***Äquivalenzklasse*** *von* n.
- $l \in K_n$ *heißt* ***Vertreter*** *oder Repräsentant von* K_n.
- *Die Familie aller dieser Äquivalenzklassen nennt man Quotientenmenge*

$$M/\sim \; = M/_R := \{K_n | n \in M\}$$

1.3. Abbildungen

Definition 6, § 1

Seien M, N Mengen. $G \subset M \times N$ heißt ***Graph****, wenn*

1. $\forall m \in M \quad \exists n \in N : (m,n) \in G$
2. $(m,n_1) \in G \wedge (m,n_2) \in G \iff n_1 = n_2$

Dann heißt $f := f_G : M \to N, \quad m \mapsto n =: f(m)$ ***Abbildung*** *zu G. $f(m)$ heißt Bild von m.*

- *Die Menge*
$$M_n = \{m \in M | f(m) = n\}$$
heißt Urbildmenge von n. m ist ein ***Urbild*** *von n.*
- *Die Menge $\mathrm{Abb}(M,N) \equiv N^M$ ist die Menge aller Abbildungen von M nach N.*
- *f heißt surjektiv $: \iff f(M) = N$*
- *f heißt injektiv $: \iff \forall m,n \in M : f(m) = f(n) \implies m = n$*
- *f heißt bijektiv $: \iff$ f surjektiv und injektiv*

Beispiel 4, § 1

- *Sei M Menge. Die „identische Abbildung“ $\mathrm{id}_M : M \to M, \quad m \mapsto m$ ist bijektiv.*
- *Sei $N \subset M, \quad i : N \to M, \quad n \mapsto n$. i heißt „Inklusion“ und ist injektiv, aber nicht surjektiv.*
- *Sei M Menge, R Äquivalenzrelation auf M.*
$$k : M \to M/_R \quad m \mapsto K_m$$
ist surjektiv.

Bemerkung 3, § 1

Seien M, N Mengen und $f : M \to N$ eine Abbildung. Die Urbildmengen $\{M_n | n \in f(M)\}$ bildet eine Partition von M.

Beweis : Nach vorheriger Bemerkung reicht zu zeigen, dass $(k,l) \in R \iff k \in M_n \wedge l \in M_n \iff f(k) = n = f(l) \implies$ ist Äquivalenzrelation. ■

Definition 7, § 1

~~L, M~~, N Mengen. $g : L \to M, f : M \to N$. Dann heißt $f \circ g : L \to N, l \mapsto f(g(l))$ ***Abbildungsprodukt*** *von f und g.*

Bemerkung 4, § 1

1. *Das Abbildungsprodukt zweier Abbildungen ist wieder eine Abbildung*
2. *Abbildungsprodukt ist* assoziativ, *d.h. mit* $h : K \to L, g : L \to M, f : M \to N$ *gilt*

$$f \circ (g \circ h) = (f \circ g) \circ h$$

Beweis : 1. $G = \{(l, (f \circ g)(l)) | l \in L\}$ ist ein Graph!

2. $(f \circ (g \circ h))(x) = f(g(h(x))) = ((f \circ g) \circ h)(x)$ ■

Bemerkung 5, § 1

M, N Mengen, $f : M \to N$ *bijektiv* $\Longrightarrow$ *es gibt genau eine Abbildung* $f^{-1} : N \to M$ *mit* $f \circ f^{-1} = \mathrm{id}_N$ *und* $f^{-1} \circ f = \mathrm{id}_M$

Beweis : f surjektiv $\Longrightarrow \forall n \in N : \quad \exists m \in M : f(m) = n$

f injektiv $\Longrightarrow$ m ist durch n eindeutig bestimmt (m_n).

Existenz der Umkehrabbildung:

$$f^{-1} : N \to M, n \mapsto m_n$$
$$(f \circ f^{-1})(n) = f(f^{-1}(n)) = f(m_n) = n$$
$$(f^{-1} \circ f)(m) = m$$

Eindeutigkeit: Beweis durch Annahme von Existenz einer weiteren Abbildung $\tilde{f}^{-1}$ mit den geforderten Eigenschaften.

$$f^{-1} = \mathrm{id}_M \circ f^{-1} = (\tilde{f}^{-1} \circ f) \circ f^{-1} = \tilde{f}^{-1} \circ (f \circ f^{-1}) = \tilde{f}^{-1} \circ id_M = \tilde{f}^{-1}$$

■

Bemerkung 6, § 1

Für das Abbildungsprodukt zweier Abbildungen $f : N \to L, g : M \to N$ *gilt:*

1. f, g *surjektiv* $\Longrightarrow$ $f \circ g$ *surjektiv*
2. f, g *injektiv* $\Longrightarrow$ $f \circ g$ *injektiv*
3. $f \circ g$ *surjektiv* $\Longrightarrow$ f *surjektiv*
4. $f \circ g$ *injektiv* $\Longrightarrow$ g *injektiv*
5. $f \circ g$ *bijektiv* $\Longrightarrow$ f *surjektiv,* g *injektiv*

Beweis : 1. klar

2. $(f \circ g)(m_1) = (f \circ g)(m_2) \implies f(g(m_1)) = f(g(m_2)) \overset{f \text{ inj.}}{\Longrightarrow} g(m_1) = g(m_2) \overset{g \text{ inj.}}{\Longrightarrow} m_1 = m_2$

3. Angenommen, f wäre nicht surjektiv $\Longrightarrow \exists n \in N, n \notin f(N) \Longrightarrow \exists k \notin f(g(M)) \Longrightarrow f \circ g$ nicht surjektiv $\lightning$
4. Angenommen, g wäre nicht injektiv $\Longrightarrow \exists l \neq l' : g(l) = g(l') \Longrightarrow f(g(l)) = f(g(l')) \Longrightarrow$ $f \circ g$ nicht injektiv $\lightning$
5. folgt aus 3. und 4. ■

Satz 1, § 1

Jede Abbildung einer Menge M in N lässt sich schreiben als Abbildungsprodukt einer surjektiven, einer bijektiven und einer injektiven Abbildung.

Beweis :

$$
\begin{aligned}
&f : M \to N, \quad \bar{M} = \{M_n | n \in f(M)\} \\
&k : M \to \bar{M}, \quad m \mapsto M_{f(m)} \quad \text{Abb., surj.} \\
&\bar{f} : \bar{M} \to f(M), \quad M_n \mapsto n \quad \text{Abb., bijektiv} \\
&\quad \text{surj. klar; inj., da } \bar{f}(M_n) = \bar{f}(M_{n'}) \Longrightarrow n = n' \Longrightarrow M_n = M_{n'} \\
&i : f(M) \to N, \quad n \mapsto n \quad \text{Abb. injektiv} \\
&i \circ \bar{f} \circ k = f = (m \mapsto f(m)) \\
&m \mapsto M_{f(m)} \mapsto f(m) \mapsto f(m) = (m \mapsto f(m))
\end{aligned}
$$

■

1.4. Gruppen

Der Gruppenbegriff

Definition 8, § 1

- *Gegeben sei eine Menge G mit Verknüpfung (Abbildung).*

$$G \times G \to G, \quad (a, b) \mapsto a * b$$

- *G heißt **Halbgruppe** $\Longleftrightarrow \forall a, b, c, \in G : \quad (a*b)*c = a*(b*c)$ (Assoziativität).*
- *G heißt **Halbgruppe mit Eins** $\Longleftrightarrow$ G Halbgruppe und $\exists e \in G : \quad \forall a \in G : e * a = a * e = a$*
- *G heißt **Gruppe** $\Longleftrightarrow$ G Halbgruppe mit Eins und $\forall a \in G \quad \exists b \in G : \quad a * b = b * a = e$. Schreibweise: $(G, *)$*
- *G heißt kommutative oder **abelsche Gruppe** $\Longleftrightarrow$ G Gruppe und $\forall a, b \in G : a * b = b * a$*

Beispiel 5, § 1

1. *$(\mathbb{R}, +), (\mathbb{R}_{>0}, \cdot)$ sind abelsche Gruppen. $(\mathbb{R}_{>0}, +)$ ist Halbgruppe.*

2. *M Menge, $M^M = \mathrm{Abb}(M,M)$ ist Halbgruppe mit Eins.*
   $(S_M, \circ)$ ist (nicht-abelsche) Gruppe mit $S_M = \{f \in M^M | f \text{ bijektiv}\}$.

Bemerkung 7, § 1

$(G,*) \implies$

1. *$e \in G$ (neutrales Element) ist eindeutig bestimmt*
2. *Zu jedem $a \in G$ ist das Inverse $b = a^{-1}$ eindeutig bestimmt.*

Beweis: 1. Angenommen $\exists e, \tilde{e} \implies e = e * \tilde{e} = \tilde{e}$

2. Angenommen $\exists b, \tilde{b}$ invers zu $a \implies b * a = e = a * \tilde{b} \implies b = b * e = b * (a * \tilde{b}) = (b * a) * \tilde{b} = e * \tilde{b} = \tilde{b}$. ■

Satz 2, § 1

$G \neq \varnothing$ Menge, $*$ Verknüpfung auf G. Dann gilt: G ist Gruppe $\iff$

1. *$*$ ist assoziativ*
2. *$\forall a, b \in G \exists x, y : x * a = b, a * y = b$. Dabei sind x, y eindeutig durch a, b bestimmt.*

Beweis: „$\implies$“ G Gruppe, $x := b * a^{-1}$, $y := a^{-1} * b \implies x, y$ eindeutig mit $x * a = (b * a^{-2}) * a = b * (a^{-1} * a) = b, (a * a^{-1}) * b = b$.

„$\Leftarrow$“ zu zeigen: Einselement und Inverse existieren.

- Sei $a \in G \implies \exists e : e * a = a \wedge \forall b : \exists y : a * y = b \implies e * b = e * (a * y) = (e * a) * y = a * y = b$
  $\forall b \in G : \exists f \in G : b * f = b \wedge \forall a \in G : \exists y : y * b = a \implies a * f = a$ und $e = e * f = f$
- $\forall a \in G : \exists x \in G : x * a = e$ und $\exists y \in G : a * y = e \implies x = x * e = x * (a * y) = (x * a) * y = e * y = y$ ■

Definition 9, § 1

$(G,*)$ Gruppe. Eine Teilmenge $H \subset G$, $H \neq \varnothing$ heißt ***Untergruppe*** *$H < G \iff \forall a, b \in H : a * b \in H \wedge a^{-1} \in H \implies (H,*)$ ist Gruppe.*

Beispiel 6, § 1

- *Aus Analysis: $(\mathbb{R}_{>0}, \cdot)$ ist Gruppe $< (\mathbb{R}^* := \mathbb{R}\backslash\{0\}, \cdot)$ und $(\mathbb{Z}, +) < (\mathbb{R}, +)$.*
- *M Menge, $N \subset M$. $f \in S_N$ (Gruppe der bijektiven Selbstabbildungen).*
  $\exists! \tilde{f} \in S_M : \quad f = \tilde{f}|_N \wedge \tilde{f}|_{M\backslash N} = \mathrm{id}_{M\backslash N}$
  $j_N : S_N \to S_M, \quad f \mapsto \tilde{f}$ ist injektive Abbildung ($\tilde{f} = \tilde{g} \implies f = g$).

1.5. Homomorphismen

Definition 10, § 1

$(G,*),(H,\circ)$. $f \in Abb(G,H)$ heißt ***Homomorphismus*** : $\iff \forall a,b \in G: \quad f(a*b) = f(a)\circ f(b)$.
Ein injektiver Homomorphismus heißt ***Monomorphismus****.*
Ein surjektiver Homomorphismus heißt ***Epimorphismus****.*
Ein bijektiver Homomorphismus heißt ***Isomorphismus*** *($G \cong H$).*

Beispiel 7, § 1

$\exp\colon (\mathbb{R},+) \to (\mathbb{R}^*,\cdot)$ *ist Homomorphismus:* $\exp(x+y) = \exp(x)\exp(y)$ *ist Isophormismus auf* $(\mathbb{R}_{>0},\cdot)$.

Bemerkung 8, § 1

$(G,\cdot),(H,\cdot)$ *Gruppen mit Einsen* e_G *und* e_H, $f\colon G \to H$ *Homomorphismus.*

1. $f(e_G) = e_H$
2. $\forall a \in G: f(a)^{-1} = f(a^{-1})$
3. f *Isomorphismus* $\implies$ f^{-1} *Isomorphismus*

Beweis : 1. $e_H \cdot f(e_G) = f(e_G) = f(e_G\cdot e_G) = f(e_G)\cdot f(e_G) \overset{\cdot f(g)^{-1}}{\implies} e_H = f(e_G)$

2. $e_H = f(e_G) = f(aa^{-1}) = f(a)f(a^{-1}) \overset{f(a^{-1})\cdot}{\implies} f(a^{-1})e_H = f(a)^{-1}f(a)f(a^{-1}) \implies f(a)^{-1} = f(a^{-1})$
3. $\forall \tilde{a},\tilde{b} \in H \quad \exists! a,b \in G: f(a)=\tilde{a}, f(b)=\tilde{b}.\ f(ab) = f(a)f(b) = \tilde{a}\tilde{b} \implies f^{-1}(\tilde{a}\tilde{b}) = ab = f^{-1}(\tilde{a})\cdot f^{-1}(\tilde{b}) \implies f^{-1}$ Homomorphismus. ∎

Definition 11, § 1

G,H *Gruppen,* $g\colon G \to H$ *Homomorphismus.*

$$\implies \ker f := \{a \in G | f(a) = e_H\} \tag{I.1}$$

heißt Kern von f.

Bemerkung 9, § 1

1. $\ker f < G$
2. *Auf* G *wird durch* $a \sim b$ $(a \equiv b) : \iff ab^{-1} \in \ker f$ *eine Äquivalenzrelation definiert mit* $a \equiv \tilde{a} \wedge b \equiv \tilde{b} \implies ab \equiv \tilde{a}\tilde{b}$.
3. *Die Quotientenmenge* $\bar{G} := G/_{\ker f}$ *mit Verknüpfung* $\bar{G}\times\bar{G} \to \bar{G}, \quad (\bar{a},\bar{b}) \mapsto \bar{a}\cdot\bar{b} := \overline{a\cdot b} \quad (\bar{a} := k(a), \quad k\colon G \to G)$ *bildet eine Gruppe.*

4. *f injektiv* $\iff \ker f = \{e_G\}$

Beweis: 1. $a,b \in \ker f \implies f(a) = e_H = f(b) \implies f(ab) = f(a)f(b) = e_H e_H = e_H \implies ab \in \ker f$

$f(a^{-1}) = f(a)^{-1} = e_H^{-1} = e_H \implies a^{-1} \in \ker f \implies \ker < G$

2. $ab^{-1} \in \ker f \iff f(ab^{-1}) = e_H \iff f(a)f(b)^{-1} = e_H \overset{\cdot f(b)}{\iff} f(a) = f(b) \implies \equiv$ ist Äquivalenzrelation.

$a \equiv \tilde{a} \wedge b \equiv \tilde{b} \implies f(a) = f(\tilde{a}) \wedge f(b) = f(\tilde{b})$

$f(ab) = f(a)f(b) = f(\tilde{a})f(\tilde{b}) = f(\tilde{a}\tilde{b}) \implies ab \equiv \tilde{a}\tilde{b}$

3. wie oben ist wohldefiniert, $k\colon G \to \bar{G}$ ist surjektiver Gruppenhomophormismus, d.h. die Gruppenstruktur überträgt sich.

4. „⇒“ f injektiv $\implies f(x) = e_H = f(y) \implies x = y$.

Wir wissen: $f(e_G) = e_H \implies (f(x) = e_H \implies x = e_G)$

$\implies \ker f = \{e_G\}$

„⇐“ $f(x) = f(y) \overset{\cdot f(y)^{-1}}{\implies} f(x)f(y)^{-1} = f(xy^{-1}) = e_H \implies xy^{-1} = e_G \iff x = y \implies$ f injektiv. ■

Satz 3, § 1 (*Homomorphiesatz*)

G, H Gruppen, $f\colon G \to H$ Homomorphismus. $\implies f(G) < H, \quad f(G) \cong G/_{\ker f}$

Beweis:

$$\tilde{a},\tilde{b} \in f(G) \implies \exists a,b \in G: \quad f(a) = \tilde{a}, f(b) = \tilde{b} \tag{I.2}$$

$$\tilde{a}\tilde{b} = f(a)f(b) = f(ab) \implies \tilde{a}\tilde{b} \in f(G) \tag{I.3}$$

$$\tilde{a} \in f(G) \implies \exists a: \quad f(a) = \tilde{a} \implies f(a^{-1}) = \tilde{a}^{-1} \tag{I.4}$$

$$\implies \tilde{a}^{-1} \in f(G) \quad \text{Damit } f(G) < H \tag{I.5}$$

$$\implies \bar{f}\colon \bar{G} \to f(G), \quad \bar{a} \mapsto f(a) \text{ wohldef.} \tag{I.6}$$

$$\text{bijektiv (Satz 1.1) mit } \bar{f}(\bar{a}\bar{b}) = \bar{f}(\overline{ab}) = f(ab) = f(a)f(b) \tag{I.7}$$

$$= \bar{f}(\bar{a})\bar{f}(\bar{b}) \implies f \text{ ist Isomorphismus. } f\colon G/_{\ker f} \xrightarrow{\sim} f(G) \tag{I.8}$$

■

1.6. Permutationen

Definition 12, § 1

Sei M eine Menge. Eine bijektive Selbstabbildung $f\colon M \to M$ heißt ***Permutation*** *von M. $(S_M, \circ)$ Gruppe der Permutationen von M oder auch* ***symmetrische Gruppe****.*

Bemerkung 10, § 1

~~$g: M \to N$~~ sei Bijektion. Dann

Beweis: Sei $f \in S_M \implies \tilde{f}: N \to N, \quad b \mapsto \tilde{f}(b) := g \circ f \circ g^{-1}(b) \implies g \circ f \circ g^{-1}$ ist bijektiv, $\tilde{f} \in S_M$ und $S_M \to S_N, f \mapsto \tilde{f}$ ist ein Isomorphismus.

Homomorphie :

$$\tilde{f_1} \circ \tilde{f_2} = g \circ f_1 \circ g^{-1} \circ g \circ f_2 \circ g^{-1} \tag{I.9}$$
$$= g \circ f_1 \circ f_2 \circ g^{-1} \tag{I.10}$$
$$= \widetilde{f_1 \circ f_2} \tag{I.11}$$

Surjektivität Sei $h: N \to N \in S_N$. Sei $f = g^{-1} \circ h \circ g$ bijektive Abbildung auf N. $\tilde{f} = g \circ g^{-1} \circ h \circ g \circ g^{-1} = h$

Inkjektivität $g \circ f \circ g^{-1} = \mathrm{id}_N \implies f = g^{-1} \circ \mathrm{id}_N \circ g = \mathrm{id}_M \implies \ker(\sim) = \{\mathrm{id}_M\} \iff \sim$ injektiv ■

Schreibweisen M endliche Menge $M = \{1, 2, 3, \ldots, n\} \subset \mathbb{R}$. $f \in S_M = S_n$.

Permutationsschreibweise

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix} \tag{I.12}$$

Zyklenschreibweise

$$(1, f(1), f(f(1)), \ldots, f^{-1}(1)) \circ (m, f(m), f^2(m), \ldots, f^{-1}(m)) \circ \ldots \quad m \notin \{1, f(1), \ldots f^{-1}(1)\} \tag{I.13}$$

Beispiel 8, § 1

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\} \tag{I.14}$$
$$\equiv \big\{\mathrm{id}, (2,3), (1,3), (1,2), (1,2,3), (1,3,2)\big\} \tag{I.15}$$

Bemerkung 11, § 1

1. *$n \in \mathbb{N}$. S_n besitzt $n!$ Elemente.*
$$\#S_n = n!$$
2. *Jedes Element aus S_n lässt sich als Produkt von Transpositionen $t = (k, l), k \neq l$ schreiben.*

Beweis: 1. klar

2. Zerlege Zyklen in Produkt von Transpositionen, $(\dots, m, n, k, \dots) = (\dots, m, n) \circ (n, k, \dots)$ ■

Satz 4, § 1

Die Abbildung ***Signum*** $\operatorname{sign}\colon (S_N, \circ) \to (\mathbb{R}^*, \cdot)$

$$f \mapsto \prod_{1 \leqslant i < j \leqslant n} \frac{f(j) - f(i)}{j - i} \tag{I.16}$$

ist Homomorphismus von S_N *auf* $\{-1, 1\}$ *und* $\operatorname{sign}(t) = -1$ *für Transpositionen* $t = (k, l), k \neq l$.

Beweis: 1. $\operatorname{Bild}(\operatorname{sign}) = \{1, -1\}$, da mit (j, i) bzw. $(f(j), f(i))$ alle zwei-Elementigen Teilmengen von $\{1, \dots, n\}$ durchlaufen werden.

2. sign ist Homomorphismus:

$$\operatorname{sign}(f \circ g) \stackrel{!}{=} \operatorname{sign}(f) \cdot \operatorname{sign}(g) \tag{I.17}$$

$$\operatorname{sign}(f \circ g) = \prod_{i<j} \frac{f \circ g(j) - f \circ g(i)}{j - i} \tag{I.18}$$

$$= \prod_{i<j} \frac{f \circ g(j) - f \circ g(i)}{g(j) - g(i)} \cdot \prod_{i<j} \frac{g(j) - g(i)}{j - i} \tag{I.19}$$

$$= \prod_{i<j} \frac{f \circ g(j) - f \circ g(i)}{g(j) - g(i)} \cdot \operatorname{sign}(g) \tag{I.20}$$

$$= \prod_{\substack{i<j \\ g(i)<g(j)}} \frac{f \circ g(j) - f \circ g(i)}{g(j) - g(i)} \cdot \prod_{\substack{i<j \\ g(i)>g(j)}} \frac{f \circ g(j) - f \circ g(i)}{g(j) - g(i)} \cdot \operatorname{sign}(g) \tag{I.21}$$

$$= \prod_{\substack{i<j \\ g(i)<g(j)}} \frac{f \circ g(j) - f \circ g(i)}{g(j) - g(i)} \cdot \prod_{\substack{i<j \\ g(i)>g(j)}} \frac{f \circ g(i) - f \circ g(j)}{g(i) - g(j)} \cdot \operatorname{sign}(g) \tag{I.22}$$

$$\text{subst. } k = g(i), l = g(j) \tag{I.23}$$

$$= \prod_{k<l} \frac{f(k) - f(l)}{k - l} \cdot \operatorname{sign}(g) \tag{I.24}$$

$$= \operatorname{sign}(f) \cdot \operatorname{sign}(g) \tag{I.25}$$

3. $\operatorname{sign} t = -1$ für $t = (1, 2) : t = (k, l), (k, l) \neq (1, 2)$.

$$f = \begin{pmatrix} 1 & 2 & 3 & k & l \\ k & l & 3 & 1 & 2 \end{pmatrix} \Longrightarrow \tag{I.26}$$

$$f^{-1} \circ t \circ f = (1, k) \circ (2, l) \circ (k, l) \circ (1, k) \circ (2, l) = (1, 2) \tag{I.27}$$

$$\Longrightarrow \operatorname{sign}(f^{-1} \circ t \circ f) = \operatorname{sign}(f^{-1}) \cdot \operatorname{sign}(t) \cdot \operatorname{sign}(f) \tag{I.28}$$

$$= \operatorname{sign}(t) = \operatorname{sign}(1, 2) = -1 \tag{I.29}$$

■

Definition 13, § 1

sign *heißt* ***Vorzeichen von*** S_n.

$$A_n := \ker \operatorname{sign} n = \{f \in S_n | \operatorname{sign} f = 1\} \tag{I.30}$$

heißt ***alternierende Gruppe***.

§ 2. Natürliche Zahlen

klar[1]: $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ mit Addition $+$.

Axiomatische Einführung (Peano) Ein Tupel $(N, 0, s)$ bestehend aus einer Menge $N, 0 \in N, s\colon N \to N$ heißt System natürlicher Zahlen[2] : $\Longleftrightarrow$

1. $0 \notin s(N)$
2. $s\colon N \to N$ ist injektiv
3. $M \subseteq N \wedge 0 \in M \wedge s(M) \subseteq M \implies M = N$

Beispiel 1, § 2

$\mathbb{N} = (N, 0, s)$ *System natürlicher Zahlen und sei* $f\colon N \to \tilde{N}$ *bijektiv* $\implies \tilde{\mathbb{N}} = (\tilde{N}, \tilde{0}, \tilde{s}), \sigma = f(0), \tilde{s} = f \circ s \circ f^{-1} \implies \tilde{N}$ *System natürlicher Zahlen, zum Beispiel* $\mathbb{N} = \{0, 1, 2, \dots\}$ *und* $\tilde{\mathbb{N}} = \{0, -1, -2, \dots\}, \tilde{0} = 0, \tilde{s}(n) = n - 1$.

Satz 1, § 2 (*Eindeutigkeit*)

$(\mathbb{N}, 0, s), (\tilde{\mathbb{N}}, \tilde{0}, \tilde{s})$ *seien gegebene Systeme natürlicher Zahlen. Dann gibt es genau eine bijektive Abbildung* $f\colon \mathbb{N} \to \tilde{N}$ *mit* $f(0) = \tilde{0}$ *und* $f \circ s = \tilde{s} \circ f$.

Satz 2, § 2 (*Addition*)

$\mathbb{N}$ *System natürlicher Zahlen* $\implies$ *es gibt eine eindeutig bestimmte Verknüpfung* $+\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N} \quad (m, n) \mapsto m + n$ *mit*

1. $\forall m \in \mathbb{N}: \quad m + 0 = m$
2. $\forall m \in \mathbb{N} \forall n \in \mathbb{N}: \quad m + s(n) = s(m + n)$

Diese Verknüpfung heißt Addition.

[1] Literaturempfehlung für exakte Einführung: Ebbinghaus: „Zahlen“

[2] $s\colon n \mapsto n + 1$

Satz 3, § 2 (*Grundregeln der Addition*)

$\mathbb{N}$ *System natürlicher Zahlen,* $l, m, n \in \mathbb{N}$*. Dann:*

1. $m + 0 = m$ *(Eins)*
2. $m + n = n + m$ *(kommutativ)*

3. $(l+m)+n = l+(m+n)$ *(assoziativ)*
4. $l+n = m+n \implies l = m$ *(Kürzungsregel)*
5. $m+n = 0 \implies m = 0 \wedge n = 0$

$\implies$ $(\mathbb{N}, +)$ *kommutative Halbgruppe mit neutralem Element* 0.

Satz 4, § 2

$\mathbb{N}$ *System natürlicher Zahlen. Dann existiert eine eindeutig bestimmte Verknüpfung* $\cdot : N \times N \to N, \quad (m,n) \mapsto m \cdot n$ *mit*

- $\forall m \in \mathbb{N} : m \cdot 0 = 0$
- $\forall m, n \in \mathbb{N} : m(n+1) = mn + m$ *wobei* $1 = s(0)$.

Satz 5, § 2 (*Grundregeln der Multiplikation*)

$\mathbb{N}$ *System natürlicher Zahlen,* $l, m, n \in \mathbb{N}$.

1. *Neutrales Element:* $m \cdot 1 = m$
2. *Kommutativität:* $m \cdot n = n \cdot m$
3. *Assoziativität:* $(l \cdot n) \cdot m = l \cdot (n \cdot m)$
4. *Nullteilerfreiheit:* $m \cdot n = 0 \implies m = 0 \vee n = 0$
5. *Kürzungsregel:* $n \neq 0 \wedge ln = mn \implies l = m$
6. *Distributivität:* $(l+m) \cdot n = ln + mn$

$(\mathbb{N}, \cdot)$ *ist Halbruppe mit neutralem Element* $1 = s(0)$.

§ 3. Vollständige Induktion

Bemerkung 1, § 3

Sei $A(n)$ *eine Aussage für* $n \in \mathbb{N}$. *Dann:*

$$A(0) \wedge (n \in N : A(n) \implies A(n+1)) \implies \forall n \in \mathbb{N} : A(n) \tag{I.31}$$

Beweis :

$$W_A := \{n \in \mathbb{N} | A(n)\} \subset \mathbb{N} \tag{I.32}$$
$$A(0) \iff 0 \in W_A \tag{I.33}$$
$$(A(n) \implies A(n+1)) \iff (n \in W_A \implies n+1 \in W_A) \tag{I.34}$$
$$\iff (n \in W_A \implies s(n) \in W_A) \tag{I.35}$$
$$\implies W_A = \mathbb{N} \tag{I.36}$$

■

Bemerkung 2, § 3

$\mathbb{N}$ *System natürlicher Zahlen* $\implies \forall n \in \mathbb{N} : n \neq n+1$

Beweis : Durch vollständige Induktion: $A(n) : n \neq n+1$

Induktionsanfang: $A(0)$: (Peano 1) $\implies 0 \notin s(\mathbb{N}) \implies s(0) \neq 0$

Induktionsschluss: $A(n) \implies A(n+1)$

$$n \neq n+1 \implies n+1 = s(n) \neq s(n+1) = (n+1)+1 \tag{I.37}$$
$$\implies A(n+1) \implies A(n) \text{ gilt } \forall n \in \mathbb{N} \tag{I.38}$$

■

Definition 1, § 3

$m, n \in \mathbb{N}$. Dann heißt m ***kleinergleich*** *$m \leqslant n :\iff \exists a \in \mathbb{N} : m + a = n$. a heißt* ***Differenz*** *von m und n: $a =: n - m$.*
(a ist eindeutig wegen der Kürzungsregel: $m + a' = n = m + a \implies a = a'$.)

Bemerkung 3, § 3

1. $\forall n \in \mathbb{N} : 0 \leqslant n$
2. $\forall n \in \mathbb{N}, n \neq 0 : 1 \leqslant n$

Beweis : 1. $n + 0 = n$

2. $A(n) : n = 0 \vee 1 \leqslant n$

   Induktionsanfang: $A(0)$

   Induktionsschluss: $A(n) \implies A(n+1)$

$$A(n) : n = 0 \vee 1 \leqslant n \implies n+1 = 0 \vee 1 \leqslant n+1 \implies A(n+1)$$

■

Satz 1, § 3 (*Grundregeln für Ordnung*)

Die Relation $\leqslant$ ist auf $\mathbb{N}$ eine Totalordnung mit den Eigenschaften

1. $\forall l, m, n \in \mathbb{N} : l \leqslant m \implies l + n \leqslant m + n$

2. $l \leqslant m \implies ln \leqslant mn$

Beweis: **reflexiv** $m \leqslant m : m + 0 = m$

transitiv $m \leqslant n, n \leqslant l, \implies m \leqslant l$

$$m + a = n, n + b = l \implies m + (a + b) = n + b = l \implies m \leqslant l$$

antisymmetrisch

$$\begin{aligned} m \leqslant n, \quad & n \leqslant m && \implies n = m && \text{(I.39)} \\ m + a = n, \quad & n + b = m && \implies n + b + a = n \implies b + a = 0 && \text{(I.40)} \\ & && \implies a = b = 0 \implies n = m && \text{(I.41)} \end{aligned}$$

Totalordnung $A(n) : m \leqslant n \vee n \leqslant m$

Induktionsanfang: $m \leqslant 0 \vee 0 \leqslant m \implies A(0)$

Induktionsschluss: 2 Fälle:

- $$\begin{aligned} m \leqslant n &\implies \exists a \in \mathbb{N} : m + a = n && \text{(I.42)} \\ &\implies (m + a) + 1 = n + 1 && \text{(I.43)} \\ &\implies m \leqslant n + 1 && \text{(I.44)} \end{aligned}$$

- $$\begin{aligned} n \leqslant m &\implies \exists a \in \mathbb{N} : n + a = m && \text{(I.45)} \\ \text{Wenn } a = 0 &\implies m \leqslant n && \text{(I.46)} \\ \text{Wenn } a \neq 0 &\implies a \geqslant 1 \implies \exists b \in \mathbb{N} : 1 + b = a && \text{(I.47)} \\ &\implies n + (1 + b) = m \implies (n + 1) + b = m && \text{(I.48)} \\ &\implies n + 1 \leqslant m \implies A(n + 1) && \text{(I.49)} \end{aligned}$$

Behauptung 1 $l \leqslant m \implies \exists a \in \mathbb{N} : l + a = m \implies (l + a) + n = m + n \implies l + n \leqslant m + n$

Behauptung 2 $(l + a)n = ln + an \implies ln \leqslant mn$ ■

Bemerkung 4, § 3

Es sei $A(n)$ eine Aussage für $n \in \mathbb{N}$, $m \leqslant n$.

$$\begin{aligned} & A(0) \wedge (\forall m \in \mathbb{N} : A(m) \implies A(n + 1)) && \text{(I.50)} \\ & \implies \forall n \in \mathbb{N} : A(n) && \text{(I.51)} \end{aligned}$$

Beweis :

$$A^*(m) : [\forall m \leqslant n : A(m)] \tag{I.52}$$
$$\text{Induktionsanfang: } A^*(0) = A(0) \tag{I.53}$$
$$\text{Induktionsschluss: } A^*(m) \implies A^*(m+1) : \forall m \leqslant n : A(m) \implies A(n+1) \tag{I.54}$$
$$\implies \forall m \leqslant n+1 : A(m) \implies A^*(m+1) \leqslant \forall n \in \mathbb{N} : A^*(m) \tag{I.55}$$
$$\implies \forall n \in \mathbb{N} : A(m) \tag{I.56}$$

■

Satz 2, § 3

Jede nichtleere Teilmenge $M \subseteq \mathbb{N}$ besitzt ein kleinstes Element, d.h. $\exists m \in M : \forall n \in M : m \leqslant n$.

Beweis : Sei $A(n) : n \in M \implies M$ besitzt ein kleinstes Element.

Induktionsanfang: $A(0)$: Sei $0 \in M \implies \forall m \in M : 0 \leqslant m$ (Achtung: Aussage auch wahr, wenn $n \notin M$, da aus einer falsche Aussage immer eine wahre folgt!)

Induktionsschluss: $A(n) \implies A(n+1)$: Sei $n+1 \in M$ und $A(m)$ sei wahr für $m \leqslant n$. Zwei Fälle:

- $\exists m \in M : m \leqslant n \implies A(m) \implies M$ besitzt kleinstes Element
- Falls $\forall m \in M : n+1 \leqslant m \implies n+1$ kleinstes Element $\implies A(n+1)$.

■

§ 4. Ganze Zahlen und Restklassenringe

4.1. Konstruktion ganzer Zahlen

Konstruktion aus $\mathbb{N} : \mathbb{N} \times \mathbb{N} = M$

$$((m,r),(n,s)) \in R : \iff m + s = n + r \tag{I.57}$$

ist Äquivalenzrelation.
$Z = M/_R$: Quotientenmenge mit

$$(\overline{m,r}) =: m - r$$

Definition 1, § 4

*Eine Menge R mit zwei Verknüpfungen $(R,+,\cdot)$ heißt (kommutativer) **Ring** mit Eins $\iff$*

1. *$(R,+)$ ist eine kommutative Gruppe mit neutralem Element 0_R*
2. *$(R,\cdot)$ ist eine kommutative Halbgruppe mit neutralem Element 1_R*
3. *$\forall x,y,z \in R : x(y+z) = xy + xz$ und $(x+y)z = xz + yz$*

Ein bezüglich $\cdot$ nullteilerfreier kommutativer Ring heißt Integritätsbereich.
*Ein kommutativer Ring heißt **Körper**, falls $1 \neq 0$ und $(R\backslash\{0\},\cdot)$ eine Gruppe ist.*

Satz 1, § 4

1. *Auf $\mathbb{N} \times \mathbb{N}$ wird durch $(m,r) \sim (n,s) :\iff m+s = n+r$ eine Äquivalenzrelation definiert.*

2. *Die Quotientenmenge $\mathbb{Z} = \mathbb{N} \times \mathbb{N}/_\sim$ mit den Abbildungen*

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, (\overline{m,r}) + (\overline{n,s}) := (\overline{m+n, r+s}) \tag{I.58}$$
$$\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, (\overline{m,r}) \cdot (\overline{n,s}) := (\overline{mn+rs, ms+nr}) \tag{I.59}$$
$$\tag{I.60}$$

   bildet einen Integritätsbereich.

3. *Auf $\mathbb{Z}$ wird durch $(\overline{m,r}) \leqslant (\overline{n,s}) :\iff m+s \leqslant n+r$ eine Totalordnung auf Z definiert mit:*

$$(\overline{m,r}) \leqslant (\overline{n,s}) \implies \forall (\overline{l,q}) \in \mathbb{Z} \tag{I.61}$$
$$(\overline{m,r}) + (\overline{l,q}) \leqslant (\overline{n,s}) + (\overline{l,q}) \tag{I.62}$$
$$(\overline{m,r}) \cdot (\overline{l,q}) \leqslant (\overline{n,s}) \cdot (\overline{l,q}) \tag{I.63}$$

4. *Es gibt eine injektive Abbildung $j_\mathbb{N} \colon \mathbb{N} \to \mathbb{Z}$ mit*

$$j_\mathbb{N}(x+y) = j_\mathbb{N}(x) + j_\mathbb{N}(y), \quad j_\mathbb{N}(xy) = j_\mathbb{N}(x) \cdot j_\mathbb{N}(y) \tag{I.64}$$

Beweis: 1. **reflexiv** $(m,r) \sim (m,r) \iff m+r = m+r$

symmetrisch $((m,r) \sim (n,s) \iff (n,s) \sim (m,r)) \iff (m+s = m+r \iff m+r = m+s)$

transitiv

$$(m,r) \sim (n,s) \wedge (n,s) \sim (o,t) \implies (m,r) \sim (o,t) \tag{I.65}$$
$$m+s = m+r \wedge n+t = s+o \iff m+t+s = n+r+t = o+s = r \tag{I.66}$$
$$\implies m+t = o+r \tag{I.67}$$

2. „+“ ist vetreterunabhängig, das heißt:

$$(\overline{m',r'}) = (\overline{m,r}) \wedge (\overline{n',s'}) = (\overline{n,s}) \tag{I.68}$$
$$\implies m'+r = m+r' \wedge n'+s = n+s' \tag{I.69}$$
$$\implies (m'+n') + (r+s) = (m+n) + (r'+s') \tag{I.70}$$
$$\implies (\overline{m'+n', r'+s'}) = (\overline{m+n, r+s}) \tag{I.71}$$

(Multiplikation analog.)

Die Halbgruppenaxiome von $\mathbb{N}$ übertragen sich:

- $(\overline{0,0})$ ist neutrales Element von $+$

- $(\overline{1,0})$ ist neutrales Element von $\cdot$
- Ist $(\overline{m,r}) \in \mathbb{Z}$, so ist $\overline{r,m}$ das Inverse bezüglich $+$
- Nullteilerfreiheit:

$$(\overline{0,0}) = 0_{\mathbb{Z}} = (\overline{m,r}) \cdot (\overline{n,s}) = (\overline{mn+rs, ms+nr}) \tag{I.72}$$

$$\implies mn + rs = ms + nr \tag{I.73}$$

$$\implies \begin{cases} n \geqslant s: & \implies m(n-s) = r(n-s) \\ n \leqslant s: & \implies m(s-n) = r(s-n) \end{cases} \tag{I.74}$$

$$\implies n = s \vee m = r \implies (\overline{r,m}) = (\overline{0,0}) \implies (\overline{n,s}) = 0 \tag{I.75}$$

3. Übungsaufgabe
4. $j_{\mathbb{N}} \colon \mathbb{N} \to \mathbb{Z}, n \mapsto (\overline{n,0})$ hat alle gewünschten Eigenschaften. ■

4.2. Teilbarkeitsrelation

Definition 2, § 4

*$y \in \mathbb{Z}$ heißt **Teiler** von $x \in \mathbb{Z} : \iff \exists q \in \mathbb{Z} : yq = z$. Man schreibt $y|x$.*
*$p \in \mathbb{N}\backslash\{0,1\}$ heißt **Primzahl** : $\iff \forall y \in \mathbb{N}\backslash\{0,1\} : y|p \rightsquigarrow y = p$. Die Menge aller Primzahlen heißt $\mathbb{P}$.*

Bemerkung 1, § 4

Die Teilbarkeit ist eine reflexive und transitive Relation auf $\mathbb{Z}$ mit:

1. $y|x \wedge x|y \implies x = y \vee x = -y$
2. $z|x \wedge z|y \implies z|(x+y), z|(x-y)$

Beweis : $R = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} | x|y\}$ ist reflexiv, da $x = 1 \cdot x$ und transitiv da:

$$y|x \wedge z|y \implies \exists r,q \in \mathbb{Z} : y \cdot r = x \wedge z \cdot q = y \implies x = (qr)z \implies z|x \tag{I.76}$$

1. ohne Einschränkung: $x \neq 0$ (sonst: $\implies y = 0$)

$$\implies \exists q,r \in \mathbb{Z} : x = qy, y = rx \implies 1x = (qr)x \tag{I.77}$$

$$\implies qr = 1 \quad (\implies q = r = 1 \vee q = r = -1) \tag{I.78}$$

$$\implies \text{falls } q,r \in \mathbb{N} : \text{ Angenommen, } r \geqslant 2, q \geqslant 1 \tag{I.79}$$

$$\implies 1 + a = q \quad \forall a \in \mathbb{N} \tag{I.80}$$

$$\implies \underbrace{(1+a) + \cdots + (1+a)}_{r \text{ mal}} = 1 \implies a + \cdots + (1+a) = 0 \tag{I.81}$$

$$\implies a = 0 \wedge 1 + a = 0 \implies 1 = 0 \lightning \tag{I.82}$$

2. $x = qz, y = rz \implies x + y = (q+r)z \wedge x - y = (q-r)z$ ■

Folgerung 1, § 4

Teilbarkeit ist eine Ordnungsrelation auf N eingeschränkt (folgt aus Bemerkung 1, § 4.1).

Satz 2, § 4 (*Euklid*)

Es gibt unendlich viele Primzahlen.

Beweis: $2 = 1 + 1 \in \mathbb{P} \quad (y \geqslant 2 \wedge yq = 2 \implies y = 2) \implies \mathbb{P} \neq \varnothing$

Angenommen, $\mathbb{P}$ wäre endlich: $\mathbb{P} = \{p_1, \ldots, p_n\}$

$$q := p_1 \cdots p_n + 1 \in \mathbb{N} \tag{I.83}$$
$$M := \{m \in \mathbb{N}\backslash\{0,1\} | m|q\} \tag{I.84}$$
$$\implies M \neq \varnothing \implies M \text{ besitzt kleinstes Element } m \text{ mit } m \geqslant 2 \tag{I.85}$$
$$\forall r \in \mathbb{N}\backslash\{0,1\} : r|m \implies r|q \implies m \leqslant r : \exists s \in \mathbb{Z} : rs = m \tag{I.86}$$
$$\overset{m\geqslant 2}{\implies} 1 \leqslant s \implies r \leqslant rs = m \implies m = r \tag{I.87}$$
$$\implies m \in \mathbb{P}, m|q, m|p_1 \cdots p_n \tag{I.88}$$
$$\implies m|(q - p_1 \cdots p_n) \tag{I.89}$$
$$\implies m|1 \implies m \leqslant 1 \lightning \tag{I.90}$$

■

4.3. Restklassenringe

Bemerkung 2, § 4 (*Division mit Rest*)

Zu $x, y \in \mathbb{Z}, y \geqslant 1$ gibt es eindeutig bestimmte $r, q \in \mathbb{Z} : x = yq + r$ und $0 \leqslant r < y \quad (r < y \iff r \leqslant y - 1)$.

Beweis: Existenz $M = \{x - zy | z \in \mathbb{Z}\} \cap \mathbb{N} \neq \varnothing \implies M$ hat kleinstes Element $r \implies 0 \leqslant r < y$ (sonst: $r' = r - y$) $\implies \exists q \in \mathbb{Z} : r = x - qy$

Eindeutigkeit Seien $\tilde{q}, \tilde{r} \in \mathbb{Z}$ mit $x = \tilde{q} \cdot y + r, 0 \leqslant \tilde{r} < y \implies (q - \tilde{q}) \cdot y = \tilde{r} - r$.

1. Fall: $q = \tilde{q} \implies r = \tilde{r}$

2. Fall: $q - \tilde{q} \neq 0 \implies y|\tilde{r} - r \wedge -y < \tilde{r} - r < y \implies r = \tilde{r} \overset{y\neq 0}{\implies} q - \tilde{q} = 0 \lightning \implies$ 1. Fall gilt.

■

Definition 3, § 4

*$d \in \mathbb{N}$ heißt **größter gemeinsamer Teiler** von $x, y \in \mathbb{Z}$.*

$$d = \mathrm{ggT}(x, y) : \iff d|x \wedge d|y \wedge (t : t|x \wedge t|y \implies t|d) \tag{I.91}$$

Satz 3, § 4

1. *Je zwei Zahlen $(x, y) \neq (0, 0)$ besitzen einen ggT.*

2. $d = \mathrm{ggT}(x,y) \implies \exists u,v \in \mathbb{Z} : d = ux + vy$

Beweis: $M = \{ax + by | a,b \in \mathbb{Z}\}, M^* = M \cap \mathbb{N}\backslash\{0\} \neq \varnothing \implies M^*$ hat kleinstes Element d.

$$\implies \exists u,v \in \mathbb{Z} : d = ux + vy. \tag{I.92}$$

$$\text{Sei } z \in M \implies \exists q,r \in \mathbb{Z}, z = qd + r \implies r \in M \implies r = 0 \quad (0 \leqslant r < d) \tag{I.93}$$

$$\implies \forall z \in M : d|z \implies d|x, d|y \implies d \text{ gemeinsamer Teiler} \tag{I.94}$$

Sei $t \in \mathbb{Z}, t|x, t|y \implies \forall z \in M : t|z \implies t|d \implies d = \mathrm{ggT}(x,y)$. Ist d' ein anderer ggT $\implies d'|d \wedge d|d' \implies d = d'$ ∎

Definition 4, § 4

$n \in \mathbb{N}, x, y \in \mathbb{Z}$ heißen ***kongruent modulo n***

$$x \equiv y \mod n :\iff n|(x-y) \tag{I.95}$$

Satz 4, § 4

a) Die Kongruenzrelation auf $\mathbb{Z}$ ist Äquivalenzrelation.

b) Die Quotientenmengen $\mathbb{Z}/_{n\mathbb{Z}} := \mathbb{Z}/_{\equiv}$ zusammen mit den Verknüpfungen

$$+ : \mathbb{Z}/_{n\mathbb{Z}} \times \mathbb{Z}/_{n\mathbb{Z}} \implies \mathbb{Z}/_{n\mathbb{Z}}, \quad (\bar{x}, \bar{y}) \mapsto \bar{x} + \bar{y} := \overline{x+y} \tag{I.96}$$

$$\cdot : \mathbb{Z}/_{n\mathbb{Z}} \times \mathbb{Z}/_{n\mathbb{Z}} \implies \mathbb{Z}/_{n\mathbb{Z}}, \quad (\bar{x}, \bar{y}) \mapsto \bar{x} \cdot \bar{y} := \overline{xy} \tag{I.97}$$

bilden einen kommutativen Ring.

c) $Z/_{n\mathbb{Z}}$ ist ein Körper $\iff n \in \mathbb{P}$.

Beweis: a)

$$\bar{x} = \{\ldots, x-2n, x-n, x, x+n, x+2n, \ldots\} \tag{I.98}$$

$$y \equiv x \pmod n \iff n|y-x \tag{I.99}$$

$$\iff \exists a \in \mathbb{Z} : na = y - x \tag{I.100}$$

$$\iff y = x + na \tag{I.101}$$

reflexiv $x \equiv x \pmod n$

symmetrisch $y \equiv x \pmod n \iff n|y-x \iff \exists a : an = y - x \iff -an = x - y \iff n|(x-y) \iff x \equiv y \pmod n$

transitiv $x \equiv y \pmod n, y \equiv x \pmod n \iff \exists a,b \in \mathbb{Z} : x - y = an, y - z = bn \implies x - z - bn = an \iff x - z = (a+b)n \iff n|x-z \iff x \equiv z \pmod n$

b) Nur zu zeigen: $+$ und $\cdot$ sind vertreterunabhängig, dann übertragen sich die Ringeigenschaften von $\mathbb{Z}$ auf $\mathbb{Z}/_{n\mathbb{Z}}$, d.h.

$$x \equiv x' \pmod{n}, y \equiv y' \pmod{n} \tag{I.102}$$
$$\iff \exists a, b \in \mathbb{Z} : x - x' = an, y - y' = bn \tag{I.103}$$
$$\implies x + y = y' + an + y' + bn = x' + y' + (a+b)n \tag{I.104}$$
$$\iff \bar{x} + \bar{y} \equiv \bar{x}' + \bar{y}' \pmod{n} \tag{I.105}$$
$$xy = x'y' + x'bn + any' + abnn \tag{I.106}$$
$$= x'y' + (x'b + ay' + abn)n \iff \bar{x}\bar{y} \equiv \bar{x}'\bar{y}' \pmod{n} \tag{I.107}$$

c) Sei $n = p \in \mathbb{P}$. Sei $\bar{x} \neq \bar{0}, \bar{x} \in \mathbb{Z}_{p\mathbb{Z}}, x \in Z$.

$$\implies p + x \implies \mathrm{ggT}(x, p) = 1 \tag{I.108}$$
$$\implies \exists u, v \in \mathbb{Z} : 1 = ux + vp \implies \bar{1} = \bar{u}\bar{x} \pmod{p} \tag{I.109}$$

$\implies \bar{u}$ ist Inversers zu $\bar{x}$ in $\mathbb{Z}/_{pZ}$ $\implies$ Körper.

Umgekehrt: Sei $n \notin \mathbb{P} \implies \exists r, s \in \mathbb{N} : n = rs, 1 < r, s < n \implies F \not\equiv \bar{0} \pmod{n}$. Angemommen, $\mathbb{Z}/_{n\mathbb{Z}}$ wäre Körper $\implies \exists a \in \mathbb{Z} : \bar{a}\bar{s} = \bar{1} \implies \bar{0} \not\equiv \bar{r} \equiv \bar{r}\bar{1} \equiv \bar{r}\bar{s}\bar{a} \equiv \bar{n}\bar{a} \equiv \bar{0}\bar{a} \equiv \bar{0} \pmod{n}$ ↯. ■

§ 5. Rationale und reelle Zahlen

5.1. Konstruktion rationaler Zahlen

Wissen: $(\mathbb{Z}, +, \cdot)$ ist Integritätsbereich.
Frage: Was ist das Inverse bezüglich $\cdot$ in $\mathbb{Z}$?

Satz 1, § 5

a) Auf $\mathbb{Z} \times (\mathbb{Z}\backslash\{0\})$ ist durch $(x, u) \sim (y, v) : \iff xv = yu$ eine Äquivalenzrelation definiert. Man schreibt:

$$\frac{x}{u} := (\overline{x, u}) \tag{I.110}$$

b) Die Quotientenmenge $\mathbb{Q} := \mathbb{Z} \times (\mathbb{Z}\backslash\{0\})/_{\sim}$ zusammen mit

$$+ : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}, ((\overline{x, u}), (\overline{y, v})) \mapsto (\overline{x, u}) + (\overline{y, v}) := (\overline{xv + yu, uv}) \tag{I.111}$$
$$\cdot : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}, ((\overline{x, u}), (\overline{y, v})) \mapsto (\overline{x, u}) \cdot (\overline{y, v}) := (\overline{xy, uv}) \tag{I.112}$$

bildet einen Körper.

c) Es gibt eine injektive Abbildung $j_{\mathbb{Z}} : \mathbb{Z} \to \mathbb{Q}, z \mapsto (\overline{z, 1})$ mit $j_{\mathbb{Z}}(x) + j_{\mathbb{Z}}(y) = j_{\mathbb{Z}}(x + y), j_{\mathbb{Z}}(x) \cdot j_{\mathbb{Z}}(y) = j_{\mathbb{Z}}(xy)$

Beweis : a) Reflexivität und Symmetrie sind trivial. Transitivität:

Sei $(\overline{x,u}) \sim (\overline{y,v}), (\overline{y,v}) \sim (\overline{z,w}) \implies xv = yu, yw = zv \implies xvw = yuw = zvu \implies xw = zu \iff (\overline{x,u}) \sim (\overline{z,w})$

b) zu zeigen: $(x',u') \sim (x,u), (y',v') \sim (y,v) \implies (x'v' + y'u', u'v') \sim /xv + yu, uv)$

Gruppenaxiome: $(\overline{x,u}) + (\overline{y,v}) = (\overline{xv + yu, uv}) = (\overline{y,v}) + (\overline{x,u}) \implies$ kommutativ. Assoziativität analog.

Neutrales Element bezüglich Addition: $(\overline{0,1}) : (\overline{x,u}) + (\overline{0,1}) = (\overline{x \cdot 1 + u \cdot 0, u \cdot 1}) = (\overline{x,u})$

Inverses bzgl. Addition: Sei $(\overline{x,u}) \in \mathbb{Q}$. Dann ist $(\overline{-x,u})$ das Inverse: $(\overline{x,u}) + (\overline{-x,u}) = (\overline{0,u}) = (\overline{0,1})$

Neutrales Element bzgl. Multiplikation: $(\overline{1,1}) : (\overline{x,u})(\overline{1,1}) = (\overline{x \cdot 1, u \cdot 1}) = (\overline{x,u})$

Inverses bzgl. Multiplikation: Sei $(\overline{x,u}) \in \mathbb{Q} \implies (\overline{u,x}), x \neq 0$. Denn: $(\overline{x,u})(\overline{u,x}) = (\overline{xu, xu}) = (\overline{1,1})$

Distributivität: Übung!

c)

$$j_{\mathbb{Z}}(x) + j_{\mathbb{Z}}(y) = (\overline{x,1}) + (\overline{y,1}) = (\overline{x+y,1}) = j_{\mathbb{Z}}(x+y) \tag{I.113}$$

$$j_{\mathbb{Z}}(x) \cdot j_{\mathbb{Z}}(y) = (\overline{x,1}) \cdot (\overline{y,1}) = (\overline{xy,1}) = j_{\mathbb{Z}}(xy) \tag{I.114}$$

Injektivität ist klar.

Zusatz 1

$$\frac{x}{u} \in \mathbb{Q} \implies \exists (y,z) \in \mathbb{Z} \times (\mathbb{N}\backslash\{0\}) : \quad \frac{x}{u} = \frac{y}{z} \tag{I.115}$$

(da $\frac{1}{-1} = \frac{-1}{1}$) ■

5.2. Natürliche Ordnung und Betrag rationaler Zahlen

Satz 2, § 5

a) Auf $\mathbb{Q}$ wird durch

$$\frac{x}{u} \leqslant \frac{y}{v} : \iff xv \leqslant_{\mathbb{Z}} yu$$

wobei $u, v \in \mathbb{N}\backslash\{0\}$, eine Totalordnung definiert mit

$$j_{\mathbb{Z}}(x) \leqslant j_{\mathbb{Z}}(y) \iff x \leqslant_{\mathbb{Z}} y, \quad x, y \in \mathbb{Z}$$

b) $\forall r \leqslant s \in \mathbb{Q}$ gilt:

$\forall t \in \mathbb{Q} : r + t \leqslant s + t$

$\forall t \in \mathbb{Q}, t \geqslant 0, r \cdot t \leqslant s \cdot t$

Beweis: a) Falls $\frac{x}{u} = \frac{x'}{u'}, \frac{y}{v} = \frac{y'}{v'} \overset{xv \leqslant yu}{\Longrightarrow} xvu'v' \leqslant_{\mathbb{Z}} yuu'v' \iff x'uvv' \leqslant_{\mathbb{Z}} y'vuu' \iff x'v' \leqslant y'u' \iff \frac{x'}{u'} \leqslant \frac{y'}{v'} \Longrightarrow \leqslant$ ist wohldefiniert auf $\mathbb{Q}$.

Totalordnung.: Reflexivität, Transitivität und Antisymmetrie klar und $\frac{x}{u} \leqslant \frac{y}{v} \vee \frac{y}{v} \leqslant \frac{x}{u}$ gilt auch, da $\leqslant_{\mathbb{Z}}$ Totalordnung ist und $x \leqslant_{\mathbb{Z}} y \iff x \cdot 1 \leqslant_{\mathbb{Z}} y \cdot 1 \iff \frac{x}{1} \leqslant \frac{y}{1} \iff j_{\mathbb{Z}}(x) \leqslant j_{\mathbb{Z}}(y)$

b) $r = \frac{x}{u}, s = \frac{y}{v} \iff xv \leqslant_{\mathbb{Z}} yu$. Sei $t \in \mathbb{Q}, t = \frac{z}{w}$

$$\frac{x}{u} + \frac{z}{w} = \frac{(xw + zu)v}{uwv} \leqslant \frac{u(yw + zy)}{uvw} = \frac{y}{v} + \frac{z}{w}$$

Sei $t \geqslant 0, t = \frac{z}{w}$.

$$\frac{x}{u} \cdot \frac{z}{-} \frac{xzv}{uvw} \leqslant \frac{yuz}{uvw} = \frac{y}{v}\frac{z}{w}$$

mit Satz 1, § 5c. ∎

Definition 1, § 5

Die Relation $\leqslant$ heißt kleinergleich. Falls $r \in \mathbb{Q}$ heißt

$$|r| := \begin{cases} r & \text{falls } r \geqslant 0 \\ -r & \text{falls } r \leqslant 0 \end{cases} \tag{I.116}$$

***Absolutbetrag** auf $\mathbb{Q}$.*

Satz 3, § 5 (*Regeln für den Betrag*)

Sei $r, s \in \mathbb{Q}$.

a) $|r| \geqslant 0$ *und* $|r| = 0 \iff r = 0$

b) $|rs| = |r| \cdot |s|$

c) $|r + s| \leqslant |r| + |s|$

d) $\exists n \in \mathbb{N} : |n| > 1$

Beweis: a) klar

b) Per Fallunterscheidung, z.B. für $r \geqslant 0, s \leqslant 0$:

$$|r| \cdot |s| r \cdot (-s) = (-1) \cdot r \cdot s = |rs|$$

da $rs \leqslant 0$ (mit Satz 2, § 5b). Andere Fälle analog.

c)

$$r \leqslant |r|, s \leqslant |s| \implies r + s \leqslant |r| + |s| \tag{I.117}$$

$$-r \leqslant |-r|, -s \leqslant |-s| \implies -(r + s) \leqslant |r| + |s| \tag{I.118}$$

$$\implies |r + s| \leqslant |r| + |s| \tag{I.119}$$

mit $|-r| = |(-1)r| = |-1||r| = 1|r| = |r|$.

d) $|2| = 2 > 1$. ■

5.3. Körper der reellen und komplexen Zahlen

Intuitiv: $x \in \mathbb{R}, x = 3.141692\ldots$

Folgen $x = (x_0, x_1, x_2, \ldots) = (x_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}} = \mathrm{Abb}(\mathbb{N}, \mathbb{Q})$

Die Menge $\mathbb{R}$

$$\mathbb{R} := \left\{x = (x_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}} | x \text{ ist Cauchyfolge } \right\} /_\sim \tag{I.120}$$
$$+ \text{ mit } (x_n)_{n\in\mathbb{N}} + (y_n)_{n\in\mathbb{N}} = (x_n + y_n)_{n\in\mathbb{N}} \tag{I.121}$$
$$\cdot \text{ mit } (x_n)_{n\in\mathbb{N}} \cdot (y_n)_{n\in\mathbb{N}} = (x_n \cdot y_n)_{n\in\mathbb{N}} \tag{I.122}$$
$$\tag{I.123}$$

Cauchy-Folge $x \in \mathbb{Q}^{\mathbb{N}}$ ist eine Cauchy-Folge : $\Longleftrightarrow$

$$\forall \epsilon \in \mathbb{Q}, \epsilon > 0 \quad \exists N \in \mathbb{N} : \forall k, l \in \mathbb{N}, k, l \geqslant N : |x_k - y_l| < \epsilon \tag{I.124}$$

Wir definieren eine Relation $\sim$:

$$(x_n)_{n\in\mathbb{N}} \sim (y_n)_{n\in\mathbb{N}} : \Longleftrightarrow \ (x_n) - (y_n) \text{ ist eine Nullfolge} \tag{I.125}$$

(das bedeutet: $\forall \epsilon \in \mathbb{Q}, \epsilon > 0 \quad \exists N \in \mathbb{N} : \forall k \geqslant N : |x_k - y_k| < \epsilon$)
Zusatzaufgabe (schwierig!): R ist ein Körper mit komponentenweise Addition und Multiplikation. $\exists$ eine injektive Abbildung $j_{\mathbb{Q}} \colon \mathbb{Q} \to \mathbb{R}$, die $+, \cdot$ erhält.
Zum weiterlesen: https://en.wikipedia.org/wiki/Construction_of_the_real_numbers

Komplexe Zahlen Der Körper $\mathbb{C}$ wird konstruiert aus $\mathbb{R}$ mittels $\mathbb{C} := \mathbb{R} \times \mathbb{R}$ mit

$$+ \colon \mathbb{C} \times \mathbb{C} \to \mathbb{C}, ((x,u),(y,v)) \quad \mapsto (x + y, u + v) \tag{I.126}$$
$$\cdot \colon \mathbb{C} \times \mathbb{C} \to \mathbb{C}, ((x,u),(y,v)) \quad \mapsto (xy - uv, xv + uy) \tag{I.127}$$

Dies ist dann ein Körper. Die Abbildung $j_{\mathbb{R}} \colon \mathbb{R} \to \mathbb{C}, x \mapsto (x, 0)$ ist injektiv und erhält $+$ und $\cdot$.

Schreibweise

$$i := (0,1) \in \mathbb{C} \implies (x,u) = (x,0) + i \cdot (0,u) = x + iu \tag{I.128}$$

Außerdem:

$$i^2 = (0,1) \cdot (0,1) = (-1,0) \tag{I.129}$$

5.4. Charakteristik eines Körpers

Schreibweise Sei $(K, +, \cdot)$ ein Körper, $a \in K$.

$$\sum_{i=1}^{n} a = a \cdot \sum_{i=1}^{n} 1_K = a \cdot n \cdot 1_K, n \cdot 1_K =: n_K \tag{I.130}$$

$$\prod_{i=1}^{n} a =: a^n \tag{I.131}$$

Definition 2, § 5

$K, +, \cdot$ *Körper,*

$$C = \{n \in \mathbb{N}^* | n \cdot 1_K = 0\}$$

Falls $C \neq \varnothing \implies$ *C hat kleinstes Element c. Die Charakteristik von K ist* $\operatorname{char}(K) = c$.
Falls $C = \varnothing \implies \operatorname{char}(K) = 0$.

Bemerkung 1, § 5

K *Körper* $\implies \operatorname{char}(K) \in \mathbb{P} \cup \{0\}$

Beweis : Sei $\operatorname{char}(K) \neq \varnothing \implies \exists c \in \mathbb{N}^* : \operatorname{char}(K) = c \implies c \cdot 1 - K = 0$ und c ist das kleinste c mit dieser Eigenschaft.

Angenommen, $c \notin \mathbb{P} \implies \exists d, t \in \mathbb{N} : dt = c$ und $1 < d, t < c \implies (d \cdot 1_K) \cdot (t \cdot 1_K) = (c \cdot 1_K) = 0 \implies K$ enthält Nullteiler $\lightning$. (Vgl. Beweis Satz 4c, §4) ■

Beispiel 1, § 5

$\operatorname{char}(\mathbb{Q}) = 0, \operatorname{char}(\mathbb{F}_p) = p$.

II. Vektorräume

§ 6. Einführung

6.1. Begriff des Vektorraums

Definition 1, § 6

Sei $(K, +, \cdot)$ Körper. Ein Tripel $(V, +, \cdot)$ bestehend azs einer Menge $V \neq \varnothing$, die bezüglich $+$ eine abelsche Gruppe ist und bezüglich der sogenannten Skalaren Multiplikation

$$K \times V \to V, (a, v) \mapsto a \cdot v$$

die Eigenschaften ($a, b \in K, v, w \in V$)

(SM1) $a \cdot (v + w) = a \cdot v + a \cdot w$

(SM2) $(a + b) \cdot v = a \cdot v + b \cdot v$

(SM3) $a \cdot (b \cdot v) = (a \cdot b) \cdot v$

(SM4) $1_K \cdot v = v$

*hat, so nennt man V einen **Vektorraum über K**.*
Schreibweise: $(a - b)v = av - bv$. $(-1) \cdot v = -v$.
*$0_K \cdot v =: 0_V$ heißt **Nullvektor**.*

Beispiele

1) $0 = (\{0\}, +)$, der **Nullraum**, ist Vektorraum über einen beliebigen Körper K.

2) $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ ist mit $+$ wie gewohnt eine Gruppe und $\cdot \colon \mathbb{R} \times \mathbb{C} \to \mathbb{C}, (r, (x, u)) \mapsto j_{\mathbb{R}}(r) \cdot (x, u) = (rx, ru)$ liefert einen Vektorraum über R.

Satz 1, § 6

Die Menge $K^M = \mathrm{Abb}(M, K)$ (K Körper, $M \neq \varnothing$ Menge) aller Abbildungen mit

$$+ \colon K^M \times K^M \to K^m, (f, g) \mapsto f + g = [m \mapsto f(m) + g(m)] \tag{II.1}$$
$$\cdot \colon K \times K^M \to K^m, (c, f) \mapsto c \cdot f = [m \mapsto c \cdot f(m)] \tag{II.2}$$

bildet Vektorraum über K.

Beweis: 1.

$(K^M, +)$ ist abelsche Gruppe! $f, g, h \in K^M$.

kdmmutativ $\forall m \in M : (f+g)(m) = f(m)+g(m) = g(m)+f(m) = (g+f)(m) \implies f+g = g+f$

assoziativ genauso: $(f+g)+h = f+(g+h)$

Neutrales Element $0 : M \to K, m \mapsto 0_K$ $(f+0=f)$

Inverse Wenn $f\colon M \to K$, so $-f\colon M \to K, m \mapsto -f(m)$ das Inverse bezüglich $+$ zu f.

2. für $\cdot$ gilt (SM1)-(SM4): $a, b \in K$

   $\forall m \in M : (a(f+g))(m) = a(f+g)(m) = a(f(m)+g(m)) = af(m)+ag(m) = (af)(m)+(ag)(m) = (af+ag)(m)$

   $\forall m \in M : ((ab)f)(m) = (ab)f(m) = a(bf(m)) = a(bf)(m) = (a(bf))(m)$

   $\forall m \in M : ((a+b)f)(m) = (a+b)f(m) = af(m)+bf(m) = (af)(m)+(bf)(m) = (af+bf)(m)$

   $\forall m \in M : (1f)(m) = 1f(m) = f(m) = 1f = f$ ■

Beispiele

1) $M = \{1, 2, \dots, n\} \implies K^M =: K^n$ heißt **Standardvektorraum** über K. $f \in K^n$ gegeben durch $(f(1), \dots, f(n)) =: (f_1, \dots, f_n) \in K \times K \times \cdots \times K$.

   Addition: $(f_1, \dots, f_n) + (g_1, \dots, g_n) = (f_1 + g_1, \dots, f_n + g_n)$

   Skalarmultiplikation: $c(f_1, \dots, f_n) = (cf_1, \dots, cf_n), c \in K$

2) $M = \mathbb{N} \implies K^{\mathbb{N}}$ **Vektorraum aller Folgen** über K.a

   $f \in K^{\mathbb{N}} : (f_0, f_1, \dots) = (f_n)_{n\in\mathbb{N}}, \quad f_n \in K, n \in \mathbb{N}$

6.2. Unterräume

Definition 2, § 6

*$(V, +, \cdot)$ sei Vektorraum. Eine Teilmenge $\varnothing \neq W \subseteq V$, die bezüglich $+, \cdot$ von V einen Vektorraum bildet, heißt **Untervektorraum** oder Teilraum von V: $W < V$, $\mathscr{T}(v) := \{W < V\}$ **Menge der Teilräume**.*

Bemerkung 1, § 6

Sei $(V, +, \cdot)$ ein Vektorraum über $K, \varnothing \neq W \subseteq V$. Dann:

$$W < V \iff \forall v, w \in W, \forall a \in K : v + w \in W \wedge av \in W \tag{II.3}$$

Beweis: Hinrichtung ist klar, Rückrichtung: $(W, +)$ bildet abelsche Gruppe, da Assoziativ- und Kommutativgesete in V gelten. Neutrales und Inverses in W: $v \in W \implies -v \in W \implies v - v = 0_V \in W \implies (W, +, \cdot)$ ist Vektorraum, da (SM1)-(SM4) in V gelten und damit auch in W. ■

Beispiele

Homogene lineare Gleichungssysteme Gesucht sind $x_1, \dots, x_n \in K$ mit $\forall i \in \{1, \dots, m\} (n, m \in \mathbb{N})$:

$$\sum_{j=1}^{n} a_{ij} x_j = 0$$

für vorgegebene $a_{ij} \in K$. Sei $L := \{(x_1, \dots, x_n) \in K^n | \forall i = 1, \dots, m : \sum_{j=1}^{n} a_{ij} x_j = 0\} \subseteq K^n$. Dann gelten falls $x \in L \wedge y \in L \implies x + y \in L, a \in K, x \in L \implies ax \in L$.

Zum Beispiel zweiteres $ax = (ax_1, \dots, ax_n) \implies \sum_{j=1}^{n} a_{ij} a x_j = a \cdot \left(\sum_{j=1}^{n} a_{ij} x_j \right) = a \cdot 0 = 0 \forall = 1, \dots, m \implies ax \in L \implies L$ ist Untervektorraum von K^n.

Homogene lineare Rekursion über K Gegeben $x_1, \dots, c_m \in K, L = \{x \in K^{\mathbb{N}} | \forall n \in \mathbb{N} : x_{n+m} + x_{n+m-1} c_1 + \dots + c_m x_n = 0\}$

Ist $x \in L \wedge y \in L \implies x + y \in L, a \in K, x \in L \implies ax \in L$.

Zweiteres: $x = (x_0, x_1, x_2, \dots) \implies ax = (ax_0, ax_1, \dots) \implies ax_{n+m} + ax_{n+m-1} c_1 + \dots + ax_n c_m = a(x_{n+m} + x_{n+m-1} c_1 + \dots + x_n c_m) = a \cdot 0 = 0 \implies ax \in L$

Bemerkung 2, § 6

V Vektorraum über $K \implies \mathcal{T}(V)$ ist durch $<$ geordnet.

Beweis: $\forall W_i < V : W_i < W_i$

Wenn $W_i < W_j < W_k \implies W_i < W_k$.

Wenn $W_i < W_j \wedge W_j < W_i \implies W_i = W_j$ als Mengen. Da $W_i < W_j \implies W_i = W_j$ als Vektorraum. ■

6.3. Durchschnitt und Summen von Unterräumen

Bemerkung 3, § 6

V Vektorraum über Körper K, $I \neq \varnothing, \forall i \in I : W_i < V$

$$W := \bigcap_{i \in I} W_i < V$$

Beweis: $W \neq \varnothing$, da $0_V \in W_i \forall i \in I \implies O_V \in W$.

Seien $v, w \in W \implies \forall i \in I : v \in W_i \wedge w \in W_i \implies v + w \in W_i \forall i \in I \implies v + w \in \bigcap_{i \in I} W_i$.

Sei $a \in K, v \in W \implies \forall i \in I : v \in W_i \implies av \in W_i \forall i \in I \implies av \in \bigcap_{i \in I} W_i$ ■

Beispiel $V = \mathbb{R}^2, W_1 = \{(a, 0) \in \mathbb{R}^2 | a \in \mathbb{R}\}, W_2 = \{(0, b) \in \mathbb{R}^2 | b \in \mathbb{R}\}$. Dann $W_1 < \mathbb{R}^2 \implies w_1 \cap w_2 = 0$ (Nullraum).

$w_1 \cup W_2 \overset{?}{<} \mathbb{R}^2$ ist nicht der Fall, denn $(1, 1) \notin W_1 \cup W_2$ aber $(1, 0) + (0, 1) = (1, 1)$.

Definition 3, § 6

K Körper, V Vektorraum über K, $S \subseteq V$ Teilmenge.

a)

$$\langle S \rangle := \bigcap_{S \subset W < V} W$$

heißt der ***von S aufgespannte Unterraum***[1].

b) Falls $W_i < V$ für $i \in I \neq \varnothing$ ist

$$S = \bigcup_{i \in I} W_i \implies \sum_{i \in I} W_i := \langle S \rangle$$

Summe der Unterräume W_i.

Bemerkung 4, § 6

a) $S \subseteq V$ Teilmenge

$$\implies \langle S \rangle = \left\{ \sum_{i=1}^{n} a_i v_i \middle| n \in \mathbb{N}, a_i \in K, v_i \in S \right\} =: W$$

b) $W_i < V \quad \forall i \in I \neq \varnothing$. Dann $w \in \sum_{i \in I} W_i \iff \exists J \subseteq I$, J endlich, mit: $w = \sum_{j \in J} w_j$ mit $w_j \in W_j$.

Beweis: a) $v, w \in W, a \in K \implies v + w \in W, av \in W \implies W < V, S \subseteq W \implies \langle S \rangle < W$. Ist $w \in W \implies w = \sum_{i=1}^{n} a_i v_i$.

Ist $W' < V$ mit $S \subseteq W' \implies w \in W' \implies W \subseteq W' \implies W \subseteq \langle S \rangle$.

b) Ist $w \in \sum_{i \in I} W_i \overset{\text{a)}}{\implies} w = \sum_{j=1}^{n} a_j v_j, a_j \in K, v_j \in \bigcup_{i \in I} W_i \implies \exists i(j) \in I : v_j \in W_{i(j)} \implies a_j v_j \in W_{i(j)}, a_j v_j = w_{i(j)} \implies w = \sum w_{i(j)} \implies$ Behauptung. ∎

Frage: Wann ist so eine Darstellung wie in b) eindeutig?

Definition 4, § 6

K Körper, V K-Vektorraum. $I \neq \varnothing, W_i < V \forall i \in I$. Dann heißt $W < V$ ***direkte Summe*** *der Unterräume W_i :*

$$\bigoplus_{i \in I} W_i : \iff$$

1) $W = \sum W_i$

2) $\forall i \in I : W_i \cap \left(\sum_{i \neq j \in I} W_j \right) = 0$

Satz 2, § 6

K Körper, V K-Vektorraum. $I \neq \emptyset, W_i < V \forall i \in I. W < V$.
Dann: $W = \bigoplus_{i\in I} W_i \iff \forall w \in W \forall i \in I \exists! w_i \in W_i : w = \sum'_{i\in I} w_i$, wobei $w_i = 0$ für bis auf endlich viele i.
Definition $\sum'$: $\forall J \subseteq I$ endlich mit $w_i \neq 0 \implies i \in J \implies \sum'_{i\in I} w_i = \sum_{j\in J} w_j$
Falls $J' \subseteq I$ endlich mit $w_i \neq 0 \implies i \in J' \implies \sum_{j'\in J'} w_{j'} = \sum_{j\in J} w_j \implies J' = J \cup J'$ enthält alle Indizes $i \in I$. $w_i \neq 0 \implies$

$$\sum_{j'\in J'} w_{j'} = \sum_{j'\in J'} w_{j'} = \sum_{j\in J} w_j$$

Beweis : „⇒“ $W = \bigoplus W_i \implies W = \sum W_i \implies \forall w \in W, \forall i \in I \exists w_i \in W_i : w = \sum'_{i\in I} w_i$. Angenommen, $w = \sum'_{i\in I} w_i = \sum_{i\in I} \tilde{w}_i \implies 0 = \sum'_{i\in I}(w_i - \tilde{w}_i) \implies \tilde{w}_i . w_i = \sum_{i\neq j\in I}(w_j - \tilde{w}_j) \in W_i \cap \left(\sum_{i\neq j\in I} W_j\right) = 0 \implies \tilde{w}_i - w_i = 0 \implies w_i = \tilde{w}_i$

„⇐“ Bem. 4b . $W = \sum_{i\in I} W_i$. Falls $-w_i \in W_i \cup \left(\sum_{i\neq j\in I} W_j\right) \implies -w_i = \sum'_{i\neq j\in I} w_j \implies \sum'_{i\in I} = 0 = \sum'_{i\in I} 0 \implies w_i = 0 \forall i \in I \implies w_i \cap \left(\sum W_j\right) = 0$. ■

6.4. Komplement von Vektorräumen

Definition 5, § 6

*K Körper, V Vektorraum über K, $W < V$. Dann heißt $X < V$ ein **Komplement zu W**, falls $V = W \oplus X$.*

Beispiel $V = \bigoplus_{i\in I} W_i, W = W_i \implies X = \sum_{i\neq j\in I} W_j$ ist Komplement zu W.

Satz 3, § 6

K Körper, V K-Vektorraum, $W < V$ Teilraum. Dann existiert $X < V : V = W \oplus X$.

Beweis : Achtung, der Beweis erfolgt mit Wissen aus Kapitel 8!

Sei T Basis von X, $S = V \implies \exists S' \subseteq S : T \cup S'$ Basis von V. Sei $W = \langle S' \rangle \implies V = \langle T \cup S' \rangle = \langle T \rangle + \langle S' \rangle = X + W = X \oplus W$. ■

§ 7. Lineare Abbildungen

7.1. Erste Definitionen und Eigenschaften

Definition 1, § 7

*Sei K Körper, V, W K-Vektorräume. Eine Abbildung $\Phi : V \to W$ heißt **lineare Abbildung***

$:\Longleftrightarrow$

$$\forall v, w \in V : \Phi(v + w) = \Phi(v) + \Phi(w) \tag{II.4}$$
$$\forall a \in K, v \in V : \Phi(av) = a \cdot \Phi(v) \tag{II.5}$$

Φ *wird* ***Vektorraumhomomorphismus*** *genannt. Wir definieren:*

$$\ker \Phi := \{v \in V | \Phi(v) = 0_W\} \tag{II.6}$$
$$\text{Bild}\, \Phi := \{w \in W | \exists v \in V : w = \Phi(v)\} \tag{II.7}$$

Eine bijektive lineare Abbildung $\Phi\colon V \to W$ *heißt* ***Isomorphismus****:* $\Phi\colon V \xrightarrow{\sim} W$ *oder* $V \cong W$*.*

Bemerkung 1, § 7

V, W K-Vektorräume, $\Phi\colon V \to W$ *lineare Abbildung* $\Longrightarrow$

a) $\ker \Phi < V$

b) $\text{Bild}\, \Phi < W$

Beweis : a) Seien $v_1, v_2 \in \ker \Phi \implies \Phi(v_1 + v_2) = \Phi(v_1) + \Phi(v_2) = 0 + 0 = 0 \implies v_1 + v_2 \in \ker \Phi$.

Falls $a \in K, v \in \ker \Phi \implies \Phi(av) = a \cdot \Phi(v) = a \cdot 0 = 0 \implies av \in \ker \Phi$.

Außerdem $\Phi(0_V) = 0_W \implies 0_V \in \ker \Phi \implies \ker \Phi \neq \varnothing$.

b) Seien $w_1, w_2 \in \text{Bild}\, \Phi \implies \exists v_1, v_2 \in V : \Phi(v_i) = w_i \implies w_1 + w_2 = \Phi(v_1) + \Phi(v_2) = \Phi(v_1 + v_2) \implies w_1 + w_2 \in \text{Bild}\, \Phi$.

Sei $a \in K, w \in \text{Bild}\, \Phi : \exists v \in V : \Phi(v) = w \implies a \cdot w = a \cdot \Phi(v) = \Phi(av) \implies a \cdot w \in \text{Bild}\, \Phi$ und $\Phi(0) = 0 \implies 0 \in \text{Bild}\, \Phi \implies \text{Bild}\, \Phi \neq \varnothing$. ■

Bemerkung 2, § 7

$\Phi\colon V \to W$ *lineare Abbildung von K-Vektorram. Dann:*

a) Φ *surjektiv* $\Longleftrightarrow \Phi(v) = W$*.*

b) Φ *injektiv* $\Longleftrightarrow \ker \Phi = 0$ *(Nullraum).*

c) Φ *bijektiv* $\Longleftrightarrow \Phi(V) = W \wedge \ker \Phi = 0$

Beweis : a) per Definition

b) „$\Rightarrow$“ Sei Φ injektiv. $\Phi(x) = 0 = \Phi(0) \implies x = 0 \implies \ker \Phi = 0$.

„$\Leftarrow$“ $\Phi(x) = \Phi(y) \implies \Phi(x) - \Phi(y) = 0 \Longleftrightarrow \Phi(x - y) = 0 \overset{\ker \Phi = 0}{\Longrightarrow} x - y = 0 \Longleftrightarrow x = y \implies \Phi$ injektiv.

c) folgt aus a) und b) ■

Bemerkung 3, § 7

a) V, W, X K-Vektorräume, $\Phi\colon V \to W, \Psi\colon W \to X$ seien lineare Abbildungen $\Longrightarrow$ $\Psi \circ \Phi\colon V \to X$ ist lineare Abbildung.

b) $\Phi\colon V \xrightarrow{\sim} W$ Isomorphismus von K-Vektorraum $\Longrightarrow$ Φ^{-1} ist lineare Abbildung.

Beweis: a) $\Psi \circ \Phi(v_1 + v_2) = \Psi(\Phi(v_1 + v_2)) = \Psi(\Phi(v_1) + \Phi(v_2)) = \Psi(\Phi(v_1)) + \Psi(\Phi(v_2)) = \Psi \circ \Phi(v_1) + \Psi \circ \Phi(v_2)$.

$\Psi \circ \Phi(av) = \Psi(\Phi(av)) = \Psi(a\Phi(v)) = a\Psi(\Phi(v)) = a \cdot \Psi \circ \Phi(v)$

b) $\forall w \in W \quad \exists! v \in V : \Phi(v) = w \implies$ Seien $w_1, w_2 \in W \implies \exists! v_1, v_2 \in V : \Phi(v_i) = w_i \implies \Phi(v_1 + v_2) = \Phi(v_1) + \Phi(v_2) = w_1 + w_2 \implies \Phi^{-1}\colon W \to V, w \mapsto v$ (wobei $\Phi(v) = w$ eindeutig) $\implies \Phi^{-1}(w_1 + w_2) = v_1 + v_2 = \Phi^{-1}(w_1) + \Phi^{-1}(w_2)$.

$a \in K, v \in V\colon \Phi(av) = a \cdot \Phi(v) = aw \implies \Phi^{-1}(aw) = av = a \cdot \Phi^{-1}(w) \implies \Phi^{-1}$ lineare Abbildung. ■

7.2. Kongruenzrelation und Faktorräume

Definition 2, § 7

*K Körper, V K-Vektorräume. Eine Äquivalenzrelation $\equiv$ auf V heißt **Kongruenzrelation** $:\Longleftrightarrow$*

1) Falls $v \equiv v' \wedge w \equiv w' \implies v + w \equiv v' + w'$

2) Falls $a \in K, v \equiv v' \implies av \equiv av'$. $(v, v', w, w' \in V)$

Bemerkung 4, § 7

a) V K-Vektorraum. $\equiv$ Kongruenzrelation auf V $\implies$ $W := \{v \in V | v \equiv 0\} < V$ und $v \equiv w \Longleftrightarrow v - w \in W$.

b) Sei $W < V$ und sei $v \equiv w :\Longleftrightarrow v - w \in W$. Dann definiert dies eine Kongruenzrelation mit $W = \{v \in V | v \equiv 0\}$.

Beweis: Seien $v, w \in W \implies v \equiv 0, w \equiv 0 \implies v + w \equiv 0 + 0 = 0 \implies v + w \in W$.

Seien $a \in K, v \in W \implies v \equiv 0 \implies av \equiv a \cdot 0 = 0 \implies a \cdot v \in W$.

$v \equiv w \Longleftrightarrow v - w \equiv w - w = 0 \Longleftrightarrow v - w \in W$

Sei $W < V : v - v = 0 \in W \implies v \equiv v$. Wenn $v - w \in W \implies -(v - w) = w - v \in W \implies w \equiv v, v \equiv w, w \equiv x \implies v - w \in W, w - x \in W$.

$v - w = v - w + w - x = (v - w) + (w - x) \in W \implies v \equiv x$.

Seien $v \equiv v'$ und $w = w' \implies v - v' \in W \wedge w - w' \in W \implies (v - v') + (w - w') \in W$

$(v - v') + (w - w') = (v + w) - (v' + w') \in W \implies v + w \equiv v' + w'$.

Seien $a \in K, v \equiv v' \iff v - v' \in W \implies a(v - v') \in W \iff av - av' \in W \iff av \equiv av' \implies \equiv$ ist Kongruenzrel.

$W = \{v \in V | v \in W\} = \{v \in V | v - 0 \in W\} = \{v \in V | v \equiv 0\}$ ■

Schreibweise: $v \equiv w \mod W$, **Kongruenz modulo W**.

Bemerkung 5, § 7

K Körper, V K-Vektorraum. $W < V$ und $\equiv$ die Kongruenzrelation zu W. Dann $V/_{\equiv} = \bar{V}$ mit

$$+ : \bar{V} \times \bar{V} \to \bar{V}, \quad (\bar{v}, \bar{w}) \mapsto \bar{v} + \bar{w} := \overline{v + w} \tag{II.8}$$

$$\cdot : K \times \bar{V} \to \bar{V}, \quad (a, \bar{v}) \mapsto a \cdot \bar{v} := \overline{av} \tag{II.9}$$

ist ein K-Vektorraum.

Beweis: $\bar{v} = \{v' \in V | v' - v \in W\} = \{v' \in V | v' = v + w, w \in W\} =: v + W \subseteq V$.

Zu zeigen: $+, \cdot$ sind wohldefiniert: $\bar{v} = \bar{v}' \wedge \bar{w} = \bar{w}'$

$\implies v' \equiv v \wedge w \equiv w' \implies v + w \equiv v' + w' \implies \overline{v + w} = \overline{v' + w'}$.

Ist $a \in K, \bar{v} = \bar{v}' \implies v \equiv v' \implies av \equiv av' \iff \overline{av} = \overline{ab'}$. VR-Axiome übertragen sich von V. ■

Definition 3, § 7

$\bar{V} =: V/_W$ heißt Faktorraum von V nach W.

7.3. Der Hauptsatz für lineare Abbildungen

Satz 1, § 7

K Körper, $\Phi : V \to W$ lineare Abbildungen. Dann

$$V/_{\ker \Phi} \xrightarrow{\sim} \Phi(V) \subseteq W \tag{II.10}$$

$$\bar{v} \mapsto \Phi(v) \tag{II.11}$$

.

Beweis: $\Phi : V \to W \overset{\text{B 1}}{\implies} \ker \Phi < V, \text{Bild}\, \Phi < W$. Sei $\sim$ die Äquivalenzrelation zu Φ, d.h. $v \sim w : \iff \Phi(v) = \Phi(w)$. D.h. $v \sim w \iff \Phi(v) - \Phi(w) = \Phi(v - w) = 0 \iff v - w \in \ker \Phi \implies \sim$ ist die Kongruenzrelation zu $\ker \Phi \implies V/_{\sim} = V/_{\ker \Phi}$

$\kappa : V \to V_{\ker \Phi}, v \mapsto \bar{v} = v + \ker \Phi$ surjektiv nach §1, Satz 1. Seien $v, w \in V, a \in K$.

$\kappa(v + w) = \overline{v + w} = \bar{v} + \bar{w} = \kappa(v) + \kappa(w)$

$\kappa(av) = \overline{av} = a\bar{v} = a\kappa(v)$

$\Longrightarrow$ κ ist lineare Abbildung.

Betrachte $\bar{\Phi}\colon V/_{\ker\Phi} \to \Phi(V), \bar{v} \mapsto \Phi(v)$ ist wohldefinierte, bijektive Abbildung, nach §1, Satz 1.

Linearität von $\bar{\Phi}\colon \bar{v}, \bar{w} \in V/_{\ker\Phi}, a \in K$.

$$\Longrightarrow \bar{\Phi}(\bar{v}+\bar{w}) = \bar{\Phi}(\overline{v+w}) = \Phi(v+w) = \Phi(v)+\Phi(w) \tag{II.12}$$
$$= \bar{\Phi}(\bar{v}) + \bar{\Phi}(\bar{u}) \tag{II.13}$$
$$= \bar{\Phi}(a\bar{v}) = \bar{\Phi}(\overline{av}) = \Phi(av) = a\Phi(v) = a\bar{\Phi}(\bar{v}) \tag{II.14}$$

$\Longrightarrow$ $\bar{\Phi}$ ist Isomorphismus. ■

Folgerung 1, § 7

Jede lineare Abbildung $\Phi\colon V \to W$ lässt sich zerlegen in ein Produkt einer surjektiven, bijektiven und injektiven linearen Abbildung (Satz 1, § 1).
($\Phi\colon : V \xrightarrow{\kappa} V/_{\ker\Phi} \xrightarrow{\bar{\Phi}} \Phi(V) \xrightarrow{\iota} W$. $\kappa, \bar{\Phi}$ linear siehe Beweis, $\iota\colon w \mapsto w$ linear)

7.4. Der Vektorraum Hom(V,W)

Definition 4, § 7

K Körper, V, W K-Vektorräume. Wir definieren die

Menge der linearen Abbildungen (Homomorphismen)

$$\mathrm{Hom}(V,W) := \{\Phi : V \to W | \Phi \textit{ linear}\}$$

Endomorphismen

$$\mathrm{End}(V) := \mathrm{Hom}(V,V)$$

allgemeine lineare Gruppe

$$\mathrm{Gl}(V) := \{\Phi \in \mathrm{End}(V) | \Phi \textit{ bijektiv}\}$$

Definition 5, § 7

Ein K-Vektorraum $(V,+,\cdot)$ zusammen mit einem Produkt $\circ\colon V \times V \to V$, sodass $(V,+,\circ)$ ein Ring mit 1 ist und außerdem $\forall a \in K, v, w \in V : a \cdot (v \circ w) = (a \cdot v) \circ w = v \circ (a \cdot w)$ heißt ***K-Algebra (mit Eins)****.*

Satz 2, § 7

K Körper, V, W K-Vektorraum.

a) $\mathrm{Hom}(V,W)$ *ist K-Vektorraum mit*

$$+\colon \mathrm{Hom}(V,W)\times\mathrm{Hom}(V,W)\to\mathrm{Hom}(V,W), \tag{II.15}$$
$$(\Phi,\Psi)\mapsto\Phi+\Psi:=(v\mapsto\Phi(v)+\Psi(v)) \tag{II.16}$$
$$\cdot\colon K\times\mathrm{Hom}(V,W)\to\mathrm{Hom}(V,W),(a,\Phi)\mapsto a\cdot\Phi=(v\mapsto a\cdot\Phi(v)) \tag{II.17}$$

b) Der K-Vektorraum $\mathrm{End}\,V$ *ist eine K-Algebra mit* $\circ\colon \mathrm{End}\,V\times\mathrm{End}\,V\to\mathrm{End}\,V,(\Phi,\Psi)\mapsto\Phi\circ\Psi$.

c) $\mathrm{Gl}(V)$ *ist eine Gruppe.*

Beweis : a) folgt ähnlich wie bei Satz 1, § 6 (gleiches für $\mathrm{Abb}(M,K)$), z.B:

$$(\Phi+\Psi)(v)=\Phi(v)+\Psi(v)\overset{W\,\mathrm{VR}}{=}\Psi(v)+\Phi(v)=(\Psi+\Phi)(v)$$

$\Longrightarrow$ $+$ kommutativ.

Nullvektor: $0: V\to W, v\mapsto 0$, neutrales Element bezüglich $+$.

b) $\mathrm{End}\,V$ ist K-Vektorraum nach a). Ist $\Phi,\Psi\in\mathrm{End}\,V\implies\Phi\circ\Psi\in\mathrm{End}\,V$ nach Bemerkung ??.

id_V ist neutrales Element bezüglich $\circ$. Assoziativitätsgesetze gelten nach §1.

Distributivität: $\Phi,\Psi,\lambda\in\mathrm{End}(V)$

$$(\lambda\circ(\Phi+\Psi))(v)=\lambda((\Phi+\Psi)(v))=\lambda(\Phi(v)+\Psi(v))=\lambda(\Phi(v))+\lambda(\Psi(v)) \tag{II.18}$$
$$=\lambda\circ\Phi(v)+\lambda\circ\Psi(v)=(\lambda\circ\Phi+\lambda\circ\Psi)(v) \tag{II.19}$$

$(\Phi+\Psi)\circ\lambda=\Phi\circ\lambda+\Psi\circ\lambda$ analog.

$\Longrightarrow$ $(\mathrm{End}(V),+,\circ)$ ist Ring mit Ring mit Eins.

K-Algebra: $a\in K,\Phi,\Psi\in\mathrm{End}(V)$:

$$a(\Phi\circ\Psi)(v)=a\Phi(\Psi(v))=(a\Phi)(\Psi(v))=(a\Phi)\circ\Phi(v) \tag{II.20}$$
$$=\Phi(a\Psi(v))=\Phi((a\Psi)(v)) \tag{II.21}$$
$$=\Phi\circ(a\Psi)(v) \tag{II.22}$$

c) $\Phi,\Psi\in\mathrm{Gl}\,V\implies\Phi\circ\Psi$ bijektive lineare Abbildung $\implies\circ$ auf $\mathrm{Gl}\,V$ wohldefiniert. $\mathrm{Gl}\,V\subseteq S_V\implies\circ$ ist assoziativ. id_V neutrales Element bezüglich $\circ$: $\Phi\in\mathrm{Gl}\,V\implies\Phi^{-1}$ ist linear, bijektiv $\implies\Phi^{-1}\in\mathrm{Gl}\,V\implies\mathrm{Gl}\,V$ Gruppe. ■

Definition 6, § 7

K Körper, V K-Vektorraum $\implies\pi\in\mathrm{End}\,V$ *heißt* ***Projektion*** $:\iff\pi^2=\pi\circ\pi\overset{!}{=}\pi$.

Bemerkung 6, § 7

V K-Vektorraum, π *Projektion*

$$\implies V=\mathrm{Bild}\,\pi\oplus\ker\pi$$

Beweis: $v \in V \implies w = v - \pi(v) \implies \pi(v) = \pi(\pi(v)) = \pi(v) - \pi(w) \implies \pi(w) = 0 \implies w \in \ker\pi \implies v \in \text{Bild}\,\pi + \ker\pi$.

Ist $v \in \text{Bild}\,\pi \cap \ker\pi \implies \exists w : v = \pi(w) \implies 0 = \pi(v) = \pi(\pi(w)) = \pi(w) = v \implies v = 0$. ■

Bezeichnung Die Projektion in Bemerkung 6, § 7 heißt **Projektion von V auf** $\text{Bild}\,\pi$ **längs** $\ker\pi$.

Beispiel $\pi\colon \mathbb{R}^2 \to \mathbb{R}^2, (a,b) \mapsto (a-b,0)$ ist Projektion von $\mathbb{R}^2$ auf $(1,0)\mathbb{R}$ längs $(1,1)\mathbb{R}$.

§ 8. Basis und Dimension

8.1. Endlich erzeugte Vektorräume

Definition 1, § 8

- *K Körper, V K-Vektorraum.* $S \subseteq V$ *heißt ein* ***Erzeugendensystem*** $: \iff V = \langle S \rangle$.
- S *heißt* ***linear unabhängig*** $: \iff 0 = \sum'_{s\in S} a_s s$ *für* $a_s = 0$ *bis auf endlich viele, dann gilt* $a_s = 0 \forall s \in S$. *Sonst ist* S ***linear abhängig***.
- S *heißt* ***Basis*** $: \iff S$ *ist Erzeugendensystem und linear unabhängig.*

Beispiel 1, § 8

a) Basis von 0*:* $\varnothing$ *ist Basis.*

b) $V = K^n, S = \{(\overbrace{1,0,\ldots,0}^{n \text{ Elemente}}), (0,1,0,\ldots,0), \ldots, (0,\ldots,0,1)\} \subseteq V$ *ist Basis von V:*
$x \in V, x = (x_1,\ldots,x_n), x_i \in K$.
$x = x_1(1,0,\ldots,0) + x_2(0,1,0,\ldots,0) + \cdots + x_n(0,\ldots,0,1)$
$\implies S$ *ist Erzeugendensystem und linear unabhängig.*

Definition 2, § 8

V *heißt* ***endlich erzeugt*** $: \iff \exists S \subseteq V, S$ *endlich,* $V = \langle S \rangle$.

Satz 1, § 8

K Körper, V K-Vektorraum, $S \subseteq V$*. Dann sind äquivalent:*

a) S ist eine Basis

b) S ist ein minimales Erzeugendensystem, d.h. $\forall t \in S : S \setminus \{t\}$ *ist kein Erzeugendensys-*

tem

c) S ist ein maximal linear unabhängiges System, d.h. $\forall t \in V\backslash S : S \cup \{t\}$ ist linear abhängig.

d) $\forall v \in V, \forall s \in S : \exists! a_s \in K : v = \sum'_{s\in S} a_s s$ mit $a_s = 0$ für bis auf endlich viele $s \in S$.

Beweis: Wir zeigen a) $\Longrightarrow$ b) $\Longrightarrow$ d) $\Longrightarrow$ c) $\Longrightarrow$ a).

a) $\Longrightarrow$ b) S Basis $\Longrightarrow$ S Erzeugendensystem. Sei $t \in S, \tilde{S} = S\backslash\{t\}$. Angenommen, $\tilde{S}$ ist Erzeugendensystem $\Longrightarrow$ $t = \sum'_{s\in S} a_s s \Longrightarrow 0 = (-1)t + \sum'_{s\in S} a_s s$ $\lightning$ zu S linear unabhängig.

b) $\Longrightarrow$ d) Sei S min. Erzeugendensystem $\Longrightarrow$ $\forall v \in V, \forall s \in S \exists a_s \in K : v = \sum'_{s\in S} a_s s$. Angenommen, diese Darstellung ist nicht eindeutig $\Longrightarrow$ $\exists w \in V : w = \sum'_{s\in S} b_s s = \sum'_{s\in S} \tilde{b}_s s$ wobei $\exists t \in S : b_t \neq \tilde{b}_t \Longrightarrow 0 = \sum'_{s\in S}(b_3 - \tilde{b}_3)s = \sum'_{s\in S} c_s s$ wobei $c_t \neq 0 \Longrightarrow 0 = \sum' \frac{a_t}{c_t} c_s s$

$\Longrightarrow v = \sum' a_s s + 0 = \sum' a_s s + \sum' \frac{a_t}{c_t} c_s s = \sum' \left(a_s - \frac{a_t}{c_t} c_s\right) s \Longrightarrow s = t : a_t - \frac{a_t}{c_t} c_t = 0 \Longrightarrow$ $S\backslash\{t\}$ ist Erzeugendensystem $\lightning$ zu S minimal.

d) $\Longrightarrow$ c) $\forall v \in V : v = \sum' a_s s, a_s$ eindeutig $\Longrightarrow$ $v = 0 : 0 = \sum' 0s \Longrightarrow a_s = 0 \Longrightarrow$ S linear unabhängig.

Sei $t \in V\backslash S \Longrightarrow \forall s \in S \exists a_s \in K : t = \sum' a_s s \Longrightarrow 0 = (-1)t + \sum' a_s s \Longrightarrow$ $S \cup \{t\}$ linear abhängig.

c) $\Longrightarrow$ a) S maximal linear unabhängig $\Longrightarrow$ S linear unabhängig $\wedge \forall t \in V\backslash S : S \cup \{t\}$ linear abhängig $\Longrightarrow$ $\exists a_k \in K : \forall s \in S \exists a_s \in K : 0 = a_t t + \sum' a_s s$ mit $a_t = 0 \Longrightarrow t = \sum' \left(-\frac{a_s}{a_t}\right) s \Longrightarrow S$ Erzeugendensystem $\Longrightarrow S$ Basis. ■

Folgerung 1, § 8

Jeder endlich erzeugte K-Vektorraum V hat eine Basis.

Beweis: $\exists S \subseteq V, S$ endlich, $\langle S\rangle = V \Longrightarrow \exists T \subseteq S$ endlich mit T Erzeugendensystem und T minimal $\Longrightarrow T$ Basis. ■

8.2. Dimension endlich erzeugter Vektorräume

M endlich, so bezeichne $\#M \in \mathbb{N}$ die Anzahl der Elemente von M. Falls M nicht endlich, so $\#M = \infty$.

Satz 2, § 8 (*Basisergänzungssatz*)

Sei V endlich erzeugter K-Vektorraum, $S \subseteq V$ endlich mit $\langle S\rangle = V, T \subseteq V$ sei linear unabhängig $\Longrightarrow \exists U \subseteq S : T \cup U$ ist Basis von V.

Beweis: $M := \{N \subseteq V | T \subseteq N \subseteq T \cup S, N$ linear unabh. $\}$

$\Longrightarrow T \in M \Longrightarrow M \neq \emptyset$, da $\#S < \infty \Longrightarrow \#M < \infty \Longrightarrow \exists B \in M : B$ ist **obere Schranke**, d.h. falls $N \in M, B \subseteq N \Longrightarrow B = N \Longrightarrow \forall s \in S : B \cup \{s\}$ ist linear abhängig $\Longrightarrow \exists$ nicht-triviale Darstellung $0 = as + \sum_{b\in B} a_b \cdot b$ mit $a \neq 0 \Longrightarrow s \in \langle B\rangle$ S Erzeugendensystem

$\Longrightarrow \forall v \in V \exists a_s \in K : v = \sum_{s\in S} a_s s$ und außerdem $\forall s \in S \exists b_{s,b} \in K : s = \sum_{b\in B} b_{s,b} b \Longrightarrow v = \sum_{s\in S} a_s (\sum_{b\in B} b_{s,b} b) = \sum_{s\in S} \sum_{b\in B} a_s b_{s,b} b = \sum_{b\in B} (\sum_{s\in S} a_s b_{s,b}) b \Longrightarrow v \in \langle B \rangle$
$\Longrightarrow B$ Basis. $U = B \backslash T$. ■

Satz 3, § 8

V K-Vektorraum, endlich erzeugt. $S \subseteq V$ endlich erzeugte Teilmenge $T \subseteq V$ linear unabhängig $\Longrightarrow$

$$\#T \leqslant \#S$$

Beweis: 1. Schritt $\#T < \infty$ Induktion nach $\#T \backslash S$. Wenn $\#T \backslash S = 0 \Longrightarrow T \subseteq S \Longrightarrow \#T \leqslant \#S$. Sei $\#T \backslash S = n + 1$ und nach Behauptung gelte $\forall T' \subseteq V$ l.u. mit $\#T' \backslash S \leqslant n$. Es existiert $t \in T \backslash S, T_0 := T \backslash \{t\}$ ist l.u. Dann existiert $U \subseteq S$ mit $T_0 \cup U$ eine Basis $\Longrightarrow U \neq \varnothing \Longrightarrow \exists t_1 \in U \subseteq S : T_1 := T_0 \cup \{t_1\} \Longrightarrow \#(T_1 \backslash S) \leqslant n \Longrightarrow \#T = \#T_1 \leqslant \#S$

2. Schritt $\#T = \infty \Longrightarrow \exists U \subseteq T : U$ linear unabhängig und $\#U > \#S \lightning$ zu Schritt 1. ■

Folgerung 2, § 8

V endlich erzeugter K-Vektorraum $\Longrightarrow$ Jede Basis besitzt die gleiche Anzahl von Elementen.

Beweis: Sei $S \subseteq V$ endlich erzeugte Teilmenge und S_1, S_2 zwei Basen $\Longrightarrow \#S_1 < \infty \Longrightarrow S_1$ ERzeugendensystem, S_2 linear unabhängig $\Longrightarrow \#S_2 \leqslant \#S_2$ und S_2 Erzzeugendensystem, S_1 linear unabhängig $\Longrightarrow \#S_1 \leqslant \#S_2 \Longrightarrow \#S_1 = \#S_2$. ■

Definition 3, § 8

*V endlich erzeugter K-Vektorraum $\Longrightarrow$ Die Elementanzahl einer Basis heißt die **Dimension** von V:*

$$\dim_K V \text{ bzw. } \dim V$$

Beispiel: $V = K^n \Longrightarrow \dim V = n$

8.3. Isomorphiesatz

Satz 4, § 8

V, W K-Vektorräume, $\dim V = n, S = \{s_1, \ldots, s_n\} \subseteq V$ Basis von V, $T = \{t_1, \ldots, t_n\} \subseteq W$ beliebig $\Longrightarrow \exists! \Phi \in \mathrm{Hom}(V, W) : \Phi(s_i) = t_i$.
Dabei gilt:

a) Φ injektiv $\Longleftrightarrow$ T linear unabhängig

b) Φ surjektiv $\Longleftrightarrow$ T Erzeugendensystem

c) Φ bijektiv $\Longleftrightarrow$ T Basis

Beweis: **1. Schritt** Existenz und Eindeutigkeit von Φ.

Eindeutigkeit Seien $\Phi, \tilde{\Phi} \in \mathrm{Hom}(V,W) : \Phi(s_i) = t_i = \tilde{\Phi}(s_i) \implies \forall v \in V \exists a_i \in K : v = \sum_{i=1}^n a_i s_i \implies \Phi(v) = \Phi(\sum_{i=1}^n a_i s_i) = \sum a_i \Phi(s_i) = \sum a_i t_i = \sum a_i \tilde{\Phi}(s_i) = \tilde{\Phi}(v) \implies \Phi = \tilde{\Phi}$.

Existenz Seitze $\Phi(v) = \sum a_i \Phi(s_i)$, wenn $v = \sum a_i s_i, a_i \in K$.

Wenn $w \in V, w = \sum b_i s_i \implies \Phi(v+w) = \Phi\left(\sum (a_i + b_i) s_i\right) = \sum (a_i + b_i) t_i = \sum a_i t_i + \sum b_i t_i = \sum a_i \Phi(s_i) + \sum b_i \Phi(s_i) = \cdots = \Phi(v) + \Phi(w)$.

Wenn $a \in K, v \in V : \Phi(av) = \Phi(\sum a a_i s_i) = \sum a a_i t_i = a \sum a_i \Phi(s_i) = a\Phi(v) \implies \Phi \in \mathrm{Hom}(V,W)$.

2. Schritt a), b) $\implies$ c) klar.

a) T l.u. $\iff$ $(\sum a_i t_i = 0 \implies a_i = 0)$. Für $v = \sum a_i s_i \in V$

$\Phi(v) = 0 \iff 0 = a_i \iff \ker \Phi = 0 \iff \Phi$ injektiv.

b) Gilt $\Phi(V) = \langle T \rangle (= W)$. Dann: Φ surjektiv $\iff$ T Erzeugendensystem. ■

Satz 5, § 8 (*Isomorphiesatz*)

Für endlich erzeugte K-Vektorräume V, W gilt:

$$V \cong W \iff \dim V = \dim W$$

Beweis: „$\Rightarrow$“ Sei $\Phi\colon V \xrightarrow{\sim} W$ Isomorphismus, $\{s_1, \ldots, s_n\} = S$ Basis von V, $n = \dim V \implies T = \{\Phi(s_1), \ldots, \Phi(s_n)\}$ ist Basis von W (Satz 4c) $\implies \dim W = n$.

„$\Leftarrow$“ Sei $\{s_1, \ldots, s_n\} = S \subseteq V$ Basis, $\dim V = n = \dim W$, $\{t_1, \ldots, t_n\} = T \subseteq W$ Basis von W $\overset{\text{S4}}{\implies} \exists! \Phi \in \mathrm{Hom}(V,w) : \Phi(s_i) = t_i \implies \Phi$ bijektiv, also $V \cong W$. ■

8.4. Einige Dimensionssätze

Bemerkung 1, § 8

V endlich erzeugter K-Vektorraum, $W < V$ Teilraum $\implies \dim W \leqslant \dim V$.

Beweis: V endlich erzeugt $\implies$ W endlich erzeugt $\implies$ W hat endliche Basis $T \subseteq V$, linear unabhängig $\implies$ T zu einer Basis $S \supseteq T$ von V ergänzen können $\implies \dim W = \#T \leqslant \#S = \dim V$. ■

Satz 6, § 8

V endlich erzeugter K-Vektorraum, $W_i < V, i = 1,2 \implies$

a) $\dim(W_1 + W_2) = \dim W_1 + \dim W_2 - \dim W_1 \cap W_2$

b) Ist $W_1 \cap W_2 = 0 \implies \dim(W_1 \oplus W_2) = \dim W_1 + \dim W_2$

Beweis: a) $\implies$ b) klar.

a)

Sei T Basis von $W_1 \cap W_2 \implies \exists$ Basen $S_i := T \cup U_i$ von $W_i, i = 1,2$ wobei $U_i \subseteq W_i \backslash T, U_i$ l.u.

Behauptung: $S := T \cup U_1 \cup U_2$ ist Basis von $W = W_1 + W_2$. Ist $w \in W, w = w_1 + w_2$ mit $w_i \in W_i$, d.h. $w_i \in \langle S_i \rangle \implies w \in \langle S_1 \rangle + \langle S_2 \rangle = \langle S_1 \cup S_2 \rangle = \langle S \rangle \implies S$ ist Erzeugendensystem von W.

$$0 = \sum_{s \in S} a_s s = \overbrace{\sum_{t \in T} a_t t}^{A} + \overbrace{\sum_{s \in U_1} b_s s}^{B} + \overbrace{\sum_{s \in U_2} c_s s}^{C} \implies A + b = -c \in W_1 \cap W_2$$

$W_1 \cap W_2 = \langle T \rangle \ni -C$, aber auch $-C \in \langle T \rangle \oplus \langle U_1 \rangle$.

$T \cup U_1$ ist Basis von $W_1 \implies \langle T \rangle \cap \langle U_1 \rangle = 0$. Wenn $v \in \cdots \cap \cdots : v = \sum_{t \in T} a_t t = \sum_{s \in U_1} a_s s \implies 0 = \sum_{s \in T \cup U} a_s s \implies a_s = 0 \implies v = 0$

$\implies -c = x_1 + x_2, x_1 \in \langle T \rangle, x_2 \in \langle U_1 \rangle$ eindeutig! aber $-C \in \langle T \rangle \implies x_2 = 0 \implies \sum_{s \in U_1} n_s s = 0 \implies b_2 = 0 \implies A + c = -n \implies c_s = 0$ mit gleicher Überlegung $\implies a_t = 0 \forall t \in T \implies S$ linear unabhängig $\implies \dim W_1 + \dim W_2 = \#T\#U_1 + \#T + \#U_2 = \dim W_1 \cap W_2 + \dim W_1 + W_2$ ■

Folgerung

V endlich erzeugter K-Vektorraum, $W_i < V$, $i = 1, \ldots, n$

$$\implies \dim \left(\oplus_{i=1}^{n} W_i\right) = \sum_{i=1}^{n} \dim W_i$$

Satz 7, § 8

V endlich erzeugter K-Vektorraum, $W < V \implies$

$$\dim V/_W = \dim V - \dim W$$

Beweis: T Basis von $W \overset{\text{S 2,x8}}{\implies} \exists U \subseteq V \backslash T : T \cup U$ Basis von V. Sei $X = \langle U \rangle < V \implies V = \langle T \cup U \rangle = \langle T \rangle + \langle U \rangle = W + X$ und es gilt $\langle T \rangle \cap \langle U \rangle = 0$ (sonst $v = \sum_{t \in T} a_t t = \sum_{u \in U} a_u u \implies 0 = \sum_{s \in T \cup U} a_s s \implies a_s = 0 \forall s \implies v = 0$).

$\implies V = W \oplus X$. Übung: $X \cong V/_W$.

$\implies \dim V - \dim W = \dim X = \dim V/_W$. ■

Folgerung 3, § 8

V, W endlich erzeugte K-Vektorräume, $\Phi : V \to W$ linear. Dann:

a) $\dim \Phi(V) = \dim V - \dim \ker \Phi$

b) Falls $\dim V = \dim W \implies$ (Φ *surjektiv* $\iff$ Φ *injektiv*)

Beweis: a) Homomorphiesatz: $\Phi(V) \cong V/_{\ker \Phi} \overset{\text{S. 7,x8}}{\implies} \dim \Phi(V) = \dim V - \dim \ker \Phi$

b) Φ surjektiv $\iff \dim \Phi(V) = \dim W = \dim V \iff \dim \ker \Phi = 0 \iff \ker \Phi = 0 \iff \Phi$ injektiv. ■

Definition 4, § 8

$\dim \Phi(V)$ *heißt* ***Rang von*** Φ, $\dim \ker \Phi$ *heißt* ***Defekt von*** Φ.

8.5. Der allgemeine Basissatz

Bemerkung 2, § 8

V K-Vektorraum, $S \subseteq V$. Dann S linear unabhängig $\iff (\forall T \subseteq S, \#T < \infty, T \text{ l.u.})$.

Beweis : „$\Rightarrow$“ Sei S linear unabhängig, $T \subseteq S, \#T < \infty$.

$0 = \sum_{t\in T} a_t t = \sum'_{s\in S} a_s s$ mit $a_s = 0$ für $s \notin T \implies a_s = 0 \; \forall s \in S \implies a_t = 0 \; \forall t \in T \implies T$ linear unabhängig.

„$\Leftarrow$“ Angenommen, S lienar abhängig $\implies \exists 0 = \sum'_{s\in S} a_s s$ nichttrivial $\implies T := \{t \in S \,|\, a_s \neq 0\} \neq$ endlich $\implies 0 = \sum_{t\in T} a_t t$ nichttrivial $\implies T$ linear abhängig $\lightning$, also S linear unabhängig. ■

Definition 5, § 8

Eine geordnete Menge $(M, \prec)$ heißt ***induktiv geordnet*** $: \iff \forall N \subseteq M, (N, \prec)$ *ist totalgeordnet und es gilt $\exists m \in M : n \prec m \; \forall n \in N$, d.h. m ist* ***größtes Element*** *für N.*

Satz A (*Zorn'sches Lemma*)

Jede nichtleere induktiv geordnete Menge M besitzt eine ***obere Schranke*** *m, d.h. $\forall n \in M : m \succ n \implies m = n$.*

Ohne Beweis, mengentheoretische Aussage äquivalent zum Auswahlaxiom[2]. Wende an für:

Satz 8, § 8

Jeder Vektorraum hat eine Basis.

Beweis mit Zorn'schem Lemma : Wir zeigen zunächst $0 \neq V$ K-Vektorraum, $T \subseteq V$ linear unabhängig, $S \subseteq V$ Erzeugendensystem $\implies \exists S' \subseteq S \backslash T : T \cup S'$ Basis von V.

Sei $M := \{S' \subseteq S \,|\, T \cup S' \text{ l.u.}\} \neq \varnothing$, sonst:

T Basis: Sonst $\forall s \in S : T \cup \{s\}$ l.a. $\implies s = \sum'_{t\in T} a_t t \implies v \in V, v = \sum'_{s\in S} a_s s = \sum'_{s\in S} a_s \left(\sum'_{t\in T} a_t t\right) = \sum'_{t\in T} \left(\sum'_{s\in S} a_s a_t\right) t \implies T$ Erzeugendensystem.

Zeige: M induktiv geordnet bezüglich $\subseteq$.

Sei $\{S_i\}_{i\in I}$ eine totalgeordnete Teilmenge von M. Setze $\tilde{S} = \bigcup_{i\in I} S_i \subseteq S$.

zu Zeigen: $T \cup \tilde{S}$ lienar unabhängig. Sei also $A \subseteq T \cup \tilde{S}$ endlich, $A = \{s_1, \ldots, s_n\} \implies \forall j = 1, \ldots, n \; \exists i(j) \in I : s_i \in T \cup S_{i(j)} : \{S_i\}_{i\in I}$ totalgeordnet für $i, j \in I : S_i \subseteq S_j \wedge S_j \subseteq S_i \implies \exists k \in I : s_j \in S_k \cup T \; \forall j = 1, \ldots, n \implies A \subseteq T \cup S_k$ linear unabhängig $\implies \tilde{S} \cup T$ l.u., also $\tilde{S} \in M$ und $\forall S_i, i \in I : S_i \subseteq \tilde{S}$, d.h. $\tilde{S}$ maximales Element für $\{S_i\}_{i\in I}$.

[2] https://de.wikibooks.org/wiki/Beweisarchiv:_Mengenlehre:_Lemma_von_Zorn

Zorn $\Longrightarrow \exists S' \in M : S'$ obere Schranke, d.h. $S' \cup T$ ist l.u..

Behauptung: $S' \cup T$ ist Basis. Sonst: Sei $s \in S \backslash T \Longrightarrow S' \cup \{s\} \cup T$ ist l.a., da sonst $S' \subseteq S' \cup \{s\} \in M \lightning$ zu S' obere Schranke.

$\Longrightarrow \forall s \in S : s = \sum'_{t \in T \cup S'} a_t t \Longrightarrow v \in V, v = \sum'_{s \in S} a_s s = \sum'_{t \in T \cup S'} c_t t$ (vgl. vorherige Rechnung).
$\Longrightarrow S' \cup T$ ist Erzeugendensystem, also Basis.

Wende dies an für $T = \varnothing, S = V \Longrightarrow V$ hat eine Basis. ■

Anmerkung

Ist V nicht endlich erzeugt, d.h. $\dim V = \infty$, so gitl der Isomorphiesatz im allgemeinen nicht!

§ 9. Koordinatendarstellung

9.1. Koordinaten und Basiswechsel

Definition 1, § 9

K Körper, V K-Vektorraum der Dimension n, $S = \{s_1, \ldots, s_n\}$ Basis, $v \in V \Longrightarrow \exists! a_j \in K$:

$$v = \sum_{j=1}^{n} a_j s_j$$

*a_j heißt **Koordinate** von v bezüglich der geordneten Basis S.*

$$v_s = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \in K^n$$

Koordinatenvektor von v bezüglich S.
*$\gamma_S : V \to K^n, v \mapsto \gamma_S(v) = v_S$ heißt **Koordinatendarstellung von V bezüglich S.***

Anmerkung 1, § 9

γ_S ist ein Isomorphismus von K-Vektorräumen: V, K^n haben gleiche Dimension, γ_s ist injektiv (da $\gamma_S(0) = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \Longrightarrow v = \sum_{j=1}^{n} 0s \Longrightarrow v = 0 \Longrightarrow \ker \gamma_S = 0$)

$\Longrightarrow \gamma_S$ surjektiv.

Bemerkung 1, § 9

V K-Vektorraum, $\dim V = n, S = \{s_1, \ldots, s_n\}, T = \{t_1, \ldots, t_n\}$ Basen von $V \Longrightarrow$

a)

$$\exists!\, c_{ij} \in K, \quad i,k = 1,\dots,n : s_j = \sum_{i=1}^{n} c_{ij} t_i \wedge \exists! d_{ij} \in K : t_j = \sum_{i=1}^{n} d_{ij} s_i$$

b) $v_S = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}, v_T = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \Longrightarrow \forall i = 1,\dots,n : b_i = \sum_{j=1}^{n} c_{ij} a_j \wedge a_i = \sum_{j=1}^{n} d_{ij} b_j$

c)

$$\sum_{j=1}^{n} c_{ij} d_{jk} = \delta_{ik} = \sum_{j=1}^{n} d_{ij} c_{jk}, \quad i,k = 1,\dots,n$$

wobei das Kronecker-Delta ist definiert als:

$$\delta_{ik} := \begin{cases} 1 & \text{wenn } i = k \\ 0 & \text{sonst} \end{cases}$$

Beweis : a) klar

b) [3]

$$v = \sum_j a_j s_j, \quad s_j = \sum_i c_{ij} t_i \Longrightarrow v = \sum_j a_j \left(\sum_i c_{ij} t_i \right) = \sum_i \left(\sum_j c_{ij} a_j \right) t_1 = \sum_i b_i t_i$$

$$t_j = \sum_i d_{ij} s_i, v = \sum_j b_j t_j = \sum_j b_j \left(\sum_i \mathrm{d}_{ij} s_i \right) = \sum_i \left(\sum_j d_{ij} b_j \right)$$

.

c) $s_k = \sum_j c_{ik} t_j, \quad t_j = \sum_i s_{ij} s_i \Longrightarrow s_k = \sum_j c_{jk} \left(\sum_i d_{ij} s_i \right) = \sum_i \left(\sum_j d_{ij} c_{jk} \right) s_i \Longrightarrow$ Beh. Analog die andere Behauptung. ■

[3] Ihr müsst jetzt damit leben, dass diese Mitschrift von einem Physiker geschrieben wird, der viel zu wenig Zeit hierfür hat und deswegen Summationsgrenzen oft weglässt, wenn sie aus dem Kontext eindeutig sind. Gemeint ist meist eine Summe von 1 bis n, wobei n die Dimension des Raumes ist, in dem wir gerade rechnen.

Definition 2, § 9

$\gamma_s \colon V \xrightarrow{\sim} K^n, n = \dim V, S = \{s_1, \ldots, s_n\}, T = \{t_1, \ldots, t_n\}$ *Basen von* V, $s_j = \sum c_{ij} t_i,\ t_j = \sum d_{ij} s_i,\ c_{ij}, d_{ij} \in K$.

$$\begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & \cdots & \cdots & c_{nn} \end{pmatrix} =: (c_{ij})_{\substack{i=1,\ldots,n \\ j=1,\ldots,n}} =: C_T^S \tag{II.23}$$

heißt ***Basiswechselmatrix von S nach T***
$C_S^T = (d_{ij})$ *analog Basiswechselmatrix von T nach S.*

$$K^{m \times n} := \{A = (a_{ij})_{\substack{i=1,\ldots,m \\ j=1,\ldots,n}} | a_{ij} \in K\} \cong K^{m \cdot n}$$

heißt ***Vektorraum der*** $m \times n$***-Matrizen*** *(mit punktweise Addition und skalaren Multiplikation).*
Matrizenprodukt: $K^{l\times m} \times K^{m\times n} \to K^{l\times n}$

$$A = (a_{ij})_{\substack{i=1,\dots,l\\ j=1,\dots,m}}, \quad B = (n_{ij})_{\substack{i=1,\dots,m\\ j=1,\dots,n}}$$

$$A \cdot B := \left(\sum_{j=1}^{m} a_{ij} b_{jk}\right)_{\substack{i=1,\dots,l\\ k=1,\dots,n}}$$

Beispiel:

$$\begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 & 1 \\ 1 & 3 & 0 \end{pmatrix} = \begin{pmatrix} 4 & 6 & 1 \\ 7 & 9 & 2 \end{pmatrix} \tag{II.24}$$

Kurzschreibweise Bem. 1 mit Matrizenprodukt

a) $T \in K^{1\times n}, S \in K^{1\times n} \implies T = S \cdot C_S^T$ und T, S als Zeilenvektor (d.h. $T = (t_1, \dots, t_n)$).

b) v_T als Spaltenvektor, $v_T = C_T^S \cdot v_S, \quad v_S = C_S^T \cdot v_T$, insbesondere: $S \cdot v_S = S C_S^T v_T = T v_T$

c) $C_T^S C_S^T = C_S^T C_T^S = (\delta_{ij}) =: I_n$.

9.2. Die Matrix einer linearen Abbildung

Definition 3, § 9

V, W, endlich erzeugte K-Vektorräume mit Basen $S = \{s_1, \dots, s_n\}$ *bzw.* $T = \{t_1, \dots, t_m\}$, $n = \dim V$, $m = \dim W$
$\Phi \in \mathrm{Hom}(V, W) \implies \exists! d_{ij} \in K,\ i = 1, \dots, m,\ j = 1, \dots, n : \Phi(s_j) = \sum_{i=1}^{m} d_{ij} t_i$

$$D_T^S(\Phi) := (d_{ij}) \in K^{m\times n}$$

heißt ***Darstellungsmatrix*** *von* Φ *bezüglich* S *und* T.

Anmerkung 2, § 9

$$C_T^S = D_T^S(\mathrm{id}_V)$$

Bemerkung 2, § 9

V, W endlich-dimensionale K-Vektorräume, $\Phi\colon V \to W$ *linear.* $v \in V, v_S := \gamma_S(v) \in K^n, w_T := \gamma_T(\Phi(v))$,

$$w_t = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}, v_s = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \implies b_i = \sum_{j=1}^{n} d_{ij} a_j \quad \forall i = 1, \vdots, n$$

oder kurz

$$w_T = D_T^S(\Phi) \cdot v_S$$

$$\begin{array}{ccc} V & \xrightarrow{\Phi} & W \\ {\scriptstyle \gamma_S}\downarrow & & \downarrow{\scriptstyle \gamma_T} \\ K^n & \xrightarrow[D_T^S(\Phi)]{} & K^m \end{array}$$

Beweis: $\Phi(v) = \sum_j a_j \Phi(s_j) = \sum_j^n a_j \left(\sum_i^m d_{ij} t_i\right) = \sum_i^m \left(\sum_j^n d_{ij} a_j\right) t_i$ ■

Satz 1, § 9

V, W endlich-dimensionale K-Vektorräume, $S = \{s_1, \ldots, s_n\}$ Basis von V bzw. $T = \{t_1, \ldots, t_m\}$ Basis von W $\Longrightarrow$ $D_T^S : \mathrm{Hom}(V,W) \to K^{m\times n}, \Phi \mapsto D_T^S(\Phi)$ ist Vektorraumisomorphismus.

Beweis: Seien $\Phi, \Psi \in \mathrm{Hom}(V,W)$. $\Phi(s_j) = \sum_i^m d_{ij} d_{ij} t_i, \Psi(s_j) = \sum_i^m f_{ij} t_i, d_{ij}, f_{ij} \in K$.

$$\Longrightarrow (\Phi + \Psi)(s_j) = \Phi(s_j) + \Psi(s_j) = \sum_i^m (d_{ij} + d_{ij}) t_i$$

$$\Longrightarrow D_T^S(\Phi + \Psi) = (d_{ij} + f_{ij})_{i,j})(d_{ij})_{i,j} + (f_{i,j})_{i,j} = D_T^S(\Phi) + D_T^S(\Psi)$$

Sei $a \in K : D_T^S(a\Phi) = (a d_{ij})_{i,j} = a(d_{ij})_{i,j} = a D_T^S(\Phi) \Longrightarrow D_T^S$ ist linear.

Ist $A \in K^{m\times n}, A = (a_{ij}) \Longrightarrow \exists! \Phi \in \mathrm{Hom}(V,W) : \phi(s_j) = \sum_i^m a_{ij} t_i \Longrightarrow D_T^S(\Phi) = A \Longrightarrow$ surjektiv.

Ist $D_T^S(\Phi) = D_T^S(\Psi)$, so $\forall j = 1, \ldots, n : \Phi(s_j) = \sum_i^m d_{ij} t_i = \Psi(s_j) \overset{\text{§8 S4 ?}}{\Longrightarrow} \overset{\Phi=\Psi}{\Longrightarrow}$ injektiv. ■

Folgerung 1, § 9

$$\dim \mathrm{Hom}(V,W) = mn$$

Beweis: $K^{m\times n} \cong K^{mn} \Longrightarrow \dim \mathrm{Hom}(V,W) = \dim K^{m\times n} = \dim K^{mn} = mn.$ ■

9.3. Das Matrixprodukt

Satz 2, § 9

V, W, X endlich-dimensionale K-Vektorräume mit Basen S bzw. T bzw. U respektive mit $\dim V = n, \dim W = m, \dim X = l$. Seien $\Phi\colon V \to W$ und $\Psi\colon W \to X$ linear.

$$\Longrightarrow D_U^S(\Psi \circ \Phi) = D_U^T(\Psi) \cdot D_T^S(\Phi)$$

.

Beweis: $\Phi(s_k) = \sum_j^m d_{ik} t_j,\ \Psi(t_j) = \sum_i^l f_{ik} u_i \Longrightarrow (\Psi\circ\Phi)(s_k) = \Psi(\sum_j^m d_{jk} t_j) = \sum_j^m d_{jk} \left(\sum_i^l f_{ij} u_i\right) = \sum_i^l \left(\sum_j^m f_{ij} d_{jk}\right) u_i$ ■

Folgerung 2, § 9

V, W wie oben, mit Basen S, S' auf V bzw. T, T' auf W, $\Phi\colon V \to W \implies$

$$D_{T'}^{S'}(\Phi) = C_{T'}^{T} D_T^S(\Phi) C_S^{S'}$$

Beweis: $C_{T'}^{T} \cdot D_T^S(\Phi) C_S^{S'} = D_{T'}^{T}(\mathrm{id}_W) D_T^S(\Phi) D_S^{S'}(\mathrm{id}_V) = D_{T'}^{S'}(\mathrm{id}_W \circ \Phi \circ \mathrm{id}_V) = D_{T'}^{S'}(\Phi)$ ■

Satz 3, § 9

a) *Der K-Vektorraum der $n \times n$-Matrizen bildet mit dem Matrizenprodukt eine K-Algebra mit der Nullamtrix als Nullelement und* $I_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ *als Einselement.*

b) *Die Teilmenge der invertierbaren Matrizen (d.h. zu $A \in K^{n\times n} \exists A^{-1} : AA^{-1} = I_n$) bildet mit dem Matrizenprodukt eine Gruppe, genannt $\mathrm{Gl}_n(K)$.*

Beweis: 1. Vorgehensweise klar, Beispiel Distributivität.

Sei $A, B, C \in K^{n\times n}. A = D_S(\Phi), B = D_S(\Psi), C = D_S(\rho), \Phi, \Psi, \rho \in \mathrm{End}\, V$.

$$A(B+C) = D_S(\Phi)(D_S(\Psi) + D_S(\rho)) = D_S(\Phi)(D_S(\Psi+\rho)) = D_S(\Phi \circ (\Psi+\rho)) \quad \text{(II.25)}$$
$$= D_S(\Phi\circ\Psi + \Phi\circ\rho) = \cdots = D_S(\Phi)D_S(\Psi) + D_S(\Phi)D_S(\rho) = AB + AC \quad \text{(II.26)}$$

Sei V K-Vektorraum der Dimension n, $S = \{s_1, \ldots s_n\}$ eine Basis $\implies$ $D_S\colon \mathrm{End}\, V \to K^{n\times n}, \Phi \mapsto D_S(\Phi) := D_S^S(\Phi)$ ist Vektorraum Isomorphismus. $\forall \Phi, \Psi \in \mathrm{End}\, V : D_S(\Psi \circ \Phi) = D_S(\Psi) C_S(\Phi) \implies K^{n\times n}$ ist K-Algebra mit Matrixprodukt durch „Vererbung“ der K-Algebrastruktur auf $\mathrm{End}\, V$.

2. $\mathrm{Gl}_n(K) = \{A \in K^{n\times n} | A \text{ invertierbar}\} \cong \{\Phi \in \mathrm{End}\, V | \exists \Psi \in \mathrm{End}\, V : \Phi \circ \Psi = \mathrm{id}_V\} = \mathrm{Gl}(V)$ ist Gruppe. ■

9.4. Rang und Äquivalenz einer Matrix

Frage: Sei $\Phi\colon V \to W$ linear von endlich-dimensionalen K-Vektorräumen. Existieren S, T Basen von V, W, sodass $D_T^S(\Phi)$ „möglichst einfache Gestalt“ hat?

Definition 4, § 9

*K Körper, $A, B \in K^{m\times n}$ heißen **äquivalent** $: \iff \exists C \in \mathrm{Gl}_m(K),\ D \in \mathrm{Gl}_n(K)$ mit $B = CAD$. Schreibe $B \sim A$.*
*$A, B \in K^{n\times n}$ heißen **ähnlich** $: \iff \exists C \in \mathrm{Gl}_n(K) : B = C^{-1}AC$, schreibe $B \approx A$.*

Anmerkung

$\sim$ und $\approx$ definieren Äquivalenzrelationen auf $K^{m\times n}$ bzw. $K^{n\times n}$.

Definition 5, § 9

K Körper, $A \in K^{m\times n}$. Die Dimension des von den Spalten der Matrix aufgespannten Unterraums von K^m heißt der ***(Spalten-)rang*** $\operatorname{Rang} A$.
Analog heißt die Dimension des von den Zeilen von A aufgespannten Unterraums von K^n ***Zeilenrang***.

Anmerkung

Wenn $A = D_T^S(\Phi); S \subseteq V \xrightarrow{\Phi} W \supseteq T$ (multipl. Spaltenvektor aus K^n an A um lineare Abbildung $A : K^n \to K^m$ zu erhalten). Damit: $\operatorname{Rang}\Phi = \dim\Phi(V) = \dim\gamma_T(\Phi(V)) = \dim A(\gamma_S(V)) = \dim A(K^n) = \operatorname{Rang} A$ *(mit Standardbasen).*

$$\begin{array}{ccc} V & \xrightarrow{\Phi} & W \\ {\scriptstyle\gamma_S}\downarrow{\scriptstyle S} & & {\scriptstyle S}\downarrow{\scriptstyle\gamma_T} \\ K^n & \xrightarrow{A} & K^m \end{array}$$

Elementarmatrizen Multipliziere folgende Matrizen von links (bzw. von rechts) an eine gegebene Matrix $A \in K^{m\times n}$ um folgende Operationen durchzuführen:

(Z1) (bzw. (S1)) Vertausche Zeilen (Spalten) i und j:

$$V_{ij} = \begin{pmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 1 & & & & & & \\ & & & 0 & & & 1 & & \\ & & & & 1 & & & & \\ & & & & & \ddots & & & \\ & & & & & & 1 & & \\ & & & 1 & & & & 0 & \\ & & & & & & & & 1 \\ & & & & & & & \ddots & \\ & & & & & & & & 1 \end{pmatrix} \tag{II.27}$$

wobei sich die beiden 1en außerhalb der Diagonale in Zeile an den Positionen i, j und j, i befinden, die Nuller in der Dialgonalen bei i, i und j, j.

(Z2) (bzw. (S2)) Addiere zu Zeile i (bzw. zu Spalte j) das a-fache ($a \in K$) von j (bzw. i):

$$A_{ij}(a) = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & \ddots & & & \\ & & a & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} \tag{II.28}$$

wobei sich das a an der Position i, j befindet.

(Z2) (bzw. (S2)) Multipliziere eine Zeile i (bzw. Spalte j) mit $a \in K$:

$$M_i(a) = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & a & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix} \tag{II.29}$$

wobei sich das a an der Position i, j befindet.

Wir haben $V_{ij} \in \mathrm{Gl}_m(K)$ (bzw. $\mathrm{Gl}_n(K)$), da $V_{ij} \cdot V_{ij} = I_m$ (bzw. I_n).
$A_{ij}(a) \in \mathrm{Gl}_m(K)$ (bzw. $\mathrm{Gl}_n(K)$), da $A_{ij}(a) \cdot A_{ij}(-a) = I_m$ (bzw. I_n).
$M_i(a) \in \mathrm{Gl}_m(K)$ (bzw. $\mathrm{Gl}_n(K)$) für $a \neq 0$, da $M_i(a) \cdot M_i(a^{-1}) = I_m$ (bzw. I_n).

Bemerkung 3, § 9 (*Elementare Umformungen*)

Der Rang einer Matrix ändert sich nicht, wenn einer der Operationen (Z1) bis (Z3) (bzw. (S1)-(S3)) durchgeführt wird.

Beweis: Klar, da $V_{ij}, A_{ij}(a)$ und $M_i(a)$ ($a \neq 0$) $\in \mathrm{Gl}_m(K)$ (bzw. $\mathrm{Gl}_n(K)$) und isomorphe Räume die gleiche Dimension haben (vgl. vorige Anmerkung). ■

Satz 4, § 9

K Körper, $A \in K^{m\times n}$ $\Longrightarrow$

$$A \sim \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix} =: A_r \tag{II.30}$$

wobei $r = \operatorname{Rang} A$ eindeutig bestimmt ist. r bezeichnet die Anzahl der Zeilen und Spalten, die der Einheitsmatrix entsprechen.

Zusatz: A_r heißt Rangnormalform zu A. Sie kann in endlich vielen Schritten durch elementare Zeilen- bzw. Spaltenumformungen erreicht werden.

Beweis: Eindeutigkeit Angenommen $A_r \sim A_{r'}$ für $r \neq r' \implies A - r = DA_{r'}C \implies r = \operatorname{Rang} A_r = \operatorname{Rang} DA_{r'}C = \operatorname{Rang} A_{r'} = r' \lightning$.

Existenz Man geht nach folgendem Algorithmus vor:

1. $A = 0 \to$ fertig.
2. $A \neq 0 : \exists i, j : a_{ij} \neq a \implies$ vertausche Zeilen $1, i$ und Spalten $1, j \implies a_{11} \neq 0$.
3. Dividiere 1. Zeile durch a.
4. Anulliere $a_{i,1}$ für $i > 1$ durch Subtrahieren von a_{i1} (Zeile 1).
5. Annulliere a_{ij}, $j > 1$ durch Subtrahieren von a_{1j} (Spalte 1).
6. Ersetze A durch die Matrix, die durch Streichen der ersten Zeile und ersten Spalte entsteht und gehe zu Schritt 1. ■

Beispiel

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & -6 & -12 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & -6 \\ 0 & -6 & -12 \end{pmatrix} \tag{II.31}$$

$$\sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & -6 & -12 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix} \tag{II.32}$$

$$\sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} = A_2 \tag{II.33}$$

$$\implies \operatorname{Rang} A = 2 \tag{II.34}$$

§ 10. Lineare Gleichungssysteme

10.1. Hauptsatz über lineare Gleichungssysteme

Satz 1, § 10

K Körper, $A \in K^{m \times n}$, $y \in K^m$.

a) $\exists x \in K^n : A \cdot x = y \iff \operatorname{Rang} A = \operatorname{Rang}(A \vdots y)$ *mit*

$$(A \vdots y) = \begin{pmatrix} a_{11} & & & y_1 \\ & \ddots & & \vdots \\ & & a_{mn} & y_m \end{pmatrix} \tag{II.35}$$

b) $y = 0 \implies L_0 := \{x \in K^n | Ax = 0\} < K^n$ *ist Unterraum der Dimension* $n - \operatorname{Rang} A$.

c) $y \neq 0 \implies L_y := \{x \in K^n | Ax = y\} \implies L_y = x_0 + L_0$, *wobei* $x_0 \in L_y$, *d.h.* $L_y \in K^n/_{L_0}$.

Beweis: V, W K-Vektorräume mit Basen $S = \{s_1, \ldots, s_n\}$ bzw. $T = \{t_1, \ldots, t_m\}$ von V bzw. W. $\overset{\text{§8, S4?}}{\implies} \exists! \Phi \in \operatorname{Hom}(V, W) : D_T^S(\Phi) = A$.

a) $x = \gamma_S(v) = v_S$, $y = \gamma_T(w) = w_T$ für $v \in V, w \in W$. $\implies Ax = y$ lösbar $\iff w \in \Phi(V) = \langle \Phi(s_1), \ldots, \Phi(s_n) \rangle \iff w_t = y \in \langle \Phi(s_1)_T, \ldots, \Phi(s_n)_T \rangle \iff \operatorname{Rang}\langle \Phi(s_1)_T, \ldots, \Phi(s_n)_T \rangle = \operatorname{Rang}\langle \Phi(s_1)_T, \ldots, \Phi(s_n)_T, y \rangle$, d.h. $\operatorname{Rang}(A|y) = \operatorname{Rang} A$.

b) $y = 0 \implies L - 0 \leqslant K^n$ nach §6, Bsp. 1?.

$\dim L_0 = \dim \ker \Phi = n - \dim \Phi(V) = n - \operatorname{Rang} A$

c) $y \neq 0 : x_0 \in L_y \iff x \in L_y \iff x - x_0 \in L_0 \iff x \in x_0 + L_0$ ■

Beispiel

$$(A|y) = \begin{pmatrix} 1 & 2 & 3 & 1 \\ 4 & 5 & 6 & 1 \\ 7 & 8 & 9 & 1 \end{pmatrix} \overset{\text{Schritte wie oben}}{\sim} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{II.36}$$

$$\implies \operatorname{Rang}(A|y) = \operatorname{Rang} A \implies Ax = y \text{ lösbar und } \dim L_0 = 3 - \operatorname{Rang} A = 1 \tag{II.37}$$

Frage Berechnung von L_y?

10.2. Der Gauß-Algorithmus

Vorbemerkung: K Körper, $A \in K^{m \times n}$. Dann $Ax = y \iff \forall C \in \mathrm{Gl}_m(K) : CAx = Cy$.

Satz 2, § 10

K Körper, $A \in K^{m \times n}$ *kann durch endlich viele Zeilenumformungen (Z1)-(Z3) auf* ***Stufennormalform*** *gebracht werden, d.h. eine Matrix der Form* $\hat{A}$*:*

$$\hat{A} = \begin{pmatrix}
0 & \cdots & 0 & 1 & & 0 & * & \cdots & * & 0 & \cdots & 0 & & & & & * & \cdots & * & 0 & \cdots & 0 \\
\vdots & \ddots & \vdots & & \ddots & & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & & & & & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
\vdots & & \vdots & 0 & & 1 & * & \cdots & * & 0 & \cdots & 0 & & & & & \vdots & & \vdots & \vdots & & \vdots \\
\vdots & & \vdots & 0 & \cdots & 0 & 0 & \cdots & 0 & 1 & & 0 & & & & & \vdots & & \vdots & \vdots & & \vdots \\
\vdots & & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & & \ddots & & & & & & \vdots & & \vdots & \vdots & & \vdots \\
\vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & 0 & & 1 & & & & & \vdots & & \vdots & \vdots & & \vdots \\
\vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & 0 & \cdots & 0 & \cdots & & & & \vdots & & \vdots & \vdots & & \vdots \\
\vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & & 1 & & 0 & \vdots & & \vdots & \vdots & & \vdots \\
\vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & & & \ddots & & \vdots & & \vdots & \vdots & & \vdots \\
\vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & & 0 & & 1 & * & \cdots & * & \vdots & & \vdots \\
\vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & & 0 & \cdots & 0 & 0 & \cdots & 0 & \vdots & & \vdots \\
\vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & & \vdots \\
0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0
\end{pmatrix} \tag{II.38}$$

Beweis Gauß-Algorithmus : Durch Induktion nach Anzahl der Spalten j für die die SNF erreicht werden soll.

Induktionsanfang: $j = 0$ klar.

Induktionsschritt: SNF erreicht für die ersten $(j-1)$ Spalten. Definiere $i(j-1)$ als den größten Index einer Zeile mit $a_{i(j-1),j-1} \in \{1, *\}$ bzw. $j = 1 \implies i(0) = 0$.

1. Fall $\forall i > i(j-1) : a_{ij} = 0 \implies$ SNF erreicht für Spalte j.

2. Fall $\exists j > i(j-1) : a_{ij} \neq 0$

1. (Z1): Vertausche Zeilen $i(j) = i(j-1) + 1$
2. (Z3): Dividiere Zeile $i(j)$ durch $a_{i(j),j}$
3. (Z2): Für $i \neq i(j)$: Subtrahiere von Zeile i das a_{ij}-fache von Zeile $i(j) \implies \forall i \neq i(j), a_{ij} = 0$.

Spalte j in SNF. ■

Folgerung 1, § 10

Gegeben sei LGS $Ax = y$ über einem Körper K, $A \in K^{m\times n}, y \in K^{m\times 1}$. Sei $(\hat{A}\vdots\hat{y})$ die SNF zu $(A\vdots y)$. Dann gelten:

a) $Ax = y$ ist unlösbar $\iff$ $\hat{y}$ hat eine führende 1.

b) $\hat{y}$ hat keine führende 1 $\implies$ eine spezielle Lösung ist gegeben durch

$$x_0 = \begin{pmatrix} x_1 \\ \vdots \\ x_0 \end{pmatrix}, \quad x_j = \begin{cases} \hat{y}_i & \text{falls } j = j(i) \\ 0 & \text{sonst} \end{cases}$$

wobei $j(i)$ der kleinste Index einer Spalte ist, sodass $a_{1,j(i)} = 1$, sonst $j(i) = 0$.

c) $L_0 = \langle z^{(j)} \in K^{n\times 1} | i(j) = i(j-1)\rangle$ *(*-Spalten) mit*

$$z_k^{(j)} = \begin{cases} -1 & k = j \\ \hat{a}_{ij} & k = j(i) \\ 0 & \text{sonst} \end{cases}$$

Beweis: a) $(\hat{A}\vdots\hat{y})$ hat führende 1 $\iff$ $(\hat{A}\vdots\hat{y}) = \begin{pmatrix} * & \cdots & * & 0 \\ \vdots & \ddots & \vdots & \vdots \\ * & \cdots & * & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix} \implies \operatorname{Rang}(\hat{A}\vdots\hat{y}) > \operatorname{Rang}\hat{A} \implies$

$\operatorname{Rang}(A\vdots y) > \operatorname{Rang} A \implies$ LGS unlösbar.

b)

$$\forall i \in 1,\dots,m : \sum_{j=1}^{n} \hat{a}_{ij}x_j = \hat{a}_{ij(i)}\hat{y}_i = \hat{y}_i \implies \hat{A}x_0 = \hat{y}$$

c) $\forall j \forall i = 1,\dots,m : \sum_{k=1}^{n} \hat{a}_{ik}z_k^{(j)} = -\hat{a}_{ij} - \hat{a}_{ij(i)} = 0 \implies \forall j : z^{(j)}$ Lösung des hom. Systems und $-1 = z_j^{(j)} \neq 0 \wedge z_i^{(j)} = 0 \forall i > j \implies z^{(j)}$ linear unabhängig, $\#\{j | i(j) = i(j-1)\} = n - \operatorname{Rang} A = \dim L_0 \implies L_0 = \langle z^{(j)}\rangle$. ∎

Beispiel:

$$\left(\begin{array}{ccccc|c} 1 & 0 & u & 0 & w & a \\ 0 & 1 & v & 0 & x & b \\ 0 & 0 & 0 & 1 & y & c \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right) \implies \hat{A} \cdot \begin{pmatrix} a \\ b \\ 0 \\ c \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ b \\ c \\ 0 \end{pmatrix} \tag{II.39}$$

$$\hat{A} \cdot \begin{pmatrix} u & v & -1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} u-u \\ v-v \\ 0 \\ 0 \end{pmatrix} = 0 \quad \hat{A} \begin{pmatrix} w \\ x \\ 0 \\ y \\ -1 \end{pmatrix} = \begin{pmatrix} w-w \\ x-x \\ y-y \\ 0 \end{pmatrix} = 0 \tag{II.40}$$

10.3. Anwendung auf die allgemeine lineare Gruppe

Satz 3, § 10

Jede Matrix aus $\mathrm{Gl}_n(K)$ kann als endliches Produkt von Elementarmatrizen dargestellt werden.

Beweis: $A \in \mathrm{Gl}_n(K) \implies \mathrm{SNF}\ \hat{A} = I_n$ (sonst $\lightning$ zu $\operatorname{Rang} A = n$) $\implies \exists X \in \mathrm{Gl}_n(K)$, Produkt von Elementarmatrizen mit $XA = I_n, X^{-1} = A$, aber X^{-1} auch Produkt von Elementarmatrizen. ∎

Folgerung 2, § 10

Das Inverse einer Matrix $A \in \mathrm{Gl}_n(K)$ lässt sich mit dem Gauß-Algorithmus berechnen.

Beweis : Betrachte $C(A\vdots I_n) \sim (I_n\vdots C) \implies C = A^{-1}$. ■

Beispiel: Das Inverse zu $A = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}$:

$$\left(\begin{array}{cc|cc} 1 & 2 & 1 & \\ 3 & 5 & & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 0 & -1 & -3 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 0 & -5 & 2 \\ 0 & 1 & 3 & -1 \end{array}\right) \implies A^{-1} = \begin{pmatrix} 5 & 2 \\ 3 & 1 \end{pmatrix} \tag{II.41}$$

III. Lineare Operatoren

§ 11. Linearformen

11.1. Dualraum

Definition 1, § 11

*V K-Vektorraum. $V^* := \mathrm{Hom}(V, K)$ heißt **Dualraum** zu V, $f \in V^*$ heißt **Linearform**.*

Satz 1, § 11

V sei endlich-dimensionaler K-Vektorraum, $S = \{s_1, \ldots, s_n\}$ sei Basis von V, V^* Dualraum zu V $\Longrightarrow$

a) $\dim(V^*) = \dim V$

b) $T = \{t_1, \ldots t_n\}$ *mit* $t_i(s_j) = \delta_{ij}$ *bildet Basis von* V^*.

Beweis: Es reicht, b zu zeigen.

§8 Satz 4(?) $\Longrightarrow \forall i = 1, \ldots, n \exists! t_i \in V^* : t_i(s_j) = \delta_{ij}$.

Angenommen, $\sum_{i=1}^n a_i t_i = 0$ zu $V^* \Longrightarrow \forall j = 1, \ldots, n.\ 0 = \sum_{i=1}^n a_i t_i(s_j) = a_j \Longrightarrow t_1, \ldots, t_n$ linear unabhängig. Ist $f \in V^* \Longrightarrow \forall j \exists a_j \in K : f(s_j) = a_j$. Sei $\tilde{f} := \sum_{i=1}^n a_i t_i \in V^* \Longrightarrow \tilde{f}(s_j) = \sum_{i=1}^n a_i t_i(s_j) = a_j = f(s_j) \Longrightarrow \tilde{f} = f \Longrightarrow T$ Erzeugendensystem, d.h. Basis. ■

Bezeichung: $S^* := T$ heißt duale Basis zu S.

Anmerkung 1, § 11

Der Isomorphismus $V \to V^*, s_i \mapsto t_i$ ist über S definiert.

11.2. Der Dualitätssatz

V endlich-dimensionaler K-Vektorraum.

Satz 2, § 11

Die Abbildung $\Theta\colon V \to (V^*)^*, v \mapsto \Theta(v) =: \Theta_v$ mit $\Theta_v(f) := f(v)$ ist „natürlicher" Isomorphismus von V nach V^{**}.

Beweis: $\dim(V^*)^* = \dim V^* = \dim V$. Es reicht zu zeigen, dass Θ eine injektive lineare Abbildung ist (daraus folgt bereits surjektivität). Θ linear:

$\forall f \in V^*, v, w \in V : \Theta_{v+w}(f) = f(v+w) = f(v) + f(w) = \Theta_v(f) + \Theta_w(f) \implies \Theta_{v+w} = \Theta_v + \Theta_w$.
$\forall a \in K, f \in V^*, v \in V : \Theta_{av}(f) = f(av) = af(v) = a\Theta_v(f) \implies \Theta_{av} = a\Theta_v$. Insgesamt: Θ linear.
Sei $v \in \ker\Theta \implies \Theta(v) = \Theta_v = 0 \implies \forall f \in V^* : \Theta_v(f) = 0 = f(v)$. Angenommen, $v \neq 0 \implies \exists S' \subseteq V.\ S = \{v\} \cup S'$ Basis von V, $S = \{s_1, \ldots, s_n\}, s_i = v_i.S^*$ sei Dualbasis zu S $\implies s_1^*(s_i) = s_1^*(v) = 1 \lightning$ zu $f(v) = 0 \forall f \in V^* \implies v = 0 \implies \ker\Theta = 0 \implies \Theta$ injektiv, also Isomorphismus. ■

Anmerkung 2, § 11

Der Dualitätssatz gilt im allgemeinen nicht für unendlich-dimensionale Räume.

Bezeichnung: $f \in V^*, v \in V \implies \langle f, v\rangle := f(v) \in K$, d.h. $\langle\cdot,\cdot\rangle\colon V^* \times V \to K$

Anmerkung 3, § 11

$\forall v, w \in V,\ f, g \in V^*, a \in K$ *gilt:*

a) $\langle f+g, v\rangle = \langle f, v\rangle + \langle g, v\rangle$
$\langle af, v\rangle = a\langle f, v\rangle$
$\langle f, v+w\rangle = \langle f, v\rangle + \langle f, w\rangle$
$\langle f, av\rangle = a\langle f, v\rangle$

b) $v \in V, \forall f \in V^* : \langle f, v\rangle = 0 \implies v = 0$
$f \in V^*, \forall v \in V : \langle f, v\rangle = 0 \implies f = 0$

d.h. $\langle\cdot,\cdot\rangle$ *ist eine* ***nicht-ausgeartetete*** *((b) gilt)* ***Bilinearform*** *((a) gilt).*

Folgerung 1, § 11

V endlich-dimensionaler K-Vektorraum, $\{t_1, \ldots, t_n\}$ *sei Basis von* $V^* \implies \forall (b_1, \ldots, b_n) \in K^n \exists! v \in V : \langle t_i, v\rangle = b_i$.

Beweis : folgt aus Dualitätssatz: $V \xrightarrow{\sim} V^{**}$ da $t_1 \mapsto b_i \in V^{**}$, d.h. $\exists! v$ mit obiger Eigenschaft. ■

11.3. Das orthogonale Komplement

Definition 2, § 11

V K-Vektorraum. V Dualraum,* $f \in V^*, v \in V$ *heißen* ***zueinander orthogonal*** $(f \perp v)$
$:\iff \langle f, v\rangle = 0$.
Ist $S \subseteq V \implies S^\perp := \{f \in V^* | \langle f, s\rangle = 0 \forall s \in S\}$ *heißt* ***orthogonales Komplement*** *von S.*
Ist $T \subseteq V^* \implies T^\perp := \{v \in V | \langle t, v\rangle = 0 \forall t \in T\}$ *heißt orthogonales Komplement zu T.*

Beispiel (*Das bekannte Skalarprodukt in* $\mathbb{R}^2$)

$V = \mathbb{R}^2, e_1 = \begin{pmatrix}1\\0\end{pmatrix}, e_2 = \begin{pmatrix}0\\1\end{pmatrix}$, *so definiert* $\Phi\colon V \xrightarrow{\sim} V^*,\ e_i \mapsto e_i^*, i = 1,2 \implies V \times V \to V^* \times V \to K,\ (v, w) \mapsto (\Phi(v), w) \mapsto \langle\Phi(v), w\rangle$ *ist bilineare Abbildung* $\langle\cdot,\cdot\rangle_\Phi\colon V \times V \to K$

mit $\left\langle \begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} c \\ d \end{pmatrix} \right\rangle_\Phi = ac + bd$, *d.h.* $e_1 \perp e_2$.

Satz 3, § 11

V endlich-dimensionaler K-Vektorraum, V^* Dualraum $\Longrightarrow$

a) $S \subseteq \tilde{S} \subseteq V \Longrightarrow \tilde{S}^\perp \subseteq S^\perp$ *und* $\langle S \rangle^\perp = S^\perp$

b) $W < V \Longrightarrow \dim W^\perp = \dim V - \dim W$ *und außerdem* $(W^\perp)^\perp = W$.

c) $W_1, W_2 < V \Longrightarrow (W_1 \cap W_2)^\perp = W_1^\perp + W_2^\perp,\ (W_1 + W_2)^\perp = W_1^\perp \cap W_2^\perp$

Beweis: a) $S \subset \tilde{S}, f \in \tilde{S}^\perp \Longrightarrow \langle f, v \rangle = 0 \forall v \in \tilde{S} \Longrightarrow \langle f, v \rangle = 0 \forall v \in S \Longrightarrow f \in S^\perp$

Damit folgt aber wegen $S \subseteq \langle S \rangle$: $\langle S \rangle^\perp \subseteq S^\perp$: Sei $f \in S^\perp$ und $v \in \langle S \rangle$, d.h. $v = \sum'_{s \in S} a_s s, a_s \in K$, d.h. $\langle f, v \rangle = \left\langle f, \sum'_{s \in S} a_s s \right\rangle = \sum'_{s \in S} a_s \underbrace{\langle f, s \rangle}_{=0} = 0 \Longrightarrow f \in \langle S \rangle^\perp$.

b) Sei $T = \{t_1, \ldots, t_n\}$ Basis von $W \overset{\text{Basiserg.}}{\Longrightarrow} V$ hat Basis S.

$S = \{s_1, \ldots, s_n\}$ mit $s_i = t_i$ für $i = 1, \ldots, m$. Sei $S^* = \{s_1^*, \ldots, s_n^*\}$ duale Basis, $f \in V^* \Longrightarrow \exists a_i \in K : f = \sum_{i=1}^n a_i s_i^*$. Dann: $f \in W^\perp \overset{(a)}{\Longleftrightarrow} f \in \{s_1, \ldots, s_m\}^\perp \Longleftrightarrow 0 = \langle f, s_j \rangle = \sum_{i=1}^n a_i \langle s_i^* s_j \rangle = a_j \ \forall j = 1, \ldots, m$.

Anders gesagt: $\Longleftrightarrow f \in \langle s_{m+1}^n, \ldots, s_n^* \rangle = W^\perp = \langle s_{m+1}^*, \ldots, s_n^* \rangle \Longrightarrow \dim W^\perp = \dim V - \dim W$.

$(W^\perp)^\perp) = \{v \in V | \langle f, v \rangle = 0 \ \forall f \in W^\perp\} \supseteq W$ und $\dim(W^\perp)^\perp = \dim V^* - \dim W^\perp = \dim V - \dim V + \dim W = \dim W \Longrightarrow W = (W^\perp)^\perp$.

c) $S^\perp < V^* : f, g \in S^\perp, s \in S$: $\langle f + g, s \rangle = \langle f, s \rangle + \langle g, s \rangle = 0 + 0 = 0,\ a \in K : \langle af, s \rangle = a \langle f, s \rangle = a \cdot 0 = 0$.

$W_1 \cap W_2 \subseteq W_i,\ i = 1, 2 (W_1 \cap W_2)^\perp \supseteq W_i^\perp \Longrightarrow (W_1 \cap W_2)^\perp \overset{(1)}{\supseteq} W_1^\perp + W_2^\perp$

$W_i \subseteq W_1 + W_2,\ i = 1, 2 \Longrightarrow (W_i + W_2)^\perp \subseteq W_i^\perp \Longrightarrow (W_1 + W_2)^\perp \overset{(2)}{\subseteq} W_1^\perp \cap W_2^\perp$.

Setze $V_i := W_i^\perp$, d.h. (1), (2) gelten für V_i und $V_i^\perp = (W_i^\perp)^\perp = W_i$.

$(V_1 \cap V_2)^\perp \supseteq V_1 \perp + V_2^\perp$, d.h. $(W_1^\perp \cap W_2^\perp)^\perp \supseteq W_1 + W_2$, d.h. $W_1^\perp \cap W_2^\perp \subseteq (W_1 + W_2)^\perp$, d.h. „=“ bei (2).

$(V_1 + V_2)^\perp \subseteq V_1^\perp \cap V_2^\perp$, d.h. $(W_1^\perp + W_2^\perp)^\perp \subseteq W_1 \cap W_2$, d.h. $W_1^\perp + W_2^\perp \supseteq (W_1 \cap W_2)^\perp$, d.h. „=“ bei (1). ■

11.4. Die duale lineare Abbildung

Satz 4, § 11

V, W K-Vektorräume, $\Phi \in \mathrm{Hom}(V, W)$. *Dann existiert genau eine lineare Abbildung* $\Phi^* \in \mathrm{Hom}(W^*, V^*)$ *mit* $\langle \Phi^*(g), v \rangle = \langle g, \Phi(v) \rangle \ \forall v \in V, g \in W^*$.

Beweis: $g \in W^*$, Def. $\Phi^*(g) = \Phi_g^* \colon V \to K, v \mapsto \langle g, \Phi(v)\rangle = g(\Phi(v))$. Φ_g^* ist linear aufgrund der Bilinearität der $\langle , \rangle$-Klammer: $(a \in K, v, w \in V)$: $\Phi_g^*(av + w) = \langle g, \Phi(av + w)\rangle = \cdots = a\langle g, \Phi(v)\rangle + \langle g, \Phi(w)\rangle = a\Phi_g^*(v) + \Phi_g^*(w) \implies \Phi_g^* \in V^*$.

$\Phi^* \colon W^* \to V^*$ ist linear: $(g, h \in W^*, a \in K, v \in V) : \Phi^*_{ag+h}(v) = \langle ag + h, \Phi(v)\rangle = a\langle g, \Phi(v)\rangle + \langle h, \Phi(v)\rangle = a\Phi_g^*(v) + \Phi_h^*(v)$, d.h. $\Phi^*(ag + h) = a\Phi^*(g) + \Phi^*(h)$ mit der geforderten Eigenschaft. ■

Definition 3, § 11

*V, W K-Vektorräume, $\Phi \in \mathrm{Hom}(V, W)$, so heißt $\Phi^* \in \mathrm{Hom}(W^*, V^*)$ die **duale lineare Abbildung** bzw. **transponierte Abbildung**.*

Satz 5, § 11

V, W endlich-dimensionale K-Vektorräume, $\Phi \in \mathrm{Hom}(V, W) \implies$

a) $\Phi^*(W^*) = \ker \Phi^\perp, \ker \Phi^* = \Phi(V)^\perp$

b) $\mathrm{Rang}\, \Phi^* = \mathrm{Rang}\, \Phi$. [1]

Beweis: a) $v \in \ker \Phi \overset{\text{Anm 3, § 11}}{\iff} \forall g \in W^* : \langle g, \Phi(v)\rangle = 0 = \langle \Phi^*(g), v\rangle \iff v \in \Phi^*(W^*)^\perp$, d.h. $\ker \Phi^\perp = \Phi^*(W^*)$. ist $g \in \ker \Phi^* \iff \forall v \in V : \langle \Phi^*(g), v\rangle = 0 = \langle g, \Phi(v)\rangle \iff g \in \Phi(V)^\perp$.

b) $\mathrm{Rang}\, \Phi^* = \dim \Phi^*(W^*) \overset{\text{a)}}{=} \dim \ker \Phi^T = \dim V - \dim \ker \phi = \dim \Phi(V) = \mathrm{Rang}\, \Phi$ ■

Folgerung 2, § 11

K Körper, $A = (a_{ij}) = K^{m\times n}$.
*$A^{tr} := (a_{ji}) \in K^{n\times m}$ **transponierte Matrix** $\implies \mathrm{Rang}\, A^{tr} = \mathrm{Rang}\, A$.*

Beweis: $V = K^n, W = K^m$ mit Basen $S = \{s_1, \ldots, s_n\}$ bzw. $T = \{t_1, \ldots, t_n\}$ von V bzw. W. $\implies \exists!\Phi \in \mathrm{Hom}(V, W) : D_T^S(\Phi) = A$.

Seien S^*, T^* die dualen Basen zu S, T. Behauptung: $D_{S^*}^{T^*}(\Phi^*) = A^{tr}$, denn: $\Phi(s_j) = \sum i = 1^m a_{ij}t_i, \Phi^*(t_i^*) = \sum_{j=1}^n b_{ji}s_j^* \implies \langle \Phi^*(t_i^*), s_j\rangle = \begin{cases} \langle t_i^*, \Phi(s_j)\rangle = \sum_{k=1}^n a_{kj} < t_i^*, t_k\rangle \underset{k=i}{=} a_{ij} \\ \sum_{k=1}^n b_{ki}\langle s_k^*, s_j\rangle \underset{k=j}{b}_{ji} \end{cases} \implies a_{ij} = b_{ji}$, d.h. Behauptung.

$\implies \mathrm{Rang}\, A = \mathrm{Rang}\, \Phi \overset{S.5,x11}{=} \mathrm{Rang}\, \Phi^* = \mathrm{Rang}\, A^{tr}$. ■

§ 12. Alternierende Multilinearformen

12.1. Einleitung

Definition 1, § 12

V K-Vektorraum, $m \in \mathbb{N}$, $V^m := \prod_{i=1}^m V = V \times \cdots \times V$ ist K-Vektorraum (komponen-

tenweise) das ***m-fache Produkt von V.***
$f\colon V^m \to K$ *heißt* ***Multilinearform*** $:\iff \forall i = 1,\dots,m : f_i\colon V \to K, v \mapsto f(v_1,\dots,v,\dots,v_m)$,
$v_1,\dots,v_{i-1},v_{i+1},\dots v_m \in V$ *ist linear* ($f \notin (V^m)^*$ *im allgemeinen!)*
Sei $\mathcal{M}_m(V,K)$ *die* ***Menge der m-fachen Multilinearformen.***
$f \in \mathcal{M}_m(V)$ *heißt* ***alternierend*** $:\iff (\forall v_1,\dots,v_m$ *l.a.* $\implies f(v_1,\dots,v_m) = 0)$.
Sei $\mathcal{A}_m(V,K) = \mathcal{A}_m(V)$: ***Menge der alternierenden m-fachen Multilinearformen.***

Anmerkung 1, § 12

$\mathcal{M}_m(V), \mathcal{A}_m(V)$ *sind K-Vektorräume.*

Bemerkung 1, § 12

V K-Vektorraum, $f \in \mathcal{M}_m(V) \implies$

$$f \in \mathcal{A}_m(V) \iff (\forall (v_1,\dots,v_m) \in V^m : \exists i \neq j : v_i = v_j \implies f(v_1,\dots,v_m) = 0)$$

Beweis: „⇒“ $\exists i \neq j : v_i = v_j \implies v_1,\dots,v_m$ l.a. $\implies f(v_1,\dots,v_m) = 0$.

„⇐“ Seien $v_1,\dots,v_m$ linear abhängig $\implies \exists k \in \{1,\dots,m\}$.

$v_k = \sum_{\substack{i=1\\ i\neq k}}^{m} a_i v_i, \quad a_i \in K \implies$

$$f(v_1,\dots,v-m) = f\left(v_1,\dots,\sum_{i\neq k} a_i, v_i,\dots,v_m\right) = \sum_{i\neq k} a_i \underbrace{f(v_1,\dots,v_i,\dots,v_m)}_{=0} = 0$$

$\implies f \in \mathcal{A}_m(V)$. ■

Bemerkung 2, § 12

V K-Vektorraum, $f \in \mathcal{A}_m(V) \implies \forall \sigma \in S_m$ *(bij. Selbstabbildungen von* $\{1,\dots,m\}$*)*
$\forall v_1,\dots,v_m \in V$:

$$f(v_{\sigma(1)},\dots,v_{\sigma(m)}) = \operatorname{sign}\sigma \cdot f(v_1,\dots,v_m)$$

Beweis: Sei $\sigma = \tau = (i\ j) \overset{i<j}{\implies} 0 \overset{\text{B. 1, § 12}}{=} f(v_1,\dots,v_i+v_j,\dots,v_i+v_j,\dots,v_m) = f(v_1,\dots,v_i,\dots,v_j,\dots,v_m) + f(v_1,\dots,v_j,\dots,v_i,\dots,v_m) \implies f(v_{\sigma(1)},\dots,v_{\sigma(m)}) = (-1)\cdot f(v_1,\dots,v_m),\ (-1) = \operatorname{sign}\tau$

Ist $\sigma \in S_m \implies \sigma = \tau_1 \cdots \tau_r$ mit τ_k Transposition.

Induktiv: $f(v_{\sigma(1)},\dots,v_{\sigma(m)}) = (-1)^r f(v_1,\dots,v_m)$ und $(-1)^r = \operatorname{sign}\sigma$ da sign Gruppenhomomorphismus. ■

12.2. $\dim \mathcal{A}_m(V)$

Bemerkung 3, § 12

V K-Vektorraum mit Bais $S = \{s_1,\dots,s_n\}$. $I,J \subseteq \{1,\dots,n\}$ *mit* $\#I = \#J = m$, $J =$

$\{j_1, \ldots, j_m\}$ *mit* $j_1 < \cdots < j_m \implies$

$$\exists t_I \in \mathcal{A}_m(V) : t_I(s_{j1}, \ldots, s_{jm}) = d_{IJ} := \begin{cases} 1, & I = J \\ 0, & I \neq J \end{cases}$$

Beweis: Induktion nach m. Induktionsanfang: $m = 1 \implies \mathcal{A}_1(V) \overset{0\mapsto 0}{\Longrightarrow} \mathcal{M}_1(V) = \mathrm{Hom}(V, K) = V^*$ hat Basis $S^* = \{s_1^*, \ldots, s_n^*\} \implies t_{\{i\}} := s_i^*$ macht das Richtige.

Induktionsschritt: $I = \{i_1, \ldots, i_{m+1}\} \subseteq \{1, \ldots, n\}$, $I := I \backslash \{i_1\}$ mit $i_1 < \cdots < i_{m+1}$.

$$t_I(v_1, \ldots, v_{m+1}) := \sum_{j=1}^{m+1} (-1)^{j-1} t_{\{i\_j\}}(v_j) t_I(v_1, \ldots, \check{v}_j, \ldots, v_{m+1}$$

wobei $\check{v}_j$: setze alles ein bis auf an der Stelle j.

$\implies t_I \in \mathcal{M}_m(V)$. Ist $i < j : v_i = v_j$

$$t_I(v_1, \ldots, v_{m+1}) \overset{\text{B. 1, § 12}}{=} (-1)^{i-1} t_{i_1}(v_i) t_I(v_1, \ldots, \check{v}_i, \ldots, \check{v}_j, \ldots, v_m + 1) \tag{III.1}$$

$$= (-1)^{j-1} \underbrace{t_{i_1}(v_j) t_I(v_1, \ldots, \check{v}_i, \ldots, \check{v}_j, \ldots, v_m + 1)}_{=C} \tag{III.2}$$

$$= \left((-1)^{i-1}(-1)^{j-i-1} + (-1)^{j-1}\right) C = (-1 + 1)c = 0 \tag{III.3}$$

$\implies t_I \in \mathcal{A}_m(V)$

$J = I : t_I(s_{j1}, \ldots, s_{jm+1}) = 1.$

$t_{I'}(s_{j2}, \ldots, s_{jm+1}) = 1 \cdot 1 = 1.$

$I \neq J : j_1 \neq i_1 \wedge I' \neq J' \implies$ in obiger Definition verschwindet jeder Summand $\implies t_I(s_{j1}, \ldots, s_{jm+1}) = 0.$ ∎

Satz 1, § 12

V K-Vektorraum, $\dim V = n \implies \dim \mathcal{A}_n(V) = 1.$

Beweis: $f \in A_n(V), I = \{1, \ldots, n\}, S = \{s_1, \ldots, s_n\}$ Basis, $(v_1, \ldots, v_n) \in V^n, v_i = \sum_{j=1}^n a_{ij} a_j \implies$ $f(v_1, \ldots, v_n) = \sum_{j_1=1}^n \cdots \sum_{j_n=1}^n \underbrace{a_{1j_1} a_{2j_1} \cdots a_{nj_n}}_{=C} f(s_{j_1}, \ldots, s_{j_n}) = \sum \cdots \sum C a t_I(s_{j1}, \ldots, s_{jn}) = a t_I(v_1, \ldots, v_n).$

Da $f(s_{\sigma(1)}, \ldots, s_{\sigma(n)}) = \operatorname{sign}\sigma \underbrace{f(s_1, \ldots, s_n)}_{=a} = \operatorname{sign}\sigma a t_I(s_1, \ldots, s_n) = a t_I(s_{\sigma(1)}, \ldots, s_{\sigma(n)})$ und $t_I \neq 0 \implies \dim \mathcal{A}_n(V) = 1.$ ∎

Anmerkung

$\{t_I | I \subseteq \{1, \ldots, n\}, \#I = m\}$ *bildet Basis von* $\mathcal{A}_m(V)$.

$$\dim \mathcal{A}_m(V) = \binom{n}{m} = \frac{n(n+1)\cdots(n-m+1)}{m!}$$

Definition 2, § 12

V K-Vektorraum, $\dim V = n \implies 0 \neq d \in \mathcal{A}_n(V)$ *heißt* ***Determinantenfunktion****.*

Folgerung 1, § 12

V K-Vektorraum, $\dim V = n, 0 \neq d \in \mathcal{A}_n(V)$*. Dann:* $\forall (v_1, \ldots, v_n) \in V^n : v_1, \ldots, v_n$ *linear unabhängig* $\iff d(v_1, \ldots, v_n) \neq 0$*.*

Beweis: „⇒“ $I = \{1, \ldots, n\} : t_I \neq 0 \implies d = c \cdot t_I \neq 0$ und $c \neq 0 \implies d(v_1, \ldots, v_n) \neq 0$.

„⇐“ Def. von alternierend ■

12.3. Determinante eines Endomorphismus

Bemerkung 4, § 12

V K-Vektorraum, $\dim V = n, \Phi \in \operatorname{End} V \implies \exists! \det \Phi \in K : \forall 0 \neq d \in \mathcal{A}_n(V) \forall v_1, \ldots, v_n \in V : d(\Phi(v_1), \ldots, \Phi(v_n)) = \det \Phi \cdot d(v_1, \ldots, v_n)$

Beweis: Sei $0 \neq d \in \mathcal{A}_n(V), \Phi \in \operatorname{End} V$, $d_\Phi \colon V^n \to K, (v_1, \ldots, v_n) \mapsto d(\Phi(v_1), \ldots, \Phi(v - n))$ ist in $\mathcal{A}_n(V), \dim \mathcal{A}_n(V) = 1 \implies \exists! \det_d \Phi \in K$ mit $d_\Phi = \det_d \Phi \cdot d$. Ist $0 \neq \tilde{d} \in \mathcal{A}_n(V) \implies \exists c \in K : \tilde{d} = cd \implies \tilde{d}_\Phi = cd_\Phi = c \det_d \Phi d = \det_d \Phi \tilde{d} \implies \det_{\tilde{d}} \Phi = \det_d \Phi$ unabhängig von der Wahl von $d = \det \Phi$. ■

Definition 3, § 12

V K-Vektorraum, $\Phi \in \operatorname{End} V, \det \Phi \in K$ *heißt* ***Determinante von*** Φ*.*

Satz 2, § 12

V K-Vektorraum, $\dim V = n$*.*

a) $\Phi, \Psi \in \operatorname{End} V \implies \det(\Psi \circ \Phi) = \det \Psi \cdot \det \Phi$ *und* $\det \mathrm{id}_V = 1$*.*

b) $\Phi \in \mathrm{Gl}(V) \iff \det \Phi \neq 0$*, insbesondere* $\det \Phi^{-1} = (\det \Phi)^{-1}$*.*

Beweis: $S = \{s_1, \ldots, s_n\}$ Basis von V. Dann $\Phi \in \mathrm{Gl}(V) \iff \Phi(s_1), \ldots, \Phi(s_n)$ linear abhängig $\iff 0 = d(\Phi(s_1), \ldots, \Phi(s_n)) = \det \Phi \cdot \underbrace{s_1, \ldots, s_n}_{\neq 0} \iff \det \Phi = 0$.

a) o.E. $\Phi, \Psi \in \mathrm{Gl}(V) \implies \det \Psi \circ \Phi =$

$$\frac{d_{\Psi \circ \Phi}(s_1, \ldots, s_n)}{d(s_1, \ldots, s_n)} = \frac{d_\Psi(\Phi(s_1), \ldots, \Phi(s_n))}{\mathrm{d}_\Psi(s_1, \ldots, s_n)} \cdot \frac{d_\Psi(s_1, \ldots, s_n)}{d(s_1, \ldots, s_n)} = \det \Psi \cdot \det \Phi$$

$\det \mathrm{id}_V = 1$ klar.

b) $\Phi \in \mathrm{Gl}\, V \implies \exists \Phi^{-1} \in \mathrm{Gl}\, V, \Phi^{-1} \circ \Phi = \mathrm{id}_V \implies 1 = \det \mathrm{id}_V = \det \Phi^{-1} \circ \Phi \overset{\text{a}}{\det} \Phi^{-1} \det \phi \implies$ Beh. ■

§ 13. Determinanten

13.1. Determinante einer Matrix

Definition 1, § 13

K Körper, $V = K^n, S = \{s_1, \ldots, s_n\}$. $A \in K^{n\times n} \implies \exists! \Phi \in \operatorname{End} V : D_S(\Phi) = A$. Setze $\det A := \det \Phi \in K$ *genannt* ***Determinante*** *von A.*

Satz 1, § 13

K Körper, $A, B \in K^{n\times n}$

a) $\det(AB) = \det A \cdot \det B$, $\det I_n = 1$

b) $A \in \mathrm{Gl}_n(K) \iff \det A \neq 0$, $\det A^{-1} = (\det A)^{-1}$

Daraus folgt insbesondere: $\det A$ *ist unabhängig von der Wahl von S.*

Beweis: Satz 2, § 12 unter K-Algebrenisomorphismus: $D_S : \operatorname{End} V \to K^{n\times n}$: z.B. $\det A \cdot B = \det(D_S(\Phi) \cdot D_S(\Psi)) = \det(D_S(\Phi \circ \Psi)) = \det \Phi \circ \Psi = \det \Phi \cdot \det \Psi = \det D_S(\Phi) \cdot \det D_S(\Psi) = \det A \cdot \det B$ für gewisse $\Phi, \Psi \in \operatorname{End} V$.

Rest analog. ∎

Damit: $\det A = \det D_S(\Phi) = \det D_S^T(\mathrm{id}) D_T(\Phi) D_T^S(\mathrm{id}) = \det(C^{-1}A'C)$ für andere Basis T von V.

Satz 2, § 13 (*Leibniz'sche Summenformel*)

K Körper, $A \in K^{n\times n} \implies$

$$\det A = \sum_{\sigma\in S_n} \left(\operatorname{sign}\sigma \cdot \prod_{i=1}^{n} a_{\sigma(i),i} \right) \tag{III.4}$$

$$= \sum_{\sigma\in S_n} \left(\operatorname{sign}\sigma \cdot \prod_{i=1}^{n} a_{i,\sigma(i)} \right) \tag{III.5}$$

Beweis: $S = \{s_1, \ldots, s_n\}$ Basis von $V = K^n \implies \exists \Phi_A \in \operatorname{End} V : D_S(\Phi_A) = A$.
$\Phi_A(s_j) = \sum_{i=1}^n a_{ij} s_i \implies \det A = \det \Phi_A$

$$\frac{d(\Phi_A(s_1), \ldots, \Phi(s_n))}{d(s_1, \ldots, s_n)} = \frac{d\left(\sum_{i=1}^n a_{i1}s_i, \ldots, \sum_{i=1}^n a_{in}s_i\right)}{d(s_1, \ldots, s_n)} = \sum_{i_n=1}^{n} a_{i_1,1}a_{i_1,2}\cdots a_{i_n,n} \cdot \underbrace{\frac{d(s_{i_1}, \ldots, s_{i_n})}{d(s_1, \ldots, s_n)}}_{(*)} \tag{III.6}$$

$$(*) = \begin{cases} 0 & \text{falls } s_{i_j} = s_{i_k} \text{ für } j \neq k \\ \operatorname{sign}\sigma & \text{falls} \sigma = \begin{pmatrix} 1 & \cdots & n \\ i_1 & \cdots & i_n \end{pmatrix} \end{cases}$$

d.h. $\det A = \sum_{\sigma\in S_n} \operatorname{sign}\sigma \cdot a_{\sigma(1),1}\cdots a_{\sigma(n),n}\cdot 1 = \sum_{\sigma\in S_n}\operatorname{sign}\sigma\cdot\prod_{j=1}^{n} a_{\sigma(j),j}$ und $\forall j\exists!i$: $j=\sigma^{-1}(i)$, d.h. $\det A = \sum_{\sigma in S_n}\operatorname{sign}\sigma\prod_{i=1}^{n} a_{i,\sigma^{-1}(i)} = \sum_{\sigma\in S_n}\operatorname{sign}\sigma\prod_{i=1}^{n} a_{i,\sigma(i)}$ und $\operatorname{sign}\sigma = \operatorname{sign}\sigma^{-1} = (\operatorname{sign}\sigma)^{-1}$. ■

Folgerung 1, § 13

$A\in K^{n\times n} \implies \det A = \det A^{tr}$ *folgt direkt aus Satz 2.*

Beispiel

1) $A\in K^{2\times 2} \implies$

$$\det A = a_{11}a_{22} - a_{21}a_{12}$$

2) $A\in K^{3\times 3} \implies$

$$\det A = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} \quad \text{(III.7)}$$
$$- a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32} \quad \text{(III.8)}$$

Merken mit der Regel von Sarrus[2]!

13.2. Numerische Berechnung von Determinanten

Bemerkung 1, § 13

$A=(a_{ij})\in K^{n\times n}$

a) Bei Vertauschung zweier Zeilen oder Spalten ändert sich das Vorzeichen der Determinante

b) Bei Addition des a-fachen einer Zeile bzw. Spalte i auf eine Zeile bzw. Spalte j mit $i\neq j$ ändert sich die Determinante nicht.

c) Bei Multiplikation einer Zeile bzw. Spalte von A mit $a\in K$ ändert sich die Determinante zu $(\det A)\cdot a$.

d) Gilt $a_{ij}=0$ für $i>j$ (Dreiecksmatrix) $\implies \det A = \prod_{i=1}^{n} a_{i,i}$

Beweis: Folgerung 1, § 13 $\implies$ reicht für Zeilenoperationen zu zeigen, z.B.:

$$\det(A\cdot V_{ij}) = \det(V_{ij}^{tr}\cdot A^{tr}) = -detA^{tr} = -\det A$$

a)
$$\det V_{ij} = (-1) \implies \det(V_{ij}A) = \det V_{ij}\cdot\det A = -\det A$$

b) $\det A_{ij}(a)$, sei $i<j \implies a_{ij}=0\forall i>j \implies$ Ist $\sigma\in S_n, \sigma\neq \mathrm{id} : \exists i : i>\sigma(i) \implies a_{\sigma(1),1}\cdots a_{\sigma(n),n}=0 \implies \det A_{ij}(a)=\prod_{i=1}^{n}1=1 \implies \det(A_{ij}(a)\cdot A) = \det A_{ij}(a)\cdot\det A = \det A$

c) $\det M_i(a) = 1 \cdots 1 \cdot a \cdot 1 \cdots 1 = a$

d) vgl. b) ■

Beispiel

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & -6 & -21 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 4 \\ 0 & -3 & -6 \\ 0 & 0 & -9 \end{pmatrix} \tag{III.9}$$

$\Longrightarrow \det A = 1(-3)(-9) = 27.$

13.3. Komplementäre Matrix

Definition 2, § 13

K Körper, $A = (a_{ij}) \in K^{n\times n} \implies A_{ij} \in K^{n\times n}$ *entsteht aus A durch Substitution der i-ten Zeile und der j-ten Spalte durch* 0 *bis auf* $a_{ij} = 1$, $A'_{ij} \in K^{(n-1)\times(n-1)}$ *durch Streichen von Zeile i und Spalte j.*
$a^{\#}_{ij} := \det A_{ji} \overset{!}{=} (-1)^{i+j} \det A'_{ji} \in K$ *heißt* ***Komplement*** *von* a_{ij}, *vergleiche Beispiel.*
$A^{\#} := \mathrm{Adj}(A) := (a^{\#}_{ij})_{i,j}$ *heißt* ***komplementäre (adjunkte) Matrix zu A****.*

Beispiel

$$A = \begin{pmatrix} * & * & * \\ * & * & * \\ * & * & * \end{pmatrix} \rightsquigarrow A_{22} = \begin{pmatrix} * & 0 & * \\ 0 & 1 & 0 \\ * & 0 & * \end{pmatrix}$$

Vertausche so, dass $\begin{pmatrix} 1 & 0 & 0 \\ 0 & * & * \\ 0 & * & * \end{pmatrix}$, *d.h. allg.* $(j-1)$ *Spaltenvektoren und* $(i-1)$ *Zeilenvektoren vertauschen* $\Longrightarrow$

$$\det \begin{pmatrix} * & 0 & * \\ 0 & 1 & 0 \\ * & 0 & * \end{pmatrix} = \underbrace{(-1)^{(i-1)+(j-1)}}_{=(-1)^{i+j}} \det \begin{pmatrix} 1 & 0 & 0 \\ 0 & * & * \\ 0 & * & * \end{pmatrix} = \det \begin{pmatrix} * & * \\ * & * \end{pmatrix}$$

da nur σ *mit* $\sigma(1) = 1$.

Satz 3, § 13

K Körper, $A \in K^{n\times n}$

a) $A^{\#}A = AA^{\#} = \det A \cdot I_n$

b) $A \in \mathrm{Gl}_n(K) \implies A^{-1} = \frac{1}{\det A} A^{\#}$

c) $\det A^{\#} = (\det A)^{n-1}$

Beweis: a) $A = (a^{(1)}, \ldots, a^{(n)}), a^{(j)} = j$-te Spalte von A.

$a^j \in K^n, C = A^{\#}A, C = c_i j$

$c_{ik} = \sum_{j=1}^n a_{ij}^{\#} a_{jk} = \sum_{j=1}^n a_{jk} \cdot \det A_{ji} \overset{(*)}{=} \sum_{j=1}^n a_{jk} \cdot \det(a^{(1)}, \ldots, a^{(i-1)}, e_j, a^{(i+1)}, \ldots, a^{(n)}) = \det(a^{(1)}, \ldots, a^{(i-1)}, a^{(k)}, a^{(i+1)}, \ldots, a^{(n)}) = \delta_{ik} \det A.$

(*) gilt, da in Leibnizformel nur die σ „überleben“ mit $\sigma(i) = j \implies \sigma(k) \neq j \forall k \neq i \implies a_{jk}$ kommen nicht in der Formel vor. Genauso: $AA^{\#} = \det A \cdot I_n$.

b) folgt aus a)

c) folgt auch mit a) und Rechenregel aus Bemerkung 1, § 13 ($a^{\#} = \det A \cdot A^{-1}$) ■

Folgerung 2, § 13 (*Entwicklungssatz von Laplace*)

$$\det A = \sum_{j=1}^n a_{ij} a_{ji}^{\#} = \sum_{j=1}^n a_{ij}^{\#} a_{ji}$$

Beispiel

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

Entwicklung nach erster Zeile ($i = 1, \det A = \sum_{j=1}^3 a_{1j} a_{j1}^{\#}$)

$$\det A = a_{11} \cdot \det \begin{pmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{pmatrix} - a_{12} \cdot \det \begin{pmatrix} a_{21} & a_{23} \\ a_{32} & a_{33} \end{pmatrix} + a_{13} \cdot \det \begin{pmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix}$$

Folgerung 3, § 13 (*Cramer'sche Regel*)

K Körper, $A \in \mathrm{Gl}_n(K), x, n \in K^n, Ax = b \implies$

$$x_i = \frac{\det(a^{(1)}, \ldots, a^{(i-1)}, b, a^{(i+1)}, \ldots, a^{(n)})}{\det A}$$

Beweis: $Ax = b \implies x = A^{-1}b = \frac{1}{\det A} A^{\#} b \implies x_i = \frac{1}{\det A} \sum_{j=1}^n a_{ij}^{\#} b_j \overset{\text{Laplace}}{=} \frac{1}{\det A} \det(a^{(1)}, \ldots, a^{(i-1)}, b, a^{(i+1)}, \ldots, a$ ■

Beispiel (*Vandemond'sche Determinante*)

$a_1, \ldots, a_n \in K.$

$$V(a_1, \ldots, a_n) = \det \begin{pmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{pmatrix} \tag{III.10}$$

$$= \det \begin{pmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 0 & a_2 - a_1 & a_2^2 - a_1^2 & \cdots & \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & a_n - a_1 & \cdots & \cdots & a_n^{n-1} - a_1^{n-1} \end{pmatrix} \tag{III.11}$$

$$\overset{(*)}{=} \det \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & a_2 - a_1 & (a_2 - a_1)a_2 & \cdots & (a_2 - a_1)a_2^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & a_n - a_1 & (a_n - a_1)a_n & \cdots & (a_n - a_1)a_n^{n-2} \end{pmatrix} \tag{III.12}$$

(*): i, j-ter Eintrag ($j \geqslant 2$): $a_i^{j-1} - a_1^{j-1} - a_1(a_i^{j-2} - a_1^{j-2}) = a_i^{j-1} - a - 1a_1^{j-2} = (a_i - a_1)a_i^{j-2}$
$\Longrightarrow \det A = \prod_{i=2}^{n}(a_i - a_1) \cdot V(a_2, \ldots, a_n) = \prod_{i=2}^{n}(a_i - a_1) \prod_{j=3}^{n}(a_j - a_1)V(a_1, \ldots, a_n) = \cdots = \prod_{1 \leqslant i < j \leqslant n}(a_j - a_i)$

13.4. Unterdeterminanten

Definition 3, § 13

$A \in K^{m \times n}$. $I = \{i_1, \ldots, i_k\} \subseteq \{1, \ldots, m\}, i_1 < \cdots < i_k, J = \{j_1, \ldots, j_k\} \subseteq \{1, \ldots, n\}, j_1 < \cdots < j_k$
$A_{IJ} := (a_{ij})_{\substack{i \in I \\ j \in J}}$
$\det A_{IJ}$ *heißt* ***k-reihige Unterdeterminante (Minore)*** *von* A.

Satz 4, § 13

$A \in K^{m \times n}$. Die folgenden Aussagen sind äquivalent:

a) $\operatorname{Rang} A = r$

b) Es gibt eine nicht-verschwindende r-reihige Unterdeterminante und jede $r+1$-reihige Unterdeterminante ist 0.

Beweis: Zeige $\operatorname{Rang} A \geqslant r \iff \exists A'$ r-reihige Untermatrix mit $\det A' \neq 0$ (d.h. $\operatorname{Rang} A < r+1 \iff \forall A'$ $(r+1)$-reihige Untermatrix gilt $\det A' = 0$)

„⇐“ $\det A' \neq 0 \Longrightarrow \operatorname{Rang} A' = r \Longrightarrow \operatorname{Rang} A \geqslant r$

„⇒“ $\operatorname{Rang} A \geqslant r \Longrightarrow A$ besitzt r linear unabhängige Zeilen. Sei B die Matrix aus diesen Zeilen $\Longrightarrow \operatorname{Rang} B = r$, sei A' die Matrix aus den r linear unabhängigen Spalten von $B \Longrightarrow \operatorname{Rang} A' = r \iff \det A' \neq 0$. ∎

Satz 5, § 13 (*Gram'sche Determinante*)

$A \in K^{m \times n}, m \leqslant n \Longrightarrow$

$$\det AA^{tr} = \sum_{\substack{\{i_1, \ldots, i_m\} \subseteq \{1, \ldots, n\} \\ i_1 < \cdots < i_m}} \det(a^{(i_1)}, \ldots, a^{(i_m)})$$

Ohne Beweis.

§ 14. Polynome

14.1. Konstruktion des Polynomring

Beispiel: K Körper, $f\colon K \to K, x \mapsto f(x) = \sum_{i=0}^{n} a_i x^i$ heißt Polynomfunktion, z.B. $K = \mathbb{F}_2$: $f(x) = x^2 - x$

Definition 1, § 14

K Körper, $f \in \mathrm{Abb}(\mathbb{N}, K) = K^{\mathbb{N}}$ heißt ***finit*** $:\iff \#\{n \in \mathbb{N} | f(n) \neq 0\} =: \#\mathbb{N}_f < \infty$.
$K[\mathbb{N}] := \{f \in K^{\mathbb{N}} | f \text{ finit}\}$ *Menge der finiten Abbildungen.*

Anmerkung

$K[\mathbb{N}]$ *ist UVR von* $K^{\mathbb{N}}$.

Beweis ist klar.

Satz 1, § 14

K Körper

a) $K[\mathbb{N}]$ *ist K-Algebra mit*

$$+ : K[\mathbb{N}] \times K[\mathbb{N}] \to K[\mathbb{N}],\ (f,g) \mapsto f+g,\ (f+g)(n) = f(n)+g(n) \qquad \text{(III.13)}$$
$$\cdot : K[\mathbb{N}] \times K[\mathbb{N}] \to K[\mathbb{N}],\ (f,g) \mapsto fg,\ (fg)(n) = \sum_{l+m=n} f(l)g(m) \qquad \text{(III.14)}$$

b) $\exists$ *injektive Abbildung* $\epsilon : \mathbb{N} \to K[\mathbb{N}],\ n \mapsto e_n : e_n(m) = \delta_{n,m}, e_m \cdot e_n = e_{m+n}$
$\iota : \mathbb{N} \to K[\mathbb{N}],\ a \mapsto a \cdot e_0$ *mit* $\iota(a+b) = \iota(a) + \iota(b), \iota(ab) = \iota(a)\iota(b)$

Beweis: a) $K[\mathbb{N}]$ $(K,+)$ abelsche Gruppe $\implies$ $(K[\mathbb{N}],+)$ abelsche Gruppe.

$n \in \mathbb{N} \implies \#\{(l,m) | l+m = n; l,m \in \mathbb{N}\} = n+1$

f,g finit $\implies (fg)(n) = \sum_{l+m=n} f(l)g(m) = 0 \implies fg$ finit

$\forall n \in \mathbb{N} : (fg)(n) = \sum_{l+m=n} f(l)g(m) = \sum_{m+l=n} g(m)f(l) = (gf)(h) \implies fg = gf$

$\forall n \in \mathbb{N} : ((fg)h)(n) = \sum_{l+m=n}(fg)(l)h(m) = \sum_{l+m=n}\left(\sum_{k+r=l} f(k)g(r)\right)h(m) = \sum_{k+r+m=n} f(k)g(r)h(m) = \cdots = (f(gh))(n) \implies (fg)h = f(gh)$

$\forall n \in \mathbb{N} : ((f+g)h)(n) = \sum_{l+m=n}(f+g)(l)h(m) = \sum_{l+m=n} f(l)h(m) + \sum_{l+m=n} g(l)h(m) = (fh)(n) + (gh)(n) \implies (f+h)h = fh + gh) \implies$ Distributivgesetz

$\forall n \in \mathbb{N} : (e_0 f)(n) = \sum_{l+m=n} e_0(l)f(m) = f(n) \implies e_0 f = f \implies e_0$ Einselement $\implies K[\mathbb{N}]$ Ring

Algebrenregel: genügt: $a(fg) = (af)g$

$\forall a \in K, f,g \in K[\mathbb{N}], af$ gewöhnliche Multiplikation von K auf $K^{\mathbb{N}}$. $(a(gh))(n) = a\sum_{l+m=n} f(l)g(m) = \sum_{l+m=n}(af)(l)g(m) = ((af)g)(n)$

b) $\forall n \in \mathbb{N} : (e_i e_j)(n) = \sum_{l+m=n} e_i(l)e_j(m) = \sum_{l+m=n} \delta_{il}\delta_{jm} = \begin{cases} 1 & i+j=n \\ 0 & \text{sonst} \end{cases} = e_{i+j}(n)$

$\forall n \in \mathbb{N} : (\iota(a+b))(n) = (a+b)e_0(n) = ae_0(n) + be_0(n) = \iota(a)(n) + \iota(b)(n)$, $\cdot$ genauso.
$\iota(1_K) = e_0 = 1_{K[\mathbb{N}]}$ ■

Schreibweise: $f \in K[\mathbb{N}] \implies \forall n \in \mathbb{N} : f(n) = \sum_{m\in\mathbb{N}} e_m(n)f(m) = \sum_{m\in\mathbb{N}} f(m)e_1^m(n)$. Da f finit: $\implies \exists d \in \mathbb{N}$:

$$f = \sum_{m=0}^{d} f(m)e_1^m =: \sum_{m=0}^{d} f(m)X^m,\ X := e_1$$

Definition 2, § 14

$K[X] := (K[\mathbb{N}], +, \cdot)$ *heißt* ***Polynomring*** *über* K.
$f = f(X) \in K[X]$ *heißt* ***Polynom***.
$f = \sum_{m=0}^{d} a_m X^m, \quad d = \max\{m | a_m = f(m) \neq 0\}$ *heißt* ***Grad von f***, $\mathrm{Grad}(0) := -\infty$ *mit* $a + (-\infty) := -\infty \forall a \in \mathbb{N}$.
$a_d =: \mathrm{hK}(f)$ *heißt* ***höchster Koeffizient*** *von f.*
f heißt ***normiert***, *falls* $\mathrm{hK}(f) = 1$.

Bemerkung 1, § 14

K Körper, $f, g \in K[X] \implies$

a) $\mathrm{Grad}(f + g) \leqslant \max\{\mathrm{Grad}\, f, \mathrm{Grad}\, g\}$

b) $\mathrm{Grad}(fg) = \mathrm{Grad}\, f + \mathrm{Grad}\, g$

Beweis : klar. ■

Folgerung 1, § 14

K Körper $\implies$ $K[X]$ *Integritätsbereich.*

Beweis : zu zeigen: $K[X]$ hat keine Nullteiler.

Sei $fg = 0 \implies \mathrm{Grad}\, f + \mathrm{Grad}\, g = \mathrm{Grad}\, 0 = -\infty \implies$ f oder g ist 0. ■

14.2. Nullstellen von Polynomen

Definition 3, § 14

K Körper, $f(X) \in K[X], a \in K$ *heißt* ***Nullstellte*** *von* $f :\iff f(a) = 0$.

Satz 2, § 14

K Körper, $f(X) = \sum_{i=0}^{m} a_i X^i, g(X) = \sum_{j=0}^{n} b_j X^j, a_m \neq 0, b_n \neq 0 \implies$ *Es gibt eindeutig bestimmte Polynome* $q(X), r(X) \in K[X]$:

$$f(X) = q(X)g(X) + r(X)$$

mit $\mathrm{Grad}\, r < \mathrm{Grad}\, g$.

Beweis : Induktion nach m für festes n:

$m < n \implies q(X) = 0, r(X) = f(X)$ erfüllt obiges.

Induktionsschritt $m-1$ zu $m \geqslant n$. Setze $q_0(X) := a_m b_n^{-1} X^{m-n} \implies f_1 := f - q_0 g$, Grad $f_1 \leqslant m-1$, denn $f_1 = (a_m X^m + \dots) - a_m b_n^{-1} X^{m-n}(b_n X^n + \dots) - \dots$

Induktionsargument: $\exists q_1, r_1 \in K[X] : f_1 = q_1 g + r_1 \implies f(q_1+q_0)g + r_1$ mit Grad $r_1 <$ Grad $g \implies$ Existenz.

Eindeutigkeit: Angenommen $f = qg + r = \tilde{q}g + \tilde{r}$ mit Grad $r <$ Grad g; Grad $\tilde{r} <$ Grad $g \implies (q-\tilde{q})g = \tilde{r} - r$. Ist $q = \tilde{q} \implies \tilde{r} = r$.

Also $q \neq \tilde{q} \implies$ Grad $g >$ max{Grad r, Grad $\tilde{r}$} $\geqslant$ Grad$(\tilde{r} - r)$ = Grad$((q-\tilde{q})g)$ = Grad$(q \cdot \tilde{q})$ + Grad $g \geqslant$ Grad $g \lightning \implies$ Eindeutigkeit. ■

Folgerung 2, § 14

$f \in K[X], a \in K$ Nullstelle von $f \implies (X-a) | f$ (d.h. $\exists q \in K[X] : (x-a)q = f$).

Beweis : mit Division mit Rest: $f(X) = q(X)(X-a) + r(X) \implies$ Grad $r < 1 \implies$ Angenommen $r(X) = bX_i, b \in K$

$0 = f(a) = q(a)(a-a) + b = b \implies b = 0$ ■

Satz 3, § 14

K Körper, $f(X) \in K[X]$. Grad $f = n \geqslant 0 \implies f$ hat höchstens n Nullstellen in K.

Beweis : Induktion nach n: $n = 0 \implies f = b \in K \backslash \{0\} \implies$ hat keine Nullstellen.a

Sei a Nullstelle von $f \implies f(X) = q(X)(X-a)$ mit Grad $q = n - q$. Ist $b \neq a$ Nullstelle von $f \implies 0 = f(b) = q(b)(\underbrace{b-a}_{\neq 0}) \implies q(b) = 0 \implies b$ Nullstelle von q. Induktionsargument: q hat höchstens $n-1$ Nullstellen $\implies f$ hat höchstens n Nullstellen. ■

14.3. Teiler von Polynomen

Definition 4, § 14

*K Körper, $f \in K[X], g \in K[X]$ heißt **Teiler** von f : $\iff \exists q \in K[X] : f = gq$: $g | f$.*
*g heißt **trivialer Teiler** von f : $\iff \exists 0 \neq a \in K : g = a$ oder $g = af$.*
*$p \in K[X] \backslash K$ heißt (normiertes) **Primpolynom** : $\iff$ p besitzt nur die trivialen Teiler (hK$(p) = 1$).*
$d \in K[X]$ heißt (normierter) ggT von $f, g \in K[X]$: $\iff$ $d|f, d|g \wedge$ falls $t \in K[X]$: $(t|f \wedge t|g \implies t|d)$.

Satz 4, § 14

a) Zu $f, g \in K[X]$ existtiert ein eindeutig bestimmter normierter ggT d.

b) $d =$ ggT(f,g) (im folgenden meint ggT immer normierten ggT) $\implies \exists u, v \in K[X]$: $d = af + vg$

Beweis: **Existenz** mit Euklidsischem Algorithmus

$f_0 = f, f_1 = g$. Division mit Rest:

$$f_0 = q_t f_1 + f_2,\ f_1 = q_2 f_2 + f_3,\ \ldots,\ f_{r-2} = q_{r-1} f_{r-1} + f_r,\ f_{r-1} = q_r f_r + 0$$

Reihe muss abbrechen, da Grad $f_1 >$ Grad $f_2 > \cdots >$ Grad $f_r \implies f_r | f_{r-1} \implies f_r | f_{r-2} \implies \ldots \implies f_r | f_1 = g,\ f_r | f_0 = f$.

Ist $t \in K[X] : t|f_0 \wedge t|f_1 \implies t|f_2 \implies \ldots \implies t|f_r \implies f_r$ ist ein gr. gemeinsamer Teiler von $f, g \implies d = \mathrm{hK}(f_r)^{-1}$. f_r ist normierter ggT.

Eindeutigkeit Sei $d = \mathrm{ggT}(f,g) = \tilde{d} \implies d|\tilde{d}, \tilde{d}|d \implies \exists q, \tilde{q} \in K[X] : d = \tilde{q}\tilde{d},\ \tilde{d} = qd \implies d = \tilde{q}\tilde{q}d \iff (1 - q\tilde{q})d = 0$, o.E: $d \neq 0$. Da $K[X]$ Integritätsbereich $\implies 1 - q\tilde{q} = 0 \iff q\tilde{q} = 1$, d.h. Grad $q +$ Grad $\tilde{q} = 0$ d.h. $q, \tilde{q} \in K$ und $1 = \mathrm{hK}(d) = \mathrm{hK}(\tilde{q}\tilde{d}) = \tilde{q}\,\mathrm{hK}(\tilde{d}) \implies d = \tilde{d}$.

b) Eukl. Algorithmus rückwärts, vgl. Übung bzw. Aufgabe 13. ■

Satz 5, § 14

$p \in K[X] : p(X)$ ist (normiertes) Primpolynom $\iff (\mathrm{hK}(p) = 1)$ und $\forall f, g \in K[X] : p|fg \implies p|f \vee p|g$.

Beweis: „⇐“ Sei $p = fg \implies p|fg$ o.E. $p|f$. Aber auch $f|p \implies f = ap$ mit $a \in K$ (vgl. Eindeutigkeit im vorherigen Beweis).

„⇒“ Sei $p|fg$ und ohne Einschränkung $p \not| f \implies \mathrm{ggT}(p,f) = 1 \implies \exists u, v \in K[X] : 1 = uf + vp \implies g = ufg + vpg = upq + vpg = p(uq + vg) \implies p|g$. ■

Zusatz: $p \in \mathbb{Z}$ prim $\iff p \in \mathbb{N} \wedge \forall a, b \in \mathbb{Z} : p|ab \implies p|a \vee p|b$.
Beweis: wörtlich wie Satz 5, § 14.

14.4. Primzerlegung

Beispiel

$f \in \mathbb{C}[X], f = X^2 \implies \forall a \in C, a \neq 0 : (aX)(a^{-1}X) = f \implies f$ hat ∞-viele Primzerlegungen.

Satz 6, § 14

Sei $\mathbb{P}_{K[X]}$ die Menge aller normierten Primpolynome von $K[X] \implies \forall 0 \neq f \in K[X] \exists! 0 \neq a \in K \wedge \forall p \in \mathbb{P}_{K[X]} \exists! e_p \in \mathbb{N}$:

$$f = a \prod_{p \in \mathbb{P}_{K[X]}}{}' p^{e_p}$$

($\prod'$: bis auf endlich viele $= 1$, d.h. $e_p = 0$ an diesen Stellen)

Beweis: **Existenz** Induktion nach Grad $f = n$. Sei $a = \mathrm{hK}(f) \implies f = af_1$ mit $\mathrm{hK}(f_!) = 1$. Ist $n = 0 \implies f_1 = 1, e_p = 0 \forall p \in \mathbb{P}_{K[X]}$

$n - 1 \rightsquigarrow n\ (> 1)$: Ist $f_1 \in \mathbb{P}_{K[X]}$, so fertig.

Sonst: $f_1 = g\tilde{g}$ mit $g, \tilde{g}$ nicht-triviale Teiler $\Longrightarrow$ $0 < \operatorname{Grad} g < n$, $0 < \operatorname{Grad} \tilde{g} < n$ $\Longrightarrow$ Induktionsargument

$$g = b \prod_{p \in \mathbb{P}_{K[X]}}{}' p^{d_p},\ \tilde{g} = \tilde{b} \prod_{p \in \mathbb{P}_{K[X]}}{}' p^{\tilde{d}_p} \Longrightarrow f = ab\tilde{b} \prod_{p \in \mathbb{P}_{K[X]}} p^{d_p + \tilde{d}_p}$$

Existenz durch Induktion nach $n = \operatorname{Grad} f$. Sei also

$$f = a \prod{}' p^{e_p} = \tilde{a} \prod{}' p^{\tilde{e}_p} \overset{\text{hK}}{\Longrightarrow} a = \tilde{a}$$

Ist $n = 0 \Longrightarrow e_p = 0 = \tilde{e}_p\ \forall p \in \mathbb{P}_{K[X]}$.

$n - 1 \rightsquigarrow n (\geqslant 1)$: $\operatorname{Grad} f_1 \geqslant 1 \Longrightarrow \exists q \in \mathbb{P}_{K[X]} : e_q \geqslant 1 \Longrightarrow q | f = a \prod{}' p^{\tilde{e}_p} \Longrightarrow q | p'$ für ein $p' \in \mathbb{P}_{K[X]}$.

Da $p' \in \mathbb{P}_{K[X]} \Longrightarrow q = p'$ weil normiert $\Longrightarrow \prod{}' p^{e_p - \delta_{pq}} = \prod{}' p^{\tilde{e}_p - \delta_{pq}} = \tilde{f}_2$ und $\operatorname{Grad} \tilde{f}_2 < n$.

Induktionsargument: $e_q - 1 = \tilde{e}_q - 1$ und $e_p = \tilde{e}_p \forall p \neq q \Longrightarrow e_p = \tilde{e}_p \forall p \in \mathbb{P}_{K[X]}$. ■

Zusatz 2: $0 \neq z \in \mathbb{Z} \Longrightarrow \exists! a \in \{-1, 1\} \wedge \forall p \in \mathbb{P} \exists! e - p \in \mathbb{N} : z = a \prod{}' p^{e_p}$
Beweis: wörtlich wie vorher mit Betrag statt Grad.

§ 15. Eigenräume und Eigenwerte

Definition 1, § 15

*V K-Vektorräume, $\Phi \in \operatorname{End} V$ heißt auch **linearer Operator**.*
*$a \in K$ heißt **Eigenwert** von $\Phi :\Longleftrightarrow \exists 0 \neq v \in V : \Phi(v) = av$ ($\Longleftrightarrow v \in \ker(\Phi - a \cdot \mathrm{id}_V)$).*
*$E_\Phi(a) = \ker(\Phi - a \cdot \mathrm{id}_V) < V$ heißt **Eigenraum** von Φ zum Eigenwert a. $0 \neq v \in E_\Phi(a)$ heißt **Eigenvektor** zu a. $e_\Phi(a) := \dim(E_\Phi(a))$ heißt **(geometrische) Vielfachheit**.*
$\operatorname{Spek} \Phi := \{a \in K | a \text{ Eigenwert von } V\} = \{a \in K | e_\Phi(a) \geqslant 1\}$

Beispiel

$K = \mathbb{R}, V = C^\infty(\mathbb{R})$ unendlich-oft diffbare Funktionen $f : \mathbb{R} \to \mathbb{R}$. $D : V \to V$, $f(x) \mapsto f(x)$ Differentialoperator ist linear. Ist $a \in \mathbb{R} \Longrightarrow D(\exp(ax)) = a \exp(ax) \Longrightarrow a$ Eigenwert von $D \Longrightarrow \operatorname{Spek} D = \mathbb{R}$.

Bemerkung 1, § 15

V endlich-dimensionaler K-Vektorraum. Dann sind für $\Phi \in \operatorname{End} V, a \in K$ äquivalent:

a) $a \in \operatorname{Spek} \Phi$

b) $\Phi - a \cdot \mathrm{id}_V \notin \mathrm{Gl}(V)$

c) $\det(\Phi - a \cdot \mathrm{id}_V) = 0$

Beweis: a) $\overset{\text{Def}}{\Longleftrightarrow}$ b) $\overset{\text{S. 12.2}}{\Longleftrightarrow}$ c) ■

Satz 1, § 15

V K-Vektorraum, $\Phi \in \operatorname{End} V$, $a_1, \ldots, a_n \in \operatorname{Spek} \Phi, a_i \neq a_j$.

$$iW := \sum_{i=1}^{n} E_\Phi(a-i) < V \implies W = \bigoplus_{i=1}^{n} E_\Phi(a_i)$$

Beweis : Induktion nach n. $n = 1$ klar, $n-1 \rightsquigarrow n$:

$$W_i := E_\Phi(a_i),\ X_i := W_i \cap \sum_{\substack{j=1 \\ j\neq i}}^{n} w_j,\ v \in X_i$$

$\implies \exists w_j \in W_j,\ j \neq i : v = \sum_{j=1, j\neq i}^{n} w_j \implies$

$$\sum_{\substack{j=1 \\ j\neq i}}^{n} a_i w_j = a - iv = \Phi(v) = \sum a_j w - j \implies \sum \underbrace{(a_i - a_j)}_{\neq 0} w_j = 0$$

und das $\in \sum W_j = \bigoplus W_j \iff w_j = 0 \forall j \neq i \implies v = 0 \implies X_i = 0$. ■

Anwendung 1 $\dim V < \infty \implies \sum_{i=1}^{n} e_\phi(a_i) \leqslant \dim V \implies$ es gibt nur endlich viele Eigenwerte.
Wenn $\sum e_\phi(a_i) = \dim V \implies V = \bigoplus E_\phi(a_i)$

Definition 2, § 15

V K-Vektorraum, $\Phi \in \operatorname{End} V$ *heißt* ***diagonalisierbar*** : $\iff$

$$V = \bigoplus_{a \in \operatorname{Spek} \Phi} E_\phi(a)$$

$\iff$ *V hat Basis aus EV.*

15.1. Minimalpolynom

Bemerkung 2, § 15

V K-Vektorraum, $\Phi \in \operatorname{End} V, a \in \operatorname{Spek} \Phi$, $f = \sum_{i=0}^{n} a_i X^i \in K[X] \implies f(\Phi) := \sum_{i=0}^{n} a_i \Phi^i \in \operatorname{End} V \implies$

a) $f(a) \in \operatorname{Spek} f(\Phi),\ E_\Phi(a) \leqslant E_{f(\Phi)}(f(a))$

b) $f(a) = 0 \implies E_\Phi(a) \overset{a)}{\leqslant} E_{f(\Phi)}(0) = \ker f(\Phi)$

Beweis : a) $\Phi(v) = a \cdot v \implies \Phi^i(v) = a^i \cdot v$
$f(\Phi)(v) = \sum a_i \Phi^i(v) = \sum a_i a^i v = f(a) \cdot v$

b) klar aus a) ■

Beispiel

$\dim V < \infty$, $\Phi \in \operatorname{End} V$ *sei diagonalisierbar,* $f := \prod_{a \in \operatorname{Spek}\Phi}(X - a)$
$\implies V > \ker f(\Phi) \geqslant \sum_{a \in \operatorname{Spek}\Phi} E_\Phi(a) = V \implies \ker f(\Phi) = V$

Frage: Existiert immer $f \in K[X] : f(\Phi) = 0$?

Satz 2, § 15

V endlich-dimensional, $\Phi \in \operatorname{End} V, F = \{f \in K[X] | f(\Phi) = 0\} \implies \exists! g \in F, g \neq 0 :$
$\forall f \in F : \exists q \in K[X] : f = gq$ *und g normiert.*

Beweis: $\dim V = n \implies \dim \operatorname{End} V = n^2 \implies \mathrm{id}, \Phi, \Phi^2, \ldots, \Phi^{n^2}$ sind linear abhängig $\implies$ $\exists a_i \in K : \sum_{i=0}^{n} a_i \Phi^i = 0$ nicht-trivial $\implies 0 \neq f = \sum_{i=0}^{n^2} a_i X^i : f(\Phi) = 0 \implies 0 \neq f \in F \implies \exists 0 \neq g \in F$, g normiert, g kleinsten Grades. Ist $f \in F$ beliebig $\implies f = qg + r$, $\operatorname{Grad} r < \operatorname{Grad} g \implies r(\Phi) = f(\Phi) - qg(\Phi) = 0 \implies r \in F \implies r = 0 \implies g | f$ und g eindeutig (g' normiert, $\operatorname{Grad} g' = \operatorname{Grad} g \implies g | g', g' | g \implies g = g'$). ■

Definition 3, § 15

$g \in K[X]$ *wie in Satz 2, § 15 heißt* ***Minimalpolynom*** *zu* Φ.

Anmerkung 1, § 15

$\Phi \in \operatorname{End} V$ *mit* $\dim V = \infty$, *so existiert Mipo falls* $F \neq 0$ *mit dem selben Beweis.* Φ *heißt in diesem Fall* ***algebraischer Operator***.

Krylov-Verfahren V K-Vektorraum, mit Basis $S = \{s_1, \ldots, s_n\}$, $\Phi \in \operatorname{End} V$.

1) Für $i = 1, \ldots, n$ berechnet $s_i, \Phi(s_i), \Phi^2(s_i), \ldots$. Falls l.a. $\implies \exists g_i \in K[X] : g_i(\Phi)(s_i) = 0$ normiert kleinsten Grades.

2) $g = \mathrm{kgV}(g_i) =: f$, d.h. $g_i | f$ und falls $h \in K[X]$ mit $g_i | h \forall i \implies f | h$ **kleinstes gemeinsames Vielfaches**. Existiert in diesem Fall ($K[X]$) immer[3]. $\implies \forall i : g(\Phi)(s_i) = 0 \implies g(\Phi)(V) = 0 \implies g \implies g_\Phi | g$. Ist $f \in K[X] : g(\Phi)(s_i) = 0 \forall i \implies f = q_i g_i + r_i$, $\operatorname{Grad} r_i < \operatorname{Grad} g_i$.

   $r_i(\Phi)(s_i) = f(\Phi)(s_i) - q_i g_i(\Phi) s_i = 0 \implies r_i = 0 \implies g_i | f \implies g | f$: Insbesondere wende an auf $f = g_\Phi \implies g | g_\Phi \implies g = g_\Phi$.

[3] $f, g \in K[X] \implies fg$ sicherlich gem. Vielfaches aber im allgemeinen nicht kleinstes. Betrachte Primzerlegung von f und g um kgV zu finden.

Beispiel

V K-Vektorraum, $W < V \implies \exists Y \leqslant V : V = W \oplus Y$.
$\pi_w : V \to W$ Projektvion von V auf W längs Y.
Sei S Basis von W, T Basis von $Y \implies S \cup T$ Basis von $V \implies$
$s \in S : \pi_w(s) = 1 \cdot s \implies (\pi_w - \mathrm{id}_V)(s) = 0 \implies g_s(X-1)$.
$t \in T : \pi_w(t) = 0 \cdot t \implies g_t = X$

$\Longrightarrow$ $g_{\pi_w} = X(X-1)$ *Mipo von* π_W.

15.2. Primärzerlegung

Bemerkung 3, § 15

V K-Vektorraum, $\Phi \in \operatorname{End} V : f, g \in K[X]$

a) $f|g \implies \ker f(\Phi) < \ker g(\Phi)$

b) $\operatorname{ggT}(f,g) = 1 \implies \ker(fg(\Phi)) = \ker f(\Phi) \oplus \ker g(\Phi)$

Beweis: a) $v \in \ker f(\Phi) \implies f(\Phi)(v) = 0 \overset{fq=g}{\Longrightarrow} f(\Phi)(v) = q(\Phi) \circ f(\Phi)(v)$

b) $W := \ker(f \circ g(\Phi)) \overset{\text{a)}}{\geqslant} \ker f(\Phi) + \ker g(\Phi) = W_2 + W_2 \implies \exists u, v \in K[X] : uf + vg = 1 \implies uf(\Phi) + vg(\Phi) = \mathrm{id}_V$

$\pi_1 = vg(\Pi),\ \pi_2 = uf(\Phi)$

$\implies \pi_1 + \pi_2 = \mathrm{id}_V$. Sei $w \in W \implies w = \pi_1(w) + \pi_2(w)$

mit $f(\Phi) \circ \pi_1(w) = vfg(\Phi)(w) = 0$ und $g(\Phi) \circ \pi_2(w) = ufg(\Phi)(w) = 0 \implies w \in W_1 + W_2$.

Ist $w \in W_1 \cap W_2 \implies w \in W_1 \wedge w \in W_2 \implies f(\Phi)(w) = 0, g(\Phi)(w) = 0 \implies \pi_1(w) = 0, \pi_2(w) = 0 \implies w = \pi_1(w) + \pi_2(w) = 0 + 0 = 0 \implies$ Beh. ■

Satz 3, § 15 (*Kernspaltungssatz*)

V K-Vektorraum, $\Phi \in \operatorname{End} V, f \in K[X]$ *mit* $f = \prod_i' p_i^{e_i}(x) \implies \ker f(\Phi) = \bigoplus_i \ker p_i(\Phi)^{e_i}$

Beweis: Induktiv aus Bem. 3 durch Induktion. ■

Folgerung 1, § 15

Sei Φ *algebraisch,* $g_\Phi(x) = \prod_{i=1}^r p_i(x)^{e_i}$ *Mipo* $\implies V = \bigoplus_{i=1}^r \ker p_i(\Phi)^{e_i}$

Beweis: aus Satz 3, § 15 mit $f = g\Phi$. ■

Folgerung 2, § 15

Sei Φ *algebraisch* $\implies$

a) $\operatorname{Spek}\Phi = \{a \in K : (X-a) | g_\Phi\}$

b) Φ *diagonalisierbar* $\iff g_\Phi = \prod_{a \in \operatorname{Spek}\Phi}(X-a)$

Beweis: a) „$\subseteq$“ $a \in \operatorname{Spek}\Phi \implies \exists 0 \neq v \in V : \Phi(v) = av$. Angenommen, $(X-a) \nmid g_\Phi \implies \exists \operatorname{ggT}((X-a), \mathfrak{g}_\Phi) = 1 \implies \exists t, u \in K[X]$.

$t(X-a) + ug_\Phi = 1 \implies t(\Phi)(\Phi - aI)(v) \neq 0 \implies u \cdot g_\Phi(\Phi)(v) = v \neq 0 \implies \lightning$ zu $g_\Phi(\phi)(V) = 0$.

„⊇“ Sei $(X-a)|g_\Phi \implies \exists f \in K[X] : f(X-a)g_\Phi \implies f(\Phi)(V) \neq 0 (\Phi - a\,\mathrm{id}_v) f(\Phi)(V) = g_\Phi(\Phi)(V) = 0 \implies \exists v \in V : v$ Eigenvektor zu a.

b) „⇒“ Φ diagonalisierbar $\implies V = \bigoplus_{a \in \mathrm{Spek}\,\Phi} E_\Phi(a) = \bigoplus \ker(\Phi - a \cdot \mathrm{id}_V) \implies g_\Phi | \prod_{a \in \mathrm{Spek}\,\Phi}(X-a) =: f$, $f|g_\Phi$ da $(X-a)|g_\Phi$ nach a). $f(\Phi)(V) = 0$ da $\ker f(\Phi) = V \implies f = g_\Phi$.

„⇐“ $g_\Phi = \prod_{a \in \mathrm{Spek}\,\Phi}(X-a) \implies V = \bigoplus E_\Phi(a) \implies \Phi$*diagonalisierbar*. ■

15.3. Hauptpolynom

Definition 4, § 15

R kommutativer Ring mit 1 $\implies$ $R^{n\times n}$ *mit Matrizenmultiplikation ist Ring mit* $1 = \begin{pmatrix} 1_R & & \\ & \ddots & \\ & & 1_R \end{pmatrix}$.

$A = (a_{ij}) \in R^{n\times n}$ *heißt* $n \times n$***-Matrix über R***.

$$\det A := \sum_{\sigma \in S_n} \operatorname{sign}\sigma \cdot \prod_{i=1}^{n} a_{i,\sigma(i)}$$

heißt ***Determinante von A***.

Aufgabe: $A, B \in R^{n\times n} \implies \det AB = \det A \cdot \det B$.
$AA^\# = \det A \cdot I_n$, $A^\#$ adjungierte Matrix zu A.

Definition 5, § 15

V K-Vektorraum mit Basis $S = \{s_1, \ldots, s_n\}$, $\Phi \in \mathrm{End}\,V$.
$A = D_S(\Phi) \in K^{n\times n} \implies h_\Phi(X) := \det(X \cdot I_n - A) \in K[X]$ *heißt* ***Hauptpolynom*** *(oder auch* ***charakteristisches Polynom****) von* Φ *(bzw. A).*

Bemerkung 4, § 15

Ähnliche Matrizen haben dasselbe Hauptpolynom, d.h. h_Φ *unabhängig von der Wahl von* S.

Beweis: Sei $T \subseteq V$ weitere Basis, $A = D_S(\Phi)$.

$B = D_T(\Phi) = C_T^S D_S(\Phi) C_S^T = C^{-1}AC$ ähnlich $\implies h_b(X) = \det(XI_n - B) = \det(C^{-1}XI_nC - C^{-1}AC) = \det(C^{-1}(XI_n - A)C) = \det(C^{-1})\det(XI_n - A)\det(X) = h_A(X)$ ■

Bemerkung 5, § 15

V K-Vektorraum, $\dim V = n, \Phi \in \mathrm{End}\,V \implies$

a) $\mathrm{Grad}\,h_\Phi = n$

b) $\mathrm{Spek}\,\Phi = \{a \in K | h_\Phi(a) = 0\}$

c) Φ *diagonalisierbar* $\iff \exists$ *Basis* S*:* $D_S(\Phi)$ *hat Diagonalgestalt.*

Beweis: a) $A = D_S(\Phi) = h_\Phi(X) = \det(XI_n - A) = \prod_{i=1}^n (X - a_{i,i}) + \sum_{\substack{\sigma \in S_n \\ \sigma \neq \mathrm{id}}} \operatorname{sign}\sigma \cdot \prod_{i=1}^n (\delta_{i,\sigma(i)} X - a_{i,\sigma(i)}) = X^n +$ niedrigere Terme.

b) $a \in \operatorname{Spek}\Phi \iff 0 = \det(a\,\mathrm{id}_V - \Phi) = \det(aI_n - D_S(\Phi)) = h_\Phi(a)$

c) Φ diagonalisierbar $\iff$ V hat Basis $S = \{s_1, \ldots, s_n\}$ aus EV $\iff$ $\forall i = 1, \ldots, n : \exists a_i \in \operatorname{Spek}\Phi : \Phi(s_i) = a_i s_i \iff D_S(\Phi) = \operatorname{Diag}(a_1, \ldots, a_n)$ ∎

Beispiel

$V = \mathbb{Q}^3$, $\Phi \in \operatorname{End} V$ *mit* $D_S(\Phi) = A = \begin{pmatrix} 3 & 1 & 1 \\ 2 & 4 & 2 \\ 1 & 1 & 3 \end{pmatrix}$ *bezüglich Standardbasis.*

$h_\Phi(X) = \det(XI_3 - A) = \det \begin{pmatrix} X-3 & -1 & -1 \\ -2 & X-4 & -2 \\ -1 & -1 & X-3 \end{pmatrix} = (X-3)^2(X-4) = -2 - 2 - (X-4) - 2(X-3) - 2(X-3) = X^3 - 10X^2 + 28X - 24 = (X-2)^2(X-6).$

zu 2: $Av = 2v \iff (A - 2I_3)v = 0 \iff \begin{pmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 1 & 1 & 1 \end{pmatrix} v = 0 \implies E_\Phi(2) = \langle (1,0,-1)^T, (1,-1,0)^T \rangle$

$E_\Phi(6) = \langle (-1,-2,-1)^T \rangle \overset{Krylov}{\implies} g_\Phi(X) = (X-2)(X-6)$

Satz 4, § 15 (*Cayley-Hamilton*)

V K-Vektorraum, $n = \dim V, \Phi \in \operatorname{End} V \implies h_\Phi(\Phi) = 0$ d.h. $g_\Phi | h_\Phi$.

Beweis: S Basis von V, $A = D_S(\Phi) \implies h_\Phi(X) = \det(XI_n - A) = \sum_{i=0}^n a_i X^i$ mit $a_i \in K$.

Sei $(XI_n - A)^\#$ die zu $XI_n - A$ kompl. Matrix $\implies (XI_n - A)^\# = \sum_{i=0}^{n-1} B_i X^i$ mit $B_i \in K^{n \times n} \overset{3,x13}{\implies} \left(\sum_{i=0}^{n-1} B_i X^i\right)(XI_n - a) = \det(XI_n - A) I_n$.

Mit $\sum_{i=0}^{n-1} B_i X^i = \sum_{i=0}^{n-1} B_i X^{i+1} - B_i A X^i = \sum_{i=0}^{n} (B_{i-1} - B_i A) X^i$ mit $B_1 = B_n = 0$ und einem Koeffizientenvergleich folgt:

$a_i I_n = B_{i-1} - B_i A$ für $i = 0, \ldots, n \implies \overset{\cdot A^i}{\implies} \sum_{i=0}^n a_i A^i = \sum_{i=0}^n B_{i-1} A^i - B_i A^{i+1} = B_{-1} - B_n A^{n+1} = 0 \implies h_\Phi(A) = 0 = h_\Phi(A) = D_S(h_\Phi(\Phi)) \implies h_\Phi(\Phi) = 0.$ ∎

Zusatz: Unter den Vorraussetzungen von Satz 4, § 15 gilt umgekehrt $h_\Phi | g_\Phi^n$. Insbesondere sind alle Primteiler von h_Φ auch Primteiler von g_Φ. (Beweis später.)

§ 16. Jordansche Normalform

16.1. Hauptraumzerlegung

Generalvoraussetzung in diesem Paragraphen $h_\Phi(X) = \prod_{i=0}^n (X - a_i)^{d_i}$ (allg. JNF in LA 2).

Definition 1, § 16

V K-Vektorraum, $\Phi \in \operatorname{End} V$, $W < V$ heißt Φ***-invariant*** $:\iff \Phi(W) < V$.

Satz 1, § 16 (*Hauptraumzerlegung*)

V endlich-dim., $\Phi \in \operatorname{End} V$, h_Φ wie oben.

a) $H_i := H_\Phi(a_i) := \ker(\Phi - a_i \operatorname{id}_V)^{d_i}$ ***Hauptraum*** *von Φ zu a_i ist Φ-invariant.*

b)

$$V = \bigoplus_{i=1}^{r} H_\Phi(a_i)$$

mit $\dim H_\Phi(a_i) = d_i$.

Beweis: Cayley-Hamilton $\implies h_\Phi(\Phi) = 0$ auf V. Kernspaltungssatz $\implies V = \bigoplus_{i=1}^{r} \ker\left((\Phi - a_i \operatorname{id}_V)^{d_i}\right)$.
Sei $v \in H_\Phi(a_i) \iff (\Phi - a_i \operatorname{id}_V)^{d_i}(v) = 0$.
$\implies (\Phi - a - i \operatorname{id}_V)^{d_i} \cdot \Phi(v) = \Phi \cdot (\Phi - a - i \operatorname{id}_V)^{d_i}(v) = 0$
$\implies \Phi(v) \in H_\Phi(a_i)$: Ist S_i Basis von $H_\Phi(a_i)$
$\implies S := \bigcup S_i$ Basis von V mit

$$D_S(\Phi) = \begin{pmatrix} D_{S_1}(\Phi|_{H_1}) & & \\ & \ddots & \\ & & D_{S_r}(\Phi|_{H_r}) \end{pmatrix}$$

$\implies h_\Phi(X) = \det(XI_n - D_S(\Phi)) = \prod_{i=1}^{r} (XI_{d_i} - D_{S_i}(\Phi|_{H_i})) = \prod_{i=1}^{r} h_{\Phi|_{H_i}}(X)$. zeige: $h_{\Phi|H_i}(X) = (X - a_i)^{d_i}$
Mipo: $g_{\Phi|H_i} = (X - a_i)^{e_i}$ mit $e_i = d_i$.
Wäre $(X - a_j) | h_{\Phi|H_i}$, so $a_i \in \operatorname{Spek} \Phi_{|H_i} (i \neq j)$ ↯
$\implies h_{\Phi|H_i}(X) = (X - a_i)^{c_i}$.
$c_i \geqslant e_i \implies c_i = d_i$. ∎

Bemerkung 1, § 16

R komm. Ring mit 1, $A = (a_{ij}) \in R^{r \times r}$, $A = \begin{pmatrix} A_1 & & * \\ & \ddots & \\ 0 & & A_r \end{pmatrix}$, $A_i \in R^{nri \times r_i} \implies \det A = \prod_{i=1}^{r} \det A_i$

Folgerung 1, § 16 (*Jordanzerlegung*)

$H := H_\Phi(a)$, $a = a_i$ *für ein i.*

$$\Phi|_H = a \cdot \operatorname{id}_H + \Psi$$

mit $\Psi^d = 0$ *(* $d = d_i$*).*

Beweis: $\Psi := \Phi_H - a\,\mathrm{id}_v \implies \Psi^d = 0$. ■

16.2. Nilpotente Endomorphismen

Definition 2, § 16

V K-Vektorraum, $\Psi \in \operatorname{End} V$ heißt nilpotent $:\iff \exists d \in \mathbb{N} : \Psi^d = 0$.

Satz 2, § 16

V endlich-dim. K-Vektorraum, $\Psi \in \operatorname{End} V$ nilpotent.
$e = \min\{d \in \mathbb{N} | \Psi^e = 0\} \implies \exists! d_i \in \mathbb{N}$ mit $ed_e + (e-1)d_{e-1} + \cdots + 2d_2 + 1d_1 = \dim V$
sowie Basis T von V mit:

$$D_T(\Psi) = \begin{pmatrix} J_e & & & & & & & & \\ & \ddots & & & & & & & \\ & & J_e & & & & & & \\ & & & J_{e-1} & & & & & \\ & & & & \ddots & & & & \\ & & & & & J_{e-1} & & & \\ & & & & & & \ddots & & \\ & & & & & & & J_1 & \\ & & & & & & & & \ddots \\ & & & & & & & & & J_1 \end{pmatrix} \tag{III.15}$$

wobei jedes J_k d_k-mal auftritt und J_k ***Jordankästen*** *der Form*

$$J_k = \begin{pmatrix} 0 & & & 0 \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ 0 & & 1 & 0 \end{pmatrix} \tag{III.16}$$

sind.

Beweis: Sei $U_i := \ker \Psi^i$. Dann $U_i \leqslant U_{i+1}$ da wenn $\Psi^i(v) = 0 \implies \Psi^{i+1}(v) = \Psi(\Psi^i(v)) = 0 \implies 0 = U_0 \leqslant U_1 \leqslant \ldots U_e = V$ für $i = 0, \ldots, e-1$ und sogar $<$ statt $\leqslant$, da sonst $U_i = U_{i+1} \implies \dim\ker\Psi^i = \dim\ker\Psi^{i+1}$ und $\Psi^i(V) \geqslant \Psi^{i+1}(V) = \Psi^i(\Psi(v)) \overset{\text{Dim.-Formel}}{\implies} \dim\Psi^i(V) = \dim\Psi^{i+1}(V)$.
$\implies W = \Psi^i(V) = \Psi^{i+1}(V) = \Psi(\Psi^i(V)) = \Psi(W) \implies \Psi$ bijektiv $\lightning$ zu $\Psi^e = 0$.

Behauptung 1 $\forall i = 1, \ldots, e : \{v \in V | \Psi(v) \in U_{i-1}\} \overset{\text{Def.}}{=} \Psi^{-1}(U_{i-1}) \overset{!}{\implies} U_i$ und $\Psi(U_i) \leqslant U_{i-1}$.
Gilt, da wenn $\Psi(v) \in U_{i-1} \iff \Psi^{i-1}(\Psi(v)) = 0 \iff \Psi^i(v) = 0 \iff v \in U_i$

Behauptung 2 ist $W < V$ mit $W \cap U_1 = 0 \implies \Psi|_W$ injektiv (klar).

$V = U_e$. Nach Satz **??** $\exists W_e \leqslant V : V = U_{e-1} \oplus W_e$. Nach Beh. 1: $\Psi^{-1}(U_{e-2}) = U_{e-1} \implies \Psi(W_e) \cap U_{e-2} = 0$ Nach Beh. 1: $\Psi^{-1}(U_{e-2}) = U_{e-1} \implies \Psi(W_e) \cap U_{e-2} = 0$.

$\Longrightarrow \tilde{W}_{e-1} \leqslant V : U_{e-1} = U_{e-2} \oplus \Psi(W_e) \oplus \tilde{W}_{e-1}$ da $\Psi(W_e) \leqslant \Psi(U_e) \leqslant U_{e-1}$.
Beh. 1: $\Psi^{-1}(U_{e-3}) = U_{e-2} \Longrightarrow \Psi(W_{e-1}) \cap U_{e-3} = 0 \Longrightarrow \exists \tilde{W}_{e-2}$:

$$U_{e-2} = U_{e-3} \oplus \underbrace{\Psi(W_{e-1})}_{W_{e-2}} \oplus \tilde{W}_{e-2} = U_{e-3} \oplus W_{e-2} \dots$$

$\Longrightarrow V = \bigoplus_{i=1}^{e} W_i$ und $\Psi(W_i) \leqslant W_{i-1}$ für $i = 2, \dots, e$ und $\Psi(W_i) = \Psi(U_i) = 0$ und $\Psi|_{W_i}$ injektiv für $i = 2, \dots, e$, da $W_i \cap U_i = 0$ und Beh. 2. $\Longrightarrow V$ hat folgende Basis: $T = UT_j^{(i)}$

$$W_e : s_1^{(1)}, \dots, s_{d_e}^{(1)} \tag{III.17}$$
$$W_{e-1} : \Psi(s_1^{(1)}), \dots, \Psi(s_{d_e}^{(1)}), s_1^{(2)}, \dots, s_{d_{e-1}}^{(2)} \tag{III.18}$$
$$\vdots \tag{III.19}$$
$$W_1 : \underbrace{\Psi^{(e-1)}(s_1^{(1)})}_{T_1^{(1)}}, \dots, \underbrace{\Psi^{(e-1)}(s_{d_e}^{(1)})}_{T_{de}^{(1)}}, \underbrace{\Psi^{(e-2)}(s_1^{(2)})}_{T_1^{(2)}}, \dots, \Psi^{(e-2)}(s_{d_{e-1}}^{(2)}), \dots, s_1^{(e)}, \dots s_{d_1}^{(e)} \tag{III.20}$$

und damit die Darstellungsmatrix

$$D_{T_j^{(i)}}(\Psi|_{\dots}) = \begin{pmatrix} 0 & & & & \\ 1 & 0 & & & \\ & 1 & \ddots & & \\ & & \ddots & \ddots & \\ & & & 1 & 0 \end{pmatrix} \tag{III.21}$$

Eindeutigkeit der d_i: $\forall i = 1, \dots, e : U_i = U_{i-1} \oplus W_i = U_{i-1} \oplus \Psi(W_{i+1}) \oplus \tilde{W}_i$ mit $W_{e+1} = 0 \Longrightarrow$ $d_i = \dim \tilde{W}_i = \dim U_i - \dim U_{i-1} - \dim \Psi(W_{i+1})$ ist rekursiv aus ■

16.3. Die Jordansche Normalform

Satz 3, § 16

V endlich-dimensionaler K-Vektorraum, $\Phi \in \operatorname{End} V$ mit $h_\Phi(X) = \prod_{i=1}^{r}(X - a_i)^{d_i} \Longrightarrow$ $V = \bigoplus_{i=1}^{r} H_\Phi(a_i) = \bigoplus_{i=1}^{r} H_i$ hat Basis $T = \bigcup_{i=1}^{r} T_i$ mit $D_{T_i}(\Phi|_{H_i})$ die Form hat. Dabei git $g_\Phi(X) = \prod_{i=1}^{r}(X - a_i)^{e_i}$ mit $e_i = \min\{d \in N | (\Phi - a_i)^d = 0\}$.

Beweis: Satz $\Longrightarrow V = \bigoplus_{i=1}^{r} H_i, \Phi_{H_i}$ hat Hauptpolynom $(X - a_i)^{d_i} \Longrightarrow \Psi_i := (\Phi|_{H_i} - a_i \operatorname{id}_V)$ ist nilpotent. $\Longrightarrow$ Mipo von $\Phi|_{H_i}$ ist $g(X) = (X - a_i)^{e_i}$, e_i wie oben.

Satz $\Longrightarrow \exists T_i$ Basis wie oben von H_i mit

$$\underbrace{D_{T_i}}_{a_i \operatorname{id}_V + \Psi_i}(\Phi|_{H_i}) = \begin{pmatrix} J_{e_i}(a_i) & & \\ & \ddots & \\ & & J_1(a_i) \end{pmatrix} \tag{III.22}$$

■

16.4. Berechnung der JNF

V, Φ wie in Satz . Sach gibt uns Algorithmus, wie man für $H = H_i = \ker(\Phi - a_i)^{d_i}$ eine Basis findet, dodass $\Phi|_H$ die JNF bezüglich dieser Basis ist. sei $e = e_i$ sodass $\Psi^e(\Phi - a_i)^e = 0$ minimal. Berechne $0 = U_0 < U_1 < \cdots < U_e = V$, d.h. finde Basis S_1 von in U_1, ergänze zu Basis S_2 von U_2, ergänze ....
Dann: für jedes $t_j^{(1)} \in S_e \backslash S_{e-1}$ bilde $\Psi(t_j^{(1)}) \forall j$, ergänze $\{\Psi(t_j^{(i)})\}$ aus $S_{e-1} \backslash S_{e-2}$ zu Basis von $W_{e-2}, \ldots$ usw.

Beispiel

$V = \mathbb{Q}^3, S$ *Standardbasis,* $D_S(\Phi) = \begin{pmatrix} 2 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix}$

$\implies h_\Phi(X) = \det \begin{pmatrix} X-2 & 0 & -1 \\ 0 & X-1 & 0 \\ 1 & 0 & X \end{pmatrix} = (X-2)(X-1)X + (X-1) = (X-1)(X^2 - 2X + 1) = (X-1)^3$. *Für welche* v *gilt* $\Phi(v) = 1v?$ $\iff (1\,\mathrm{id}_V - \Phi)v = 0$ $\rightsquigarrow E_\Phi(1) = \langle (0,-1,0)^T, (1,0,-1)^T \rangle$.
Ergänze zu $t = (1,0,0)^T$ *zu Basis von* $V = \ker(\Phi - 1\,\mathrm{id}_V)^2), < (1,0,0)^T >= W_2$. *Sei* $t_2 = (\Phi - 1\,\mathrm{id})(t) = (2,0,-1)^T - (1,0,0) = (1,0,-1) = t_2 \implies$ *nehme* $t_3 = (0,1,0)^T \implies$ $T = \{t_1, t_2, t_3\}$: $D_T(\Phi) = \begin{pmatrix} 1 & & \\ 1 & 1 & \\ & & 1 \end{pmatrix}$. *JNF mit* $C_S^T = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix} \implies C_T^S = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix} \implies D_T(\Phi) = C_T^S D_S(\Phi) C_S^T$.

IV. Innenprodukträume

§ 17. Innenprodukte und Orthogonalität

17.1. Hermitesche Formen

Ab jetzt: $K = \mathbb{R}, \mathbb{C}$. Betrachte $\mathbb{C} = \mathbb{R}^2$ als $\mathbb{R}$-Vektorraum mit Basis $1, i$.
$i^2 = -1,\ a \in C : a = a_0 + ia_1,\ a_0, a_1 \in \mathbb{R},\ \mathfrak{R}(a) = a_0, \mathfrak{I}(a) = a_1 \in \mathbb{R}$ heißten Realteil bzw. Imaginärteil.
Die Abbildung $\bar{\cdot}\colon \mathbb{C} \to \mathbb{C},\ a = a_0 + ia_1 \mapsto a_0 - ia_1$ heißt komplexe Konjugation mit $\overline{a+b} = \overline{a} + \overline{b}$, $\overline{ab} = \overline{a} \cdot \overline{b}$ und $\overline{(\overline{a})})a$. Die kompl. Konj. ist Körperisomorphismus.
Der Betrag $|\cdot|\colon \mathbb{C} \to \mathbb{R},\ a = a_0 + ia_1 \mapsto \sqrt{a_0^2 + a_1^2}$.
Einbettung: $\mathbb{R} \to \mathbb{C}, a \mapsto a + i \cdot 0$.

Definition 1, § 17

*$K \in \{\mathbb{R}, \mathbb{C}\}$, V K-Vektorraum. Eine Abbildung $\langle \cdot, \cdot \rangle\colon V \times V \to K,\ (v, w) \mapsto \langle v, w \rangle$ heißt eine auf V erklärte **Hermitesche Form**, falls $\forall v_i, w_i \in V,\ a \in K$ gilt:*

$$\langle av_1 + v_2, w \rangle = a\langle v_1, w \rangle + \langle v_2, w \rangle \tag{IV.1}$$

$$\langle v, bw_1 + w_2 \rangle = \overline{b}\langle v, w_1 \rangle + \langle v, w_2 \rangle \tag{IV.2}$$

$$\langle v, w \rangle = \overline{\langle w, v \rangle} \tag{IV.3}$$

*$\langle \cdot, \cdot \rangle$ heißt **positiv semidefinit** $:\iff \forall v \in V : \langle v, v \rangle \geqslant 0$. $\langle \cdot, \cdot \rangle$ heißt **positiv definit** $:\iff \forall v \neq 0 : \langle v, v \rangle > 0$.*
*Ist $K = \mathbb{R} \implies x \in K : \overline{x} = x \implies \langle \cdot, \cdot \rangle$ (pos. def.) **symmetrische Bilinearform**.*
$K = \mathbb{C} \implies \langle \cdot, \cdot \rangle$ (pos. def.) Sesquilinearform.

Beispiel 1, § 17

1) *$K = \mathbb{R}, V = \mathbb{R}^n, S$ Standardbasis, $v = \sum_{i=1}^n a_i s_i,\ w = \sum_{i=1}^n b_i s_i$.*
   $\langle v, w \rangle := \sum_{i=1}^n a_i b_i \in \mathbb{R} \implies \langle v, v \rangle = \sum_{i=1}^n a_i^2 = 0 \iff v = 0 \implies$ pos. def. symm. Bilinearform.

2) *$K = \mathbb{C}, V = \mathbb{C}^n, S, v, w$ wie im 1. Beispiel. $\implies \langle v, w \rangle := \sum -i = 1^n a_i \overline{b_i} \implies \langle v, v \rangle = \sum_{i=1}^n a_i \overline{a_i} = \sum_{i=1}^n |a_i|^2 \geqslant 0, = 0$ falls $v = 0$.*

3) *$K = \mathbb{R}, I = [0, 1]$ abg. Intervall in R, $C_I = \mathbb{R}^I$ VR der stetigen Funktionen $f\colon I \to \mathbb{R}$. Sei $\langle f, g \rangle = \int_I f(t)g(t)\,\mathrm{d}t$ und $\langle f, f \rangle = \int_I f(t)^2\,\mathrm{d}t \geqslant 0$ und $= 0 \iff f = 0$.*

4) $K = \mathbb{R}, V = \mathbb{R}^4, c \in \mathbb{R}$, $\langle v, w\rangle := \sum_{i=1}^{3} a_i b_i - c a_4 b_4$ *ist Hermitesche Form, aber nicht positiv semidefinit für* $c \neq 0$ *genannt* ***Lorentzform***.

17.2. Das Innenprodukt

Definition 2, § 17

Ein Paar $(V, \langle\cdot,\cdot\rangle)$ *bestehtnd aus einem K-VR V, einer pos. def. Hermiteschen Form* $\langle\cdot,\cdot\rangle$ *heißt* ***reeller (bzw. komplexer) Innenproduktraum*** *(bzw.* ***Euklidscher/unitärer VR****).*
$\langle v, w\rangle$ *heißt* ***inneres Profukt*** *von* v, w *(bzw.* ***Skalarprodukt****).*
v, w *heißen* ***orthogonal*** *(*$v \perp w$*)* $: \iff \langle v, w\rangle = 0$.
$v \in V \implies |v| := \sqrt{\langle v, v\rangle} \in \mathbb{R}_{\geqslant 0}$ *heißt* ***Betrag*** *oder Länge von* v. $v, w \in V : |v - w|$ ***Abstand*** *von* v, w.

Satz 1, § 17

In einem Innenproduktraum (IPR) V gelten:

a) $v \in V : |v| \geqslant 0, |v| = 0 \iff v = 0$.

b) $a \in K, v \in V : |av| = |a||v|$.

c) $\forall v, w \in V : |\langle v, w\rangle| \leqslant |v||w|$ *(Cauchy-Shwarz-Ungleichung)*

d) $\forall v, w \in V : |v + w| \leqslant |v| + |w|$ *(Minkowski-Ungleichung).*

Beweis : a) aus Def.

b) $|av|^2 = \langle av, av\rangle = a\bar{a}\langle v, v\rangle = |a|^2|v|^2$

c) 1. Fall: $w = 0 \implies \langle v, w\rangle = \langle v, 0w\rangle = 0\langle w, w\rangle = |w|^2 = |w|$.

2. Fall: $w \neq 0 \implies |w| \neq 0$. $\forall c \in \mathbb{C}$:

$$0 \leqslant \langle v - cw, v - cw\rangle = \langle v, v\rangle - c\langle w, v\rangle - \bar{c}\langle v, w\rangle + c\bar{c}\langle w, w\rangle$$

Multiplikation mit $|w|^2$, $c = \frac{\langle v,w\rangle}{|w|^2} \implies$

$$0 \leqslant |v|^2|w|^2 - \langle\overline{v, w}\rangle\langle v, w\rangle - \langle\overline{v, w}\rangle\langle v, w\rangle + \langle\overline{v, w}\rangle\langle v, w\rangle = |v|^2|w|^2 - |\langle v, w\rangle|^2$$

$\implies$ Beh.

d)

$$
\begin{aligned}
|v+w|^2 = \langle v+w, v+w\rangle &= \langle v,v\rangle + \langle v,w\rangle + \langle w,v\rangle + \langle w,w\rangle && \text{(IV.4)}\\
&= |v|^2 + 2\underbrace{\Re(\langle v,w\rangle)}_{\leqslant|\langle v,w\rangle|} + |w|^2 && \text{(IV.5)}\\
&\leqslant |v|^2 + 2\underbrace{|\langle v,w\rangle|}_{\leqslant|v||w|} + |w|^2 && \text{(IV.6)}\\
&\leqslant |v|^2 + 2|v||w| + |w|^2 && \text{(IV.7)}\\
&= (|v|+|w|)^2 && \text{(IV.8)}
\end{aligned}
$$

■

Folgerung 1, § 17 (*Satz von Pythagoras*)

$$v \perp w \implies |v+w|^2 = |v|^2 + |w|^2$$

17.3. Orthonormalbasen

Definition 3, § 17

*V IPR. Eine Menge $\{s_i | i \in I\} \subseteq V$ mit $\langle s_i, s_j\rangle = c_{ij}\delta_{ij}$, $c_{ij} = c_i \in \mathbb{R}_{\geqslant 0}$ heißt **Orthogonalsystem** (OS) von V. Es ist ein **Orthonormalsystem** falls $c_i = 1 \forall i$ (ONS) und **Orthonormalbasis** (ONB) falls Basis und ONB.*

Beispiel 2, § 17

$K = \mathbb{R}$ oder $\mathbb{C}$. $V = K^n, \langle\cdot,\cdot\rangle$ Standardskalarprodukt $\implies$ S Standardbasis von V ist ONB bzgl. $\langle\cdot,\cdot\rangle$.

Satz 2, § 17 (*Orthonormalisierungsverfahren von Gram-Schmidt*)

V IPR. $v_1, v_2, \ldots$ Folge von linear unabhängigen Vektoren $\implies$ $\exists$ gleichlange Folge $s_1, s_2, \ldots$ mit $\langle s_i, s_j = \delta_{ij}$ und $\langle s_1, \ldots, s_n\rangle = \langle v_1, \ldots, v_n\rangle \forall n$.

Beweis : Induktion nach n.

n=1: $s_1 = \frac{v_1}{|v_1|} \implies \langle s_1, s_1\rangle = 1$

n $\rightsquigarrow$ n+1: $w_{n+1} := v_{n+1} - \sum_{j=1}^{n} a_j s_j \implies \langle w_{n+1}, s_j\rangle = \langle v_{n+1}, s_j\rangle - a_j$ d.h. $w_{n+1} \perp s_j \iff a - j = \langle v_{n+1}, s_j\rangle \implies$ Wähle a_j so: $s_{m+1} := \frac{w_{n+1}}{|w_{n+1}|} \implies |s_{n+1}| = 1$, $\langle s_{n+1}, s_j\rangle = 0 \ \forall j \neq n+1$ und für $j = 1, \ldots, n : \langle s_1, \ldots, s_{n+1}\rangle = \langle v_1, \ldots, v_n, s_{n+1}\rangle = \langle v_1, \ldots v_{n+1}\rangle$. ■

Folgerung 2, § 17

Jeder endlich-dim. IPR hat eine ONB.

Anmerkung 1, § 17

Folgerung gilt auch noch für VR mit abzählbarer unendlicher Dimension (Basis durch $\mathbb{N}$

indiziert).

Beispiel (*Orthogonale Projektion*)

$K = \mathbb{R}$, $V = \mathbb{R}[X]$ *und fasse als Polynomfn in X, d.h.* $f\colon \mathbb{R} \to \mathbb{R}$. $\int_0^1 f(x)g(x)\,\mathrm{d}x$ *Innenprodukt auf* $\mathbb{R}[X]$.
Suche ONB ausgehend von $v_1 := 1, v_2 := X, v_3 := X^2, v_4 := X^3, \ldots$.
$\int_0^1 1 \cdot 1\,\mathrm{d}x = x|_0^1 = 1 \implies s_1 \implies |v_1| = 1 \implies s_1 = v_1$.
$w_2 := v_2 - \langle v_2, s_1\rangle \cdot s_1 = X - \left(\int_0^1 x \cdot 1\,\mathrm{d}x\right) \cdot 1 = X - \frac{1}{2}x^2|_0^1 = X - \frac{1}{2} \implies |w_2|^2 = \int_0^1 \left(X - \frac{1}{2}\right)^2 = \int_0^2 \left(x^2 - x + \frac{1}{4}\right) = \frac{x^3}{3} - \frac{1}{2}x^2 + \frac{1}{4}x^2|_0^1 = \frac{1}{3} - \frac{1}{2} + \frac{1}{4} = \frac{1}{1} \implies s_2 := \sqrt{12}w_2 = \sqrt{12}\left(X - \frac{1}{2}\right)$.
$s_3 = 6 \cdot \sqrt{5}\left(X^2 - X + \frac{1}{2}\right), \ldots$

17.4. Orthogonales Komplement

Definition 4, § 17

V IPR, $M \subseteq V$ *Teilmenge* $\implies$

$$M^\perp := \{v \in V | \langle v, m\rangle = 0 \ \forall m \in M\}$$

heißt ***orthogonales Komplement zu M****.*

Anmerkung 2, § 17

$M^\perp \leqslant V$ *wegen* $v_1 + v_2 \in M^\perp$ *und* $a \cdot v_1 \in M^\perp$ *für* $v_1, v_2 \in M^\perp,\ a \in K$.

Satz 3, § 17

V IPR, $W < V$ *mit W endlich-dimensional.*

$$V = W \oplus W^\perp$$

Beweis: Folgerung 1, § 17 $\implies$ W besitzt ONB $S = \{s_1, \ldots, s_n\} \subseteq V$.

$\pi_w(v) := \sum_{j=1}^n \langle v, s_j\rangle \cdot s_j \in W$ für $v \in V \implies \pi_w\colon V \to W$ ist linear und $\langle v - \pi_w(v), s_k\rangle \overset{k=j}{=} \langle v, s_k\rangle\langle v, s_k\rangle \cdot 1 = 0 \quad \forall s_k \in S \implies v - \pi_w(v) \in W^\perp \implies v = v - \underbrace{\pi_w(v)}_{\in W^\perp} + \underbrace{\pi_w(v)}_{\in W} \implies v \in W + W^\perp$.

Ist $v \in W \cup W^\perp \implies v \in W$ und $\langle v, w\rangle = 0\ \forall w \in W \implies \langle v, v\rangle = 0 \implies |v| = 0 \overset{\text{S. 1, § 17}}{=} v = 0$. ■

Anmerkung 3, § 17

Satz ist für unendlich-dim. VR im allgemeinen falsch.

Definition 5, § 17

Die Abbildung $\pi_w\colon V \to W$ *heißt* ***orthogonale Projektion*** *von V auf W.*

Folgerung 3, § 17 (*Bessel'sche Ungleichung*)

V IPR, $v \in V$, $S = \{s_1, \ldots, s_n\}$ ONB von $W < V$ endlichdim. $\Longrightarrow$

$$|\pi_w(v)|^2 = \sum_{j=1}^{n} |\langle v, s_j\rangle|^2 \leqslant |v|^2$$

Beweis: $|v|^2 = |\underbrace{v - \pi_w(v)}_{\in W^\perp} + \underbrace{\pi_w(v)}_{\in W}|^2 \overset{\text{Pyth.}}{=} \underbrace{|v - \pi_w(v)|^2}_{\geqslant 0} + |\pi_w(v)|^2 \implies |v|^2 \geqslant |\pi_w(v)|^2$

$|\pi_w(v)|^2 = \langle \pi_w(v), \pi_w(v)\rangle \overset{\text{Def.}}{=} \sum_{j=1}^n \sum_{k=1}^n \langle v, s_j\rangle \cdot \overline{\langle v, s_k\rangle} \cdot \langle s_j, s_k\rangle = \sum_{j=1}^n |\langle v, s_j\rangle|^2$. ■

Folgerung 4, § 17

V IPR, $W < V$ endlich-dim. Teilraum.

$$|v - \pi_w(v)| = \min\{|v - w| \ : \ w \in W\}$$

Beweis: $w \in W : v - w = \underbrace{v - \pi_w(v)}_{\in W^\perp} + \underbrace{\pi_w(v) - w}_{\in W} \overset{\text{Pyth.}}{\Longrightarrow} |v - w|^2 = |v - \pi_w(v)|^2 + \underbrace{|\pi_w(v) - w|^2}_{\geqslant 0}$

($w = \pi_w(v)$ nimmt Minimum an). ■

17.5. Selbstdualität

Satz 4, § 17

V endlich-dimensional. IPR über K, $V^* = \mathrm{Hom}(V, K)$ $\Longrightarrow$

$$\forall f \in V^* \ \exists! w \in V : f(v) = \langle v, w\rangle$$

Beweis: Eindeutigkeit $w_1, w_2 \in V$ mit $\langle v, w_1\rangle = \langle v, w_2\rangle \ \forall v \in V \implies \langle v, w_1 - w_2\rangle = 0 \ \forall v \in V \overset{v = w_1 - w_2}{\Longrightarrow} \langle w_1 - w_2, w_1 - w_2\rangle = 0 = |w_1 - w_2|^2 \overset{S.1, x17}{w}_1 - w_2 = 0 \implies w_1 = w_2$.

Existenz $w \in V \implies f_w \colon V \to K, v \mapsto \langle v, w\rangle \implies f_w \in V^*$ (nachrechnen).

$L = \{f_w | w \in V\} \subseteq V^*$ und UVR, da $f_{w_1} + f_{w_2} = f_{w_1 + w_2}$, $a f_w = f_{\bar{a} \cdot w}$. Sei $S = \{s_1, \ldots, s_n\}$ eine ONB von V. Wir schreiben $f_i := f_{s_i} \implies f_{s_i}(s_k) = \langle s_k, s_i\rangle \overset{\text{ONB}}{=} \delta_{ik} \overset{\text{Def.}}{\Longrightarrow} f_i = s_i^* \implies L = V*$, da UVR und alle Basiselemente enthalten. ■

Folgerung 5, § 17

Die Abb. $\lambda \colon V \to V^*, \ w \mapsto f_w = \langle \cdot, w\rangle$ ist bijektiv mit $f_{w_1 + w_2} = f_{w_1} + f_{w_2}$ und $f_{\bar{a}w} = a f_w$ für $w_i \in V, a \in K$.

Beweis: Klar mit Satz 4, § 17 ■

§ 18. Normale Operatoren

18.1. Adjungierte lineare Abbildungen

Bemerkung 1, § 18

V, W endlich-dim. IPR, $\Phi\colon V \to W$ linear $\Longrightarrow$ es existiert eine eindeutig bestimmte lineare Abbildung $\Phi^{ad}\colon W \to V$ mit

$$\langle \Phi(v), w\rangle_W = \langle v, \Phi^{ad}(w)\rangle_V \quad \forall v \in V, w \in W$$

Beweis: $\Phi \in \mathrm{Hom}(V,W)$, $w \in W \Longrightarrow \lambda\colon V \to K, \langle \Phi(v), w\rangle_W$ und $\lambda \in V^*$. Mit Satz 4, § 17 folgt dann, dass ein eindeutiges $x \in V$ existiert mit $\langle \Phi(v), w\rangle_W = \langle v, x\rangle_V \rightsquigarrow$ setze $\Phi^{ad}(w) = x$.

$\Longrightarrow$ Φ^{ad} ist wohldef. und hat die Eigenschaft

$$\langle \Phi(v), w\rangle_W = \langle v, \Phi^{ad}(w)\rangle_V \quad \forall v \in V, w \in W$$

und eindeutig dadurch bestimmt. Noch zu zeigen ist, dass Φ^{ad} linear ist.

$\forall v \in V, w_i \in W, a \in K : \langle v, \Phi^{ad}(aw_1 + w_2)\rangle_V = \langle \Phi(v), aw_1 + w_2\rangle_W = \bar{a}\langle \Phi(v), w_1\rangle_W + \langle \Phi(v), w_2\rangle_W = \langle v, \Phi^{ad}(w_1)\rangle + \langle v, \Phi^{ad}(w_2)\rangle_v = \langle v, a\Phi^{ad}(w_1)\rangle_V + \langle v, \Phi^{ad}(w_2)\rangle_V = \langle v, a\Phi^{ad}(w_2) + \Phi^{ad}(w_2)\rangle_V \ \forall v \Longrightarrow \Phi^{ad}(aw_1 + w_2) = a\Phi^{ad}(w_1) + \Phi^{ad}w_2)$ d.h. linear. ■

Definition 1, § 18

$\Phi^{ad} \in \mathrm{Hom}(W,V)$ heißt die zu Φ ***adjungierte Abbildung*** *(linear!).*

Satz 1, § 18

Für die adjungierte Abbildung gilt:

a) $(\Phi + \Psi)^{ad} = \Phi^{ad} + \Psi^{ad}$

b) $(a\Phi)^{ad} = \bar{a} \cdot \Phi^{ad}$

c) $(\Psi \circ \Phi)^{ad} = \Phi^{ad} \circ \Psi^{ad}$

d) $(\Phi^{ad})^{ad} = \Phi$

Beweis: a),b) $\Phi, \Psi \in \mathrm{Hom}(V,W), a \in K \Longrightarrow \forall v \in V : w \in W : \langle v, (a\Phi + \Psi)^{ad}(w)\rangle = \langle (a\Phi + \Psi)(v), w\rangle = a\langle \Phi(v), w\rangle + \langle \Psi(v), w\rangle = a\langle v, \Phi^{ad}(w)\rangle + \langle v, \Psi^{ad}(w)\rangle = \langle v, \bar{a}\Phi^{ad}(w) + \Psi^{ad}(w)\rangle \Longrightarrow (a\Phi + \Psi)^{ad} = \bar{a} = \Phi^{ad} + \Psi^{ad}$.

c) $\Phi\colon V \to W$, $\Psi\colon W \to X$, $\forall v \in V, x \in X : \langle v, (\Psi\circ\Phi)^{ad}(x)\rangle_V = \langle \Psi\circ\Phi(v), x\rangle_X = \langle \Phi(v), \Psi^{ad}(x)\rangle_W = \langle v, \Psi^{ad}(\Phi^{ad}(x))\ \Longrightarrow\ (\Psi \circ \Phi)^{ad} = \Phi^{ad} \circ \Psi^{ad}$

d) $\Phi \in \mathrm{Hom}(V,W) \Longrightarrow \Phi^{ad} \in \mathrm{Hom}(W,V) \Longrightarrow (\Phi^{ad})^{ad} \in \mathrm{Hom}(V,W)$ mit $\forall v \in V, w \in W\colon \langle \Phi^{ad}(w), v\rangle_V = \langle w, (\Phi^{ad})^{ad}(v)\rangle_W$. Andererseits: $\langle \Phi^{ad}(w), v\rangle_V = \overline{\langle v, \Phi^{ad}(w)\rangle} = \overline{\langle \Phi(v), w\rangle_W} = \langle w, \Phi(v)\rangle_W \ \forall v \in V, w \in W \Longrightarrow$ Beh. ■

Folgerung 1, § 18

V, W endlich-dim. K-Vektorräume, $\dim V = n$, $\dim W = m$, IPRe mit ONBs. $S = \{s_1, \ldots, s_n\}$, bzw. $T = \{t_1, \ldots, t_n\}$, $\Phi \in \mathrm{Hom}(V, W)$

$$D_S^t(\Phi^{ad}) = \overline{D_T^S(\Phi)}^{tr}$$

Beweis: $\Phi(s_j) = \sum_{i=1}^m d_{ij} t_i \implies D_T^S(\Phi) = (d_{ij})_{i,j} \in K^{m\times n}$
$\Phi^{ad}(t_i) = \sum_{k=1}^n c_{ki} s_k \implies D_S^T(\Phi^{ad}) = (c_{ki})_{ki} \in K^{n\times m}$
$d_{ij} = \langle \Phi(s_j), t_i\rangle_W = \langle s_j, \Phi^{ad}(t_i)\rangle = \overline{c_{ji}} \cdot 1 = \overline{c_{ji}}$ ■

Bezeichnung: $A \in K^{m\times n} \implies A^{ad} := \overline{A}^{tr}$ die zu **A adjungierte Matrix** $\implies (A+B)^{ad} = \overline{A}^{tr} + \overline{B}^{tr}$, $(aA)^{ad} = \overline{a} \cdot A^{ad}$, $(AB)^{ad} = B^{ad}A^{ad}$, $(A^{ad})^{ad} = A$.

18.2. Selbstadjungierte Operatoren

Definition 2, § 18

*V IPR, $\Phi \in \mathrm{End}\, V$ heißt **selbstadjungiert** :* $\iff \Phi = \Phi^{ad}$.

Satz 2, § 18

V IPR, $\Phi \in \mathrm{End}\, V$. Dann sind äquivalent:

a) Φ ist selbstadjungiert.

b) $V \times V \to K$, $(v, w) \mapsto \langle v, w\rangle_\Phi = \langle \Phi(v), w\rangle$ ist eine Hermitesche Form.

Beweis: Allg.: $\Phi \in \mathrm{End}\, V$.

$\langle v_1 + v_2, w\rangle_\Phi = \langle \Phi(v_1 + v_2), w\rangle = \langle \Phi(v_1), w\rangle + \langle \Phi(v_2), w\rangle = \langle v_1, w\rangle_\Phi + \langle v_2, w\rangle_\Phi$. analog für zweites Argument.

$\langle av, w\rangle_\Phi = \langle \Phi(av), w\rangle = a\langle \Phi(v), w\rangle = a\langle v, w\rangle_\Phi$

analog: $\langle v, aw\rangle_\Phi = \bar{a}\langle v, w\rangle_\Phi$.

Außerdem: $\overline{\langle v, w\rangle_\Phi} = \overline{\langle \Phi(v), w\rangle} = \overline{\langle v, \Phi^{ad}(w)\rangle} = \langle \Phi^{ad}(w), v\rangle$, d.h. $\overline{\langle v, w\rangle}_\Phi \overset{!}{=} \langle w, v\rangle_\Phi = \langle \Phi(w), v\rangle \iff$
$\langle \Phi(w) - \Phi^{ad}(w), v\rangle = 0 \ \forall v, w \in V \iff \Phi(w) = -\Phi^{ad}(w) = 0 \iff \Phi = \Phi^{ad}$ ■

Bezeichnung: $\Phi \in \mathrm{End}\, V$ selbstadjungiert heißt **positiv (semi-)definit** : $\iff \langle \cdot, \cdot, \rangle_\Phi$ ist positiv (semi-)definit.

Bemerkung 2, § 18

Für einen selbstadjungierten Operator Φ eines IPR gilt $\Phi = 0 \iff \langle v, v\rangle_\Phi = 0 \ \forall v \in V$.

Beweis: „⇒“ klar.

„⇐“ Zeige erst: $\langle v, w\langle = 0\ \forall v, w$.

$0 = \langle v+w, v+w\rangle_\Phi = \langle v, v\rangle_\Phi + \langle v, w\rangle_\Phi + \langle w, v\rangle_\Phi + \langle w, w\rangle_\Phi = \langle v, w\rangle_\Phi + \overline{\langle v, w\rangle_\Phi} = 2\Re(\langle v, w\rangle_\Phi)$

$\forall v \in \mathbb{C} : \Re(\langle cv, w\rangle_\Phi) = \Re(c \cdot \langle v, w\rangle_\Phi) \implies$ Sei $c = \overline{\langle v, w\rangle_\Phi} \implies 0 = 2\Re(|\langle v, w\rangle_\Phi|^2) \implies |\langle v, w\rangle_\Phi| = 0 \implies \langle v, w\rangle_\Phi = 0$.

Setze $w = \Phi(v) \implies \langle v, \Phi(v)\rangle_\Phi = \langle \Phi(v), \Phi(v)\rangle = 0 \implies |\Phi(v)|^2 = 0 \implies \Phi(v) = 0 \forall v \implies \Phi = 0$. ■

18.3. Isometrien

Definition 3, § 18

*V IPR, $\Phi \in \operatorname{End} V$ heißt **Isometrie** : $\iff \Phi^{ad} \circ \Phi = \mathrm{id}$ ($\implies$ Φ invertierbar).*

Satz 3, § 18

Für einen linearen Operator Φ eines IPR sind äquivalent

a) Φ Isometrie

b) $\forall v, w : \langle \Phi(v), \Phi(w)\rangle = \langle v, w\rangle$.

c) $\forall v \in V : |\Phi(v)| = |v|$.

Beweis : a) $\implies$ **b)** $\langle \Phi(v), \Phi(w)\rangle = \langle v, \Phi^{ad}\Phi(w)\rangle = \langle v, w\rangle$

b) $\implies$ **c)** $|\Phi(v)|^2 = \langle \Phi(v), \Phi(v)\rangle = \langle v, v\rangle = |v|^2$.

c) $\implies$ **a)** $\forall v \in V : \underbrace{\langle \Phi(v), \Phi(v)\rangle}_{\in\mathbb{R}} = \underbrace{\langle v, v\rangle}_{\in\mathbb{R}} \implies \langle \Phi^{ad}\Phi(v), v\rangle = \langle v, v\rangle\ \forall v \in V \implies \langle (\underbrace{\Phi^{ad} \circ \Phi - \mathrm{id}}_{=:\Psi})(v), v\rangle = 0$.

Ψ selbstadj.: $\Psi^{ad} = (\Phi^{ad}\circ\Phi)^{ad} - \mathrm{id}^{ad} = \Phi^{ad}\circ(\Phi^{ad})^{ad} - \mathrm{id} = \Psi \implies \Psi = 0 \implies \Phi^{ad}\circ\Phi = \mathrm{id}$. ■

Folgerung 2, § 18

Φ Isometrie $\overset{b),\,c)}{\iff}$ Φ bildet ONB auf ONB ab.

Anwendung: $A = D_T^S(\Phi)$, Φ Isomorphismus. S Standardbasis bezüglich Standardskalarprodukt $\implies$ Spalten von A bilden ONB.

Folgerung 3, § 18

Die Isometrien eines IPR bilden eine Gruppe.

Beweis : Φ Isomorphismus $\implies \Phi \in \mathrm{Gl}(V) \implies \Phi^{-1} = \Phi^{ad}$ Isometrie.

Φ, Ψ Isometrien $\overset{c)}{\implies}$ $\Phi \circ \Psi$ Isometrie ($|\Phi \circ \Psi(v) = |\Psi(v) = |v|$) $\implies$ Isomorphismen bilden Untergruppe von $\mathrm{Gl}(V)$. ■

Bezeichnung: Die Gruppe der Isomorphismen eines IPR heißt:
$K = \mathbb{C}$: **unitäre Gruppe**, $U(V)$ bzw. $U_n(\mathbb{C})$ von V.
$K = \mathbb{R}$: **orthogonale Gruppe**, $O(V)$ bzw. $O_n(\mathbb{R})$ von V.

18.4. Normale lineare Operatoren

Definition 4, § 18

V IPR, $\Phi \in \operatorname{End} V$ heißt ***normal*** $: \iff \Phi^{ad} \circ \Phi = \Phi \circ \Phi^{ad}$.

Beispiel 1, § 18

1) Φ *selbstadjungiert.* $\Phi = \Phi^{ad} \implies \Phi$ *normal.*

2) Φ *Isometrie,* $\Phi^{ad} \circ \Phi = \mathrm{id} = \Phi \circ \Phi^{ad} \implies \Phi$ *normal.*

Satz 4, § 18

Für Φ linearer Operator auf IPR ist äquivalent:

a) Φ *ist normal*

b) $|\Phi(v)| = |\Phi^{ad}(v)| \ \forall v \in V$

Beweis :

$$|\Phi(v)|^2 - |\Phi^{ad}(v)|^2 = \underbrace{\langle \Phi(v), \Phi(v) \rangle}_{\in \mathbb{R}} - \langle \Phi^{ad}(v), \Phi^{ad}(v) \rangle \tag{IV.9}$$

$$= \langle v, \underbrace{\Phi^{ad} \circ \Phi(v)}_{= \langle \Phi^{ad} \circ \Phi(v), v \rangle} \rangle - \langle \Phi \circ \Phi^{ad}(v), v \rangle \tag{IV.10}$$

$$= \langle (\underbrace{\Phi^{ad} \circ \Phi - \Phi \circ \Phi^{ad}}_{= \Psi})(v), v \rangle \tag{IV.11}$$

Ψ selbstadjungiert: $\Psi^{ad} = (\Phi^{ad} \circ \Phi)^{ad} - (\Phi \circ \Phi^{ad})^{ad} = \Phi^{ad} \circ (\Phi^{ad})^{ad} - (\Phi^{ad})^{ad} \circ \Phi^{ad} = \Psi$.
D.h. $\forall v : |\Phi(v)| = |\Phi^{ad}(v)| \iff \langle \Psi(v), v \rangle = 0 \iff \Psi = 0 \iff \Phi^{ad} \circ \Phi = \Phi \circ \Phi^{ad} \iff \Phi$ normal ∎

Satz 5, § 18

Für einen normalen Operator Φ auf V gilt (IPR).

a) $\forall a \in \operatorname{Spek} \Phi : E_\Phi(a) = E_{\Phi^{ad}}(\bar{a})$ *insbes.:* $\ker \Phi = \ker \Phi^{ad}$

b) Φ *selbstadj.* $\implies \forall a \in \operatorname{Spek} \Phi : a \in \mathbb{R}$

c) Φ *positiv (semi-)definit* $\implies \forall a \in \operatorname{Spek} \Phi : a > 0$ *(bzw.* $a \geqslant 0$*)*

d) Φ *Isometrie* $\implies \forall a \in \operatorname{Spek} \Phi : |a| = 1$

Beweis: a) $v \in \ker\Phi \iff \Phi(v) = 0 \iff |\Phi(v)| = 0 \iff |\Phi^{ad}(v)| = 0 \iff \Phi^{ad}(v) = 0 \iff v \in \ker\Phi^{ad}$

Ist $a \in \operatorname{Spek}\Phi$, $\Psi = \Phi - a\,\mathrm{id} \implies \Psi^{ad} = \Phi^{ad} - \bar{a}\cdot\mathrm{id} \implies \Psi^{ad}\circ\Phi = (\Phi - a\,\mathrm{id})(\Phi^{ad} - \bar{a}\,\mathrm{id}) = \Phi\circ\Phi^{ad} - \bar{a}\Phi - a\Phi^{ad} + a\bar{a}\,\mathrm{id} \overset{\Phi \text{ normal}}{=} \Phi^{ad}\circ\Phi - \bar{a}\Phi - a\Phi^{ad} + a\bar{a}\,\mathrm{id} = (\Phi^{ad} - \bar{a}\,\mathrm{id})(\Phi - a\,\mathrm{id}) = \Psi\circ\Psi^{ad} \implies \Psi$ normal $\implies \ker\Psi = \ker\Psi^{ad} \implies E_\Phi(a) = E_{\Phi^{ad}}(\bar{a})$.

b) Φ selbstadj. $\iff \Phi = \Phi^{ad}$, d.h. $v \in E_\Phi(a) \iff v \in E_\Phi(\bar{a}) \iff a = \bar{a} \iff a \in \mathbb{R}$.

c) Φ pos. definit, $v \in E_\Phi(a) \implies 0 \leqslant \langle v, v\rangle_\Phi = \langle\Phi(v), v\rangle = \langle av, v\rangle = a\langle \underbrace{v, v}_{=|v|^2\neq 0} \rangle \implies a \geqslant 0$

d) Φ Isomorphismus, $v \in E_\Phi(a) \implies \langle\Phi(v), \Phi(v)\rangle = \langle av, av\rangle = a\bar{a}\langle v, v\rangle = |a|^2\langle v, v\rangle.\ \langle v, v\rangle \implies |a|^2 = 1 \implies |a| = 1$ ∎